

Homework

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

物理层：这一层涉及到在通信信道上传输的原始数据位。在设计的时候必须要保证，当一方发送了“1”时，在另一方收到的也是“1”而不是“0”

数据链路层：这一层的主要任务是将一个原始的传输设施转变成一条逻辑的传输线路，在这条线路上所有未检测出来的传输错误也会反映到网络层上。

网络层：这一层控制子网的运行过程。一个关键的设计问题是确定如何将分组从源端路由到目标端。

传输层：这一层的基本功能是接受来自上一层的数据，并且在必要的时候把这些数据分割成小的单元，然后把数据单元传递给网络层，并且确保这些数据片段都能够正确到达另一端。

会话层：允许不同机器上的用户之间建立对话。

表示层：这一层关注的是所传递的信息的语法和语义。

应用层：这一层包含了各种各样的协议，这些协议往往直接针对用户的需要。

2. Please explain the meaning of the following concepts: modulation, multiplexing.

Modulation: 调制：为了发送数字信息，必须设法用模拟信号来表示比特，比特与它们的信号

之间的转换过程称为数字调制。

Multiplexing: 多路复用: 一条物理干线上并发传输多个会话。

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

接收到的坏帧被丢弃, 但坏帧后面的好帧被缓存起来, 当发送方超时后或者发送一个否定的确认帧 NAK, 激发重发。若 NAK 也丢失的话, 只能等待定时器超时。

4. Please tell why 流量控制 is needed in the data link layer protocol.

当接收方的接收速度远小于发送方的发送速度时, 若发送方持续高速往外发送帧, 会导致接收方那边的缓冲满而丢失一些帧, 从而产生错误。这就说明了控制流的需要, 这样保证发送方不会因发送数据过快而淹没了接收方。

5. What does the following abbreviation stand for: PDU、MAC、CDMA、TDM、ARP

PDU: Protocol Data Unit
t 协议数据单元

MAC: Medium Access Control
rol 介质访问控制

CDMA: Code Division Multiplexing Access 码分多路访问

TDM: Timing Division Multiplexing 时分多路复用

ARP: Address Resolution Protocol 地址解析协议

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

若没有介质访问控制子层将无法确定多路访问信道上下一个使用者，所以必须得有介质访问控制子层。

带冲突检测的CSMA，当一个站已经完成了帧的传送，其他需要发送帧的站可以开始试图发送。若有两个或多个站同时进行传送的话，则冲突会发生。站检测到冲突时会立即停止它的传送任务，并等待一段随机的时间后再次重新尝试传送。

7. Please explain the principle of the ARP protocol.

当一个主机想向另一个主机发送分组时，该主机会发送一个广播分组到以太网上，询问拥有目的IP地址的主机。该广播会访问每一台以太网中的主机，并且每台主机都会检测自己的IP地址，拥有目的IP地址的主机会以自己的以太网地址作为应答，然后该主机就得到了拥有目的IP地址的主机的以太网地址。这里的广播和得到应答两个过程所使用的协议成为ARP。

8. 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。

(handles each packet as it arrives, looking up the

outgoing line to use for it in the routing tables)

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。(making the decision which routes to use)

9. 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: 要到达目的地址包要转发到路由器的哪一个接口 (即使用那个网卡)

10. Please tell the function of the Linux shell command ifconfig, and the command route.

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

11. 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: 距离矢量路由算法中每个节点只与其邻居节点交换信息, 总是能够收敛到正确答案但是速度可能非常慢, 并且当网络拓扑结构发生变化后产生无穷级数问题。而链路状态路由算法将完整的拓扑结构发给了每一个路由器, 需要更多的内存和计算, 没有慢收敛问题。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。

12. 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

13. 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。

14. 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？

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。

15. 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？

面向连接：信息在一条早已经建好的线路（通过三次握手的方式建立起来的）传输，中间不会有什么变化，可确保数据传送的次序和传输的可靠性。就像打电话要先拨号再讲话。

面向无连接：信息的传递线路是在发起传递前临时建立的，传完线路就没有了，是不可靠的，消除了除数据通信外的其它开销，是灵活的。就像写完信直接丢在邮筒里。

P27

- a) 面向连接的服务
- b) Modeled after the telephone system 基于电话系统
- c) to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then release the connection
- d) 无连接的服务
- e) Modeled after the postal system 基于邮件系统
- f) Each message carries the full destination address, and each one is routed through the system independent of all the others.

16. 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。

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

P103

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率发送。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。

18. 请说明数据链路层协议差错控制的基本方法。

P156

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。

19. 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。

允许接收方接受并缓存环帧或者丢失帧后面的所有帧。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。

20. 请说明Ethernet网中的介质访问控制算法的基本原理。

介质访问控制(MAC)在OSI网络模型中是一个数据链路层的下层，它决定谁被在任何时间允许访问物理介质。它作为在逻辑链路子层和网络物理层之间的一个接口。这个介质访问控制子层最初与访问物理传输介质（例如那个站点附到线上或频率范围有权利进行传输）或低水平介质共享协议例如CSMA/CD控制有关。MAC为在因特网协议(IP)网络上的计算机提供独特的鉴定和访问控制。MAC分配一个独特的编码到每个IP网络适配器叫做MAC地址。

21. 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IPv6的分组(Packet)？

22. 请说明域内路由(Intradomain Routing, Interior Gateway Routing)与域间路由(Inter-domain Routing, Exterior Gateway Routing)有什么不同？

域内路由是自治系统内部使用的路由选择协议，是为了解决局域网内电脑太多，IP地址不够用的问题(eg: 内部网关协议IGP如RIP和OSPF等)

域外路由是自治系统之间使用的路由选择协议，是为了让局域网或是单台电脑共同访问互联网而设置的，**具体是将一个AS的路由选择信息传递到另一个AS中。**（eg：外部网关协议EGP，如BGP）

23. 请说明在TCP/IP网络中怎样标识一个与外界进行通信的进程？怎样标识TCP/IP网络中的一条TCP连接？

进程 = { IP地址, port }

连接 = { 源IP, 源port, 目的IP, 目的port }

24. 请说明为什么在提供面向连接服务的传输层协议中需要使用三次握手机制？

谢希仁版《计算机网络》中的例子是这样的，“已失效的连接请求报文段”的产生在这样一种情况下：client发出的第一个连接请求报文段并没有丢失，而是在某个网络结点长时间的滞留了，以致延误到连接释放以后的某个时间才到达server。本来这是一个早已失效的报文段。但server收到此失效的连接请求报文段后，就误认为是client再次发出的一个新的连接请求。于是就向client发出确认报文段，同意建立连接。假设不采用“三次握手”，那么只要server发出确认，新的连接就建立了。由于现在client并没有发出建立连接的请求，因此不会理睬server的确认，也不会向server发送数据。但server却以为新的运输连接已经建立，并一直等待client发来数据。这样，server的很多资源就白白浪费掉了。采用“三次握手”的办法可以防止上述现象发生。例如刚才那种情况，client不会向server的确认发出确认。server由于收不到确认，就知道client并没有要求建立连接。”

这个例子很清晰的阐释了“三次握手”对于建立可靠连接的意义。

在Google Groups的[TopLanguage](#)中看到一帖讨论TCP“三次握手”觉得很有意思。贴主提出“[TCP建立连接为什么是三次握手？](#)”的问题，在众多回复中，[有一条回复](#)写道：“这个问题的本质是，信道不可靠，但是通信双方需要就某个问题达成一致。而要解决这个问题，无论你在消息中包含什么信息，三次通信是理论上的最小值。所以三次握手不是TCP本身的要求，而是为了满足“在不可靠信道上可靠地传输信息”这一需求所导致的。请注意这里的本质需求，信道不可靠，数据传输要可靠。三次达到了，那后面你接着握手也好，发数据也好，跟进行可靠信息传输的需求就没关系了。因此，如果信道是可靠的，即无论什么时候发出消息，对方一定能收到，或者你不关心是否要保证对方收到你的消息，那就能像UDP那样直接发送消息就可以了。”这可视作对“三次握手”目的的另一种解答思路。

25. 请说明TCP协议中端口的作用。 请说明TCP协议中的端口（Port）与TCP套接字（socket）有什么关系？

TCP协议中的端口具体指的是什么，为什么要有端口，你是怎么理解的？

其实你在问别人端口的概念的时候，很多解释都是机器是一个房间，窗户就好像是机器的端口。这个解释基本上没什么用，或者是个误导。

我在网上也查了些，基本上是上面的解释。从我自己的理解上将为什么要有端口，怎么来规划端口，看下边。

ip能锁定一台物理机器，对应着一张网卡，外界发来的数据包网卡都会接收。但是问题来了，网卡给程序提供了接口，你监听一下我，要是消息来了，我就转发给你。这样应用程序就能收到数据了。但是问题来了，程序A和程序B都需要监听网卡接发数据，网卡说那我把接到的数据都发给你两，你们自己看着办吧。好，小A小B都接受了。但是又来了CDEF.....，不行了，每个包都被发到了所有应用程序，每个应用程序都累得不行，最终垮了。

好，那网卡说我给你们加个表示吧，我们之间可以用一个号码来作为标识，我和小A之间就用1来标识，如果外界发给1号标识的数据我就转发给你，你监听我的时候得告诉我你监听的时1，我就转发1的数据包给你。好了其他的BCD...都自己弄一个标识号，只要不重复就行。这样大家都省事了。最后设计到安全，一个标识号只能被一个应用程序监听，因为如果小A程序和小B同时监听一个标识号，那就坏了，我传的数据都被AB接到，这样数据安全性就没办法保证了。

这个标识号就是端口，最初设计网络数据交换的设计者不知道是怎么想的。这是我的理解。

其实网卡都是被系统层封装了，端口和进程之间的关

系也是系统封装好的。我们只需要用socket就行，给定一个端口号就行了。其他的事都交给操作系统去做。

套接字（socket）是通信的基石，是支持TCP/IP协议的网络通信的基本操作单元。它是网络通信过程中端点的抽象表示，包含进行网络通信必须的五种信息：连接使用的协议，本地主机的IP地址，本地进程的协议端口，远地主机的IP地址，远地进程的协议端口。

26. 请说明TCP协议的流量控制和拥塞控制机制有什么不同？

拥塞控制：防止过多的数据注入到网络中，这样可以使网络中的路由器或链路不致过载。拥塞控制所要做的都有一个前提：网络能够承受现有的网络负荷。拥塞控制是一个全局性的过程，涉及到所有的主机、路由器，以及与降低网络传输性能有关的所有因素。

流量控制：指点对点通信量的控制，是端到端正的问题。流量控制所要做的就是抑制发送端发送数据的速率，以便使接收端来得及接收。

王道考研 p209

27. 请说明TCP协议与UDP协议有和不同之处。

下面我着重讲解一下TCP协议和UDP协议的区别。
TCP（Transmission Control Protocol，传输控制协议）是面向连接的协议，也就是说，在收发数据前，必须和对方建立可靠的连接。一个TCP连接必须要经过三次“对话”才能建立起来，其中的过程非常复杂，只简单的描述下这三次对话的简单过程：主机A向主机B发出连接请求数据包：“我想给你发数据，可以

吗？”，这是第一次对话；主机B向主机A发送同意连接和要求同步（同步就是两台主机一个在发送，一个在接收，协调工作）的数据包：“可以，你什么时候发？”，这是第二次对话；主机A再发出一个数据包确认主机B的要求同步：“我现在就发，你接着吧！”，这是第三次对话。三次“对话”的目的是使数据包的发送和接收同步，经过三次“对话”之后，主机A才向主机B正式发送数据。

详细点说就是：（文章部分转载<http://zhangjiangxing-gmail-com.iteye.com>，主要是这个人讲解得很到位，的确很容易使人理解！）

TCP三次握手过程

1 主机A通过向主机B 发送一个含有同步序列号的标志位的数据段给主机B ,向主机B 请求建立连接,通过这个数据段,

主机A告诉主机B 两件事:我想要和你通信;你可以用哪个序列号作为起始数据段来回应我.

2 主机B 收到主机A的请求后,用一个带有确认 应答 (ACK)和同步序列号(SYN)标志位的数据段响应主机A,也告诉主机A两件事:

我已经收到你的请求了,你可以传输数据了;你要用哪作序列号作为起始数据段来回应我

3 主机A收到这个数据段后,再发送一个确认应答,确认已收到主机B 的数据段:"我已收到回复,我现在要开始传输实际数据了

这样3次握手就完成了,主机A和主机B 就可以传输数据了.

3次握手的特点

没有应用层的数据

SYN这个标志位只有在TCP建产连接时才会被置1

握手完成后SYN标志位被置0

TCP建立连接要进行3次握手,而断开连接要进行4次

- 1 当主机A完成数据传输后,将控制位FIN置1,提出停止TCP连接的请求
- 2 主机B收到FIN后对其作出响应,确认这一方向上的TCP连接将关闭,将ACK置1
- 3 由B端再提出反方向的关闭请求,将FIN置1
- 4 主机A对主机B的请求进行确认,将ACK置1,双方向的关闭结束.

由TCP的三次握手和四次断开可以看出,TCP使用面向连接的通信方式,大大提高了数据通信的可靠性,使发送数据端

和接收端在数据正式传输前就有了交互,为数据正式传输打下了可靠的基础

名词解释

ACK TCP报头的控制位之一,对数据进行确认.确认由目的端发出,用它来告诉发送端这个序列号之前的数据段

都收到了.比如,确认号为X,则表示前X-1个数据段都收到了,只有当ACK=1时,确认号才有效,当ACK=0时,确认号无效,这时会要求重传数据,保证数据的完整性.

SYN 同步序列号,TCP建立连接时将这个位置1

FIN 发送端完成发送任务位,当TCP完成数据传输需要断开时,提出断开连接的一方将这位置1

TCP的包头结构:

源端口 16位

目标端口 16位

序列号 32位

回应序号 32位

TCP头长度 4位

reserved 6位

控制代码 6位

窗口大小 16位

偏移量 16位

校验和 16位

选项 32位(可选)

这样我们得出了TCP包头的最小长度，为20字节。

UDP (User Data Protocol, 用户数据报协议)

(1) UDP是一个非连接的协议，传输数据之前源端和终端不建立连接，当它想传送时就简单地去抓取来自应用程序的数据，并尽可能快地把它扔到网络上。在发送端，UDP传送数据的速度仅仅是受应用程序生成数据的速度、计算机的能力和传输带宽的限制；在接收端，UDP把每个消息段放在队列中，应用程序每次从队列中读一个消息段。

(2) 由于传输数据不建立连接，因此也就不需要维护连接状态，包括收发状态等，因此一台服务机可同时向多个客户机传输相同的消息。

(3) UDP信息包的标题很短，只有8个字节，相对于TCP的20个字节信息包的额外开销很小。

(4) 吞吐量不受拥挤控制算法的调节，只受应用软件生成数据的速率、传输带宽、源端和终端主机性能的限制。

(5) UDP使用尽最大努力交付，即不保证可靠交付，因此主机不需要维持复杂的链接状态表（这里面有许多参数）。

(6) UDP是面向报文的。发送方的UDP对应用程序交下来的报文，在添加首部后就向下交付给IP层。既不拆分，也不合并，而是保留这些报文的边界，因此，应用程序需要选择合适的报文大小。

我们经常使用“ping”命令来测试两台主机之间TCP/IP通信是否正常，其实“ping”命令的原理就是向对方主机发送UDP数据包，然后对方主机确认收到数据包，如果数据包是否到达的消息及时反馈回来，那么网络就是通的。

UDP的包头结构：

源端口 16位
目的端口 16位
长度 16位
校验和 16位

小结TCP与UDP的区别：

- 1.基于连接与无连接；
- 2.对系统资源的要求（TCP较多，UDP少）；
- 3.UDP程序结构较简单；
- 4.流模式与数据报模式；
- 5.TCP保证数据正确性，UDP可能丢包，TCP保证数据顺序，UDP不保证。

TCP（Transmission Control Protocol，传输控制协议）是基于连接的协议，也就是说，在正式收发数据前，必须和对方建立可靠的连接。一个TCP连接必须要经过三次“对话”才能建立起来，其中的过程非常复杂，我们这里只做简单、形象的介绍，你只要做到能够理解这个过程即可。我们来看看这三次对话的简单过程：主机A向主机B发出连接请求数据包：“我想给你发数据，可以吗？”，这是第一次对话；主机B向主机A发送同意连接和要求同步（同步就是两台主机一个在发送，一个在接收，协调工作）的数据包：“可以，你什么时候发？”，这是第二次对话；主机A再发出一个数据包确认主机B的要求同步：“我现在就发，你接着吧！”，这是第三次对话。三次“对话”的目的是使数据包的发送和接收同步，经过三次“对话”之后，主机A才向主机B正式发送数据。

UDP（User Data Protocol，用户数据报协议）是与TCP相对应的协议。它是面向非连接的协议，它不与对方建立连接，而是直接就把数据包发送过去！UDP适用于一次只传送少量数据、对可靠性要求不

高的应用环境。比如，我们经常使用“ping”命令来测试两台主机之间TCP/IP通信是否正常，其实“ping”命令的原理就是向对方主机发送UDP数据包，然后对方主机确认收到数据包，如果数据包是否到达的消息及时反馈回来，那么网络就是通的。例如，在默认状态下，一次“ping”操作发送4个数据包（如图2所示）。大家可以看到，发送的数据包数量是4包，收到的也是4包（因为对方主机收到后会发回一个确认收到的数据包）。这充分说明了UDP协议是面向非连接的协议，没有建立连接的过程。正因为UDP协议没有连接的过程，所以它的通信效果高；但也正因为如此，它的可靠性不如TCP协议高。QQ就使用UDP发消息，因此有时会出现收不到消息的情况。

tcp协议和udp协议的差别

TCP UDP

是否连接 面向连接 面向非连接

传输可靠性 可靠 不可靠

应用场合 传输大量数据 少量数据

速度 慢 快

TCP

UDP

相同点 TCP和UDP都处于网络层（NETWORK LAYER）之上，都是传输层协议，功能都属于保证网络层数据的传输。双方的通信无论是用TCP还是UDP都是要开放端口的。

不同点 1、TCP的传输是可靠的。 1、UDP的传输是不可靠的。

2、TCP（Transmission Control Protocol，传输控制协议）是基于连接的协议，也就是说，在正式收发数据前，必须和对方建立可靠的连接。

2、UDP（User Data Protocol，用户数据报协议）是与TCP相对应的协议。它是面向非连接的协议，它不与对方建立连接，而是直接就把数据包发送过去！

3、TCP是一种可靠的通信服务，负载相对而言 3、UDP是一种不可靠



比较大。TCP采用套接字 (socket) 或者端口 (port) 来建立通信。

4、TCP包括序号、确认信号、数据偏移、控制标志 (通常说的URG、ACK、PSH、RST、SYN、FIN)、窗口、校验和、紧急指针、选项等信息。

5、TCP提供超时重发, 丢弃重复数据, 检验数据, 流量控制等功能, 保证数据能从一端传到另一端。

6、TCP在发送数据包前都在通信双方有一个三次握手机制, 确保双方准备好, 在传输数据包期间, TCP会根据链路中数据流量的大小来调节传送的速率, 传输时如果发现丢包, 会有严格的重传机制, 故而传输速度很慢。

7、TCP支持全双工和并发的TCP连接, 提供确认、重传与拥塞控制。

的网络服务, 负载比较小。

4、UDP包含长度和校验和信息。

5、UDP不提供可靠性, 它只是把应用程序传给IP层的数据报发送出去, 但是并不能保证它们能到达目的地。

6、UDP在传输数据报前不用在客户和服务器之间建立一个连接, 且没有超时重发等机制, 故而传输速度很快。

7、UDP适用于哪些系统对性能的要求高于数据完整性的要求, 需要“简短快捷”的数据交换、需要多播和广播的应用环境

流量控制

28. 请说明NAT设备的作用, 并说明NAT设备的基本工作原理。

NAT 网络地址转换, 它是一种把内部私有网络地址 (IP 地址) 翻译成合法网络 IP 地址的技术。

1) 宽带共享, 解决 IP 地址匮乏问题

简单地说, NAT 就是在局域网内部网络中使用内部地址, 而当内部节点要与外部网络进行通讯时, 就在网关处, 将内部地址替换成公用地址, 从而在外部公网 (internet) 上正常使用,

NAT 可以使多台计算机共享 Internet 连接, 只申请一个合法 IP 地址, 就把整个局域网中的计算机接入 Internet 中。这一功能很好地解决了公共 IP 地址紧缺的问题。

2) 提供安全防护

NAT 屏蔽了内部网络，所有内部网计算机对于公共网络来说是不可见的。**内部地址**（在内部网络中分配给节点的有私有 IP 地址）**只能在内部网络中使用**，不能被路由转发，隐藏保护了内网的计算机。



29. 请详细描述从校园网的一台主机访问校外的新浪网

(www.sina.com.cn) 的这一过程中使用了哪些（计算机）网络协议？

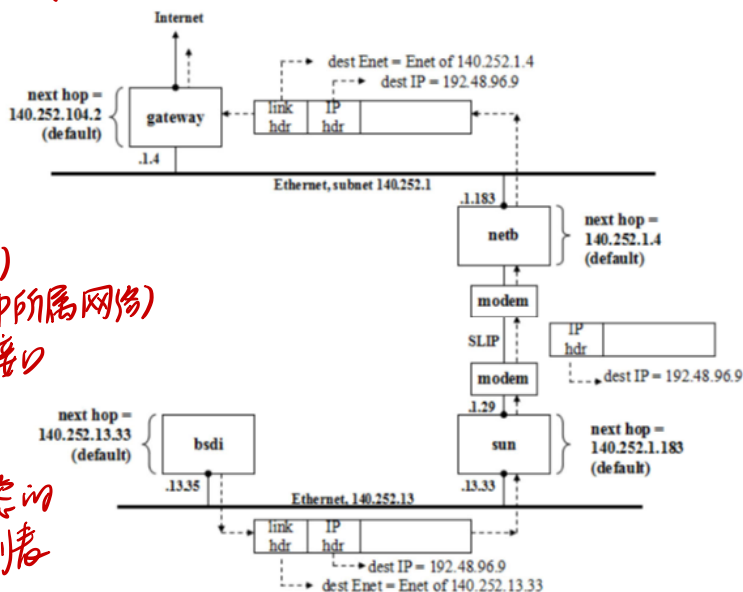


Figure 3.4 Initial path of datagram from bsdi to ftp.uu.net(192.48.96.9)

先来讲一下这个图：

(Gateway: 路由器，负责把子网内产生的到外网的数据包发送出去)

一上一下为两个子网，有两个主机 netb 和 sun，通过串口连接起来，距离长的有 Modem，在串口上的 IP 协议使用的是 SLIP 协议，这个是 Unix 系统的协议)

路由表中内容：
网络ID(目标)
子网掩码 (IP所属网络)
下一路地址 接口
Cost
路由的服务质量
路由中需要过滤的
出入 连接列表

上下两个子网通过串口连接，它们都有 IP 地址的前缀，下面的即是 140.252.13，上面的 IP 地址的前缀是 140.252.1，主机 bsdi 的地址是 [140.252.13.35](#)，sun 主机的 IP 地址是 [140.252.13.33](#)，两个口，一个是以太网，一个是串口，140.252.1.29 是上面的网地址

下面的发送 IP 包，目的地址填成 192.48.96.9，源地址是 140.252.13.35，这个包要从 gateway 发送出去到外网，就逆时针走大半个圆到 gateway，通过 3 台机器的转发。发出的 ARP 请求消息（数据链路层帧中）里包括 IP 地址和物理地址，所有计算机都能收到消息，IP 地址不吻合的对这个消息置之不理。

Bsdi 是通过查路由表知道数据包应该从 gateway 出去的（因为目的地址不是落在子网上），所以接收这个包的主机和 bsdi 不是直连的；所以下一跳地址应该是 sun，140.252.13.33，所以 bsdi 要构造数据链路层的帧，这个帧的目的 mac 地址是 sun 的 140.252.13.33 这个网卡的 mac 地址，得到下一跳路由器的 IP 地址后，而是通过 ARP 将 IP 地址转化成 MAC 地址，将其放到 Mac 帧首部，然后根据这个 Mac 地址找到下一跳路由器。这个工作是在数据链路层做的，不是网络层做的。

IP 包所对应的下一跳的路由器的 IP 地址，即 gateway 的 140.252.1.4，然后就发送给 gateway，如果有 NAT 设备，会将内网地址转为外网。内外网地址转换时，不光 IP 地址会变，Port 也会变化。

下面详细说明协议和协议过程：

这一请求过程应该涉及 DNS 协议（应用层），TCP 或 UDP 协议（传输层），ARP 协议，OSPF 协议和 BGP 协议（网络层），MAC 子层协议（数据链路层），以及物理层协议（物理层）。

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 域名和路径层，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IP；若没找到，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后则可以选择TCP或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协议是目标主机不在校园网内部，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，将消息包含主机IP和MAC地址，发送到源主机，其他主机则对该消息不做处理。

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机器。

30. 举例说明为什么会出现计算机网络协议？

计算机网络协议是有关计算机网络通信的一整套规则，或者说是为完成计算机网络通信而制订的规则、约定和标准。网络协议由语法、语义和时序三大要素组成。

关联性：上层向下层发
服务原语，而向下层
向对等实体发送PDU

31. 请说明协议数据单元 (PDU) , 服务原语 (Service Primitive) 的含义。

PDU: 协议数据单元 (Protocol Data Unit) 是指对等层次之间传递的数据单位。

服务原语: 用户和协议实体间的接口, 实际上是一段程序代码, 但其具有不可分割性。通过服务原语能实现服务用户和服务提供者间的交流, 与协议不同的是, 服务原语用于服务提供者与服务用户, 而协议是用于服务用户之间的通信。

32. 请说明回退N步的滑动窗口协议的基本工作原理。

当接收方检测出失序的信息帧后, 要求发送方重发最后一个正确接收的信息帧之后的所有未被确认的帧; 或者当发送方发送了N个帧后, 若发现该N帧的前一个帧在计时器超时后仍未返回其确认信息, 则该帧被判为出错或丢失, 此时发送方就不得不重新发送出错帧及其后的N帧。这就是GO-Back-N(退回N)法名称的由来。因为, 对接收方来说, 由于这一帧出错, 就不能以正常的序号向它的高层递交数据, 对其后发送来的N帧也可能都不能接收而丢弃。

33. 请说明在什么样的网络环境下需要使用MAC访问控制子层。

在使用广播信道的网络链路中, 例如LAN中, 特别是在无线局域网中, 因为无线本质上就是广播信道。

34. 以太网MAC地址有什么用?

一个以太网MAC地址唯一识别世界上的每一个

以太网设备。

35. 纠错编码与检错编码有什么不同？

检错：传输所接收的不正确信息，直到被正确接收。

纠错：从最初收到的可能不正确的比特中恢复正确信息。

36. 有哪几种复用技术？有哪几种调制解调技术？

复用：频分复用（FDM） — 载波带宽被划分为多种不同频带的子信道，每个子信道可以并行传送一路信号。FDM 用于模拟传输过程。

时分复用（TDM） — 在交互时间间隔内在同一信道上传送多路信号。TDM 广泛用于数字传输过程。

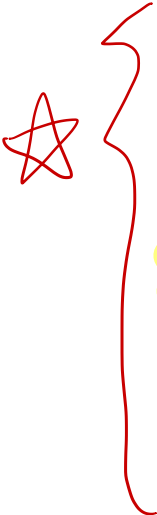
码分复用（CDM） — 每个信道作为编码信道实现位传输（特定脉冲序列）。这种编码传输方式通过传输唯一的时间系列短脉冲完成，但在较长的位时间中则采用时间片断替代。每个信道，都有各自的代码，并可以在同一光纤上进行传输以及异步解除复用。

波分复用（WDM） — 在一根光纤上使用不同波长同时传送多路光波信号。WDM 用于光纤信道。WDM与FDM 基于相同原理但它应用于光纤信道的光波传输过程。

调制解调技术：调制可分为两类：线性调制和非线性调制。线性调制包括调幅（AM）、抑制载波双边带调幅（DSB-SC）、单边带调幅（SSB）、残留边带调幅（VSB）等。非线性调幅的抗干扰性能较强，包括调频（FM）、移频键控（FSK）、移相键控（PSK）、差分移相键控（DPSK）等。线性调制特点是不改变信

号原始频谱结构，而非线性调制改变了信号原始频谱结构。根据调制的方式，调制可划分为连续调制和脉冲调制。按调制技术分，可分为模拟调制技术与数字调制技术，其主要区别是：模拟调制是对载波信号的某些参量进行连续调制，在接收端对载波信号的调制参量连续估值，而数字调制是用载波信号的某些离散状态来表征所传送信息，在接收端只对载波信号的离散调制参量进行检测。

37. 请说明以下命令的作用。



Ipconfig：显示当前的TCP/IP配置的设置值；
Route：显示，人工添加和修改路由表的项目；
Ping：用来确定网络的连通性。显示发送请求到返回应答之间的时间量，和TTL（时间生存）值，可以推算数据包通过了多少个路由器；
Traceroute：从你的计算机到互联网另一端的主机是走什么路径。
Netstat：了解网络当前的状态。显示活动的TCP连接，计算机倾听的端口，以太网统计信息，IP路由表，IPV4统计信息（对于IP,ICMP,TCP,UDP协议），以及IPV6统计信息（对于IPV6, ICMPV6,通过IPV6的TCP以及UDP协议）。使用时如果不带参数，netstat显示活动的TCP连接。

38. 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由差错控制功能。

1) 数据链路层的传输为点到点的，传输层协议控制传输为端到端的，因此，数据链路层的校验是保护一个穿过单条链路的帧，而数据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。即使每条链路校验和正确，该数据包仍可能被不正确的传递。

2) 数据链路层主要针对的是单一帧，或是字节本身的对错，而传输层是对总体控制，即对所有传输内容的总体控制，数据链路层的控制检测字节错误，但传输层检测传输的段正确到达否。



39. 连接套接字 (connected socket) 和监听套接字 (listening socket) 有什么区别？又有什么联系？

对于服务器编程中最重要的一步等待并接受客户的连接，那么这一步在编程中如何完成，`accept`函数就是完成这一步的。它从内核中取出已经建立的客户连接，然后把这个已经建立的连接返回给用户程序，此时用户程序就可以与自己的客户进行点到点的通信了。`accept`默认会阻塞进程，直到有一个客户连接建立后返回，它返回的是一个新可用的套接字，这个套接字是连接套接字。此时我们需要区分两种套接字，一种套接字正如`accept`的参数`sockfd`，它是监听套接字，在调用`listen`函数之后，一个套接字会从主动连接的套接字变身为一个监听套接字；而`accept`返回是一个连接套接字，它代表着一个网络已经存在的点点连接。自然要问的是：为什么要有两种套接字？原因很简单，如果使用一个描述字的话，那么它的功能太多，使得使用

很不直观，同时在内核确实产生了一个这样的新的描述字。

40. TCP连接的初始化序号

(ISN: Initial Sequence Number) 有什么用?

(注意双方交换序列号的问题) —— 判断包是否属于这个连接

① 客户端向服务器发送一个同步数据包请求建立连接，该数据包中，初始序列号

(ISN) 是客户端随机产生的一个值，确认号是0；② 服务器收到这个同步请求数据包

后，会对客户端进行一个同步确认。这个数据包中，序列号 (ISN) 是服务器随机产生的一个值，确认号是客户端的初始序列号+1；③ 客户端收到这个同步确认数据包

后，再对服务器进行一个确认。该数据包中，序列号是上一个同步请求数据包中的确认号值，确认号是服务器的初始序列号+1。

初始序列号 (ISN) 随时间而变化的，而且不同的操作系统也会有不同的实现方式，所以每个连接的初始序列号是不同的。

初始序列号 (ISN) 随时间而变化的，而且不同的操作系统也会有不同的实现方式，所以每个连接的初始序列号是不同的。

(38题重了，
38题靠谱)

41. 数据链路层协议的差错控制和传输层协议的差错控制有什么区别？

【1】从“干什么”的角度来讲
数据链路层负责结点之间链路的事情。把有比特查错的物理信道变成无比特差错的数据链路。

运输层负责应用进程之间端到端的事情。
就两项任务：差错管理+业务复用。

【2】从“服务”的角度来讲
当然是为上一层服务啦！
数据链路层将源机网络层来的数据可靠地