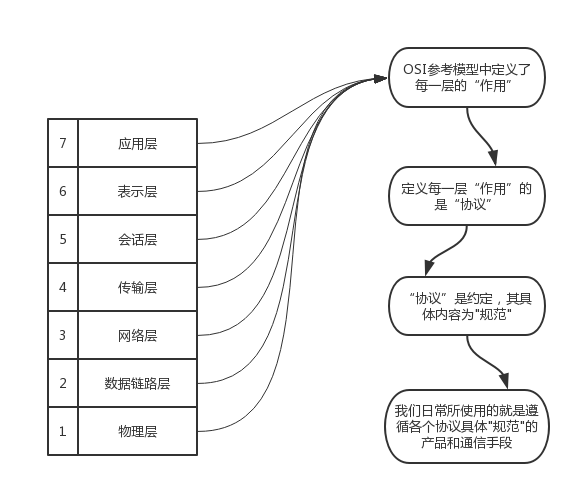
**计算机网络**

# 计算机网络体系结构



计算机网络体系结构分层



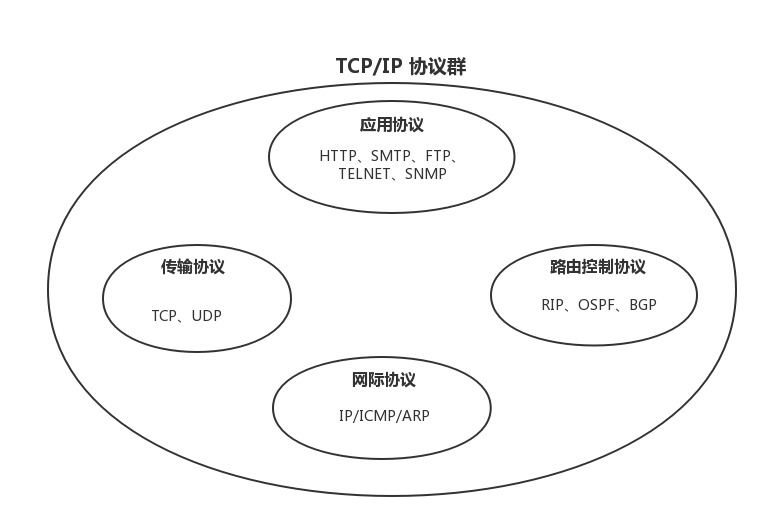
计算机网络体系结构分层

不难看出，TCP/IP 与 OSI 在分层模块上稍有区别。OSI 参考模型注重“通信协议必要的功能是什么”，而 TCP/IP 则更强调“在计算机上实现协议应该开发哪种程序”。

# TCP/IP 基础

## TCP/IP 的具体含义

从字面意义上讲，有人可能会认为 TCP/IP 是指 TCP 和 IP 两种协议。实际生活当中有时也确实就是指这两种协议。然而在很多情况下，它只是利用 IP 进行通信时所必须用到的协议群的统称。具体来说，IP或ICMP、TCP 或 UDP、TELNET 或 FTP、以及 HTTP 等都属于 TCP/IP 协议。他们与 TCP 或 IP 的关系紧密，是互联网必不可少的组成部分。TCP/IP 一词泛指这些协议，因此，有时也称 TCP/IP 为网际协议群。  
互联网进行通信时，需要相应的网络协议，TCP/IP 原本就是为使用互联网而开发制定的协议族。因此，互联网的协议就是 TCP/IP，TCP/IP 就是互联网的协议。



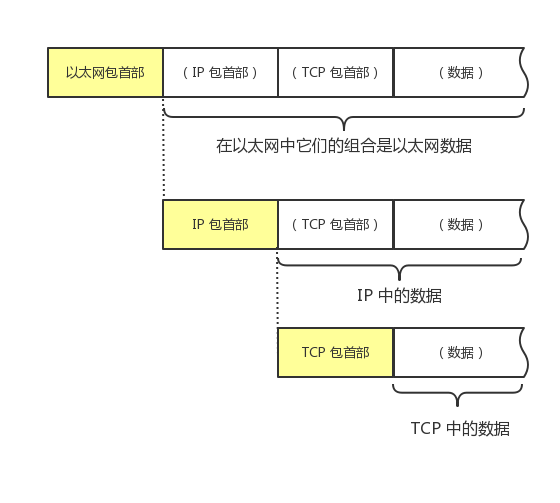
网际协议群

## 数据包

包、帧、数据包、段、消息  
以上五个术语都用来表述数据的单位，大致区分如下：

1. 包可以说是全能性术语；
2. 帧用于表示数据链路层中包的单位；
3. 数据包是 IP 和 UDP 等网络层以上的分层中包的单位；
4. 段则表示 TCP 数据流中的信息；
5. 消息是指应用协议中数据的单位。

每个分层中，都会对所发送的数据附加一个首部，在这个首部中包含了该层必要的信息，如发送的目标地址以及协议相关信息。通常，为协议提供的信息为包首部，所要发送的内容为数据。在下一层的角度看，从上一层收到的包全部都被认为是本层的数据。

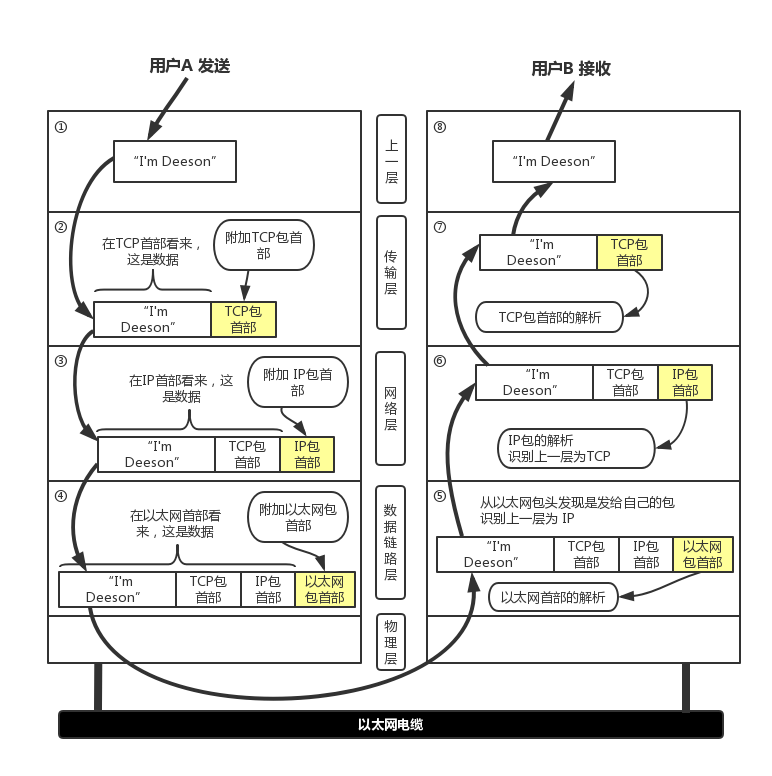


数据包首部

网络中传输的数据包由两部分组成：一部分是协议所要用到的首部，另一部分是上一层传过来的数据。首部的结构由协议的具体规范详细定义。在数据包的首部，明确标明了协议应该如何读取数据。反过来说，看到首部，也就能够了解该协议必要的信息以及所要处理的数据。包首部就像协议的脸。

## 数据处理流程

下图以用户 a 向用户 b 发送邮件为例子：



数据处理流程

1. 应用程序处理  
    首先应用程序会进行编码处理，这些编码相当于 OSI 的表示层功能；  
   编码转化后，邮件不一定马上被发送出去，这种何时建立通信连接何时发送数据的管理功能，相当于 OSI 的会话层功能。
2. TCP 模块的处理  
    TCP 根据应用的指示，负责建立连接、发送数据以及断开连接。TCP 提供将应用层发来的数据顺利发送至对端的可靠传输。为了实现这一功能，需要在应用层数据的前端附加一个 TCP 首部。
3. IP 模块的处理  
    IP 将 TCP 传过来的 TCP 首部和 TCP 数据合起来当做自己的数据，并在 TCP 首部的前端加上自己的 IP 首部。IP 包生成后，参考路由控制表决定接受此 IP 包的路由或主机。
4. 网络接口（以太网驱动）的处理  
    从 IP 传过来的 IP 包对于以太网来说就是数据。给这些数据附加上以太网首部并进行发送处理，生成的以太网数据包将通过物理层传输给接收端。
5. 网络接口（以太网驱动）的处理  
    主机收到以太网包后，首先从以太网包首部找到 MAC 地址判断是否为发送给自己的包，若不是则丢弃数据。

如果是发送给自己的包，则从以太网包首部中的类型确定数据类型，再传给相应的模块，如 IP、ARP 等。这里的例子则是 IP 。

1. IP 模块的处理  
    IP 模块接收到 数据后也做类似的处理。从包首部中判断此 IP 地址是否与自己的 IP 地址匹配，如果匹配则根据首部的协议类型将数据发送给对应的模块，如 TCP、UDP。这里的例子则是 TCP。  
   另外吗，对于有路由器的情况，接收端地址往往不是自己的地址，此时，需要借助路由控制表，在调查应该送往的主机或路由器之后再进行转发数据。
2. TCP 模块的处理  
    在 TCP 模块中，首先会计算一下校验和，判断数据是否被破坏。然后检查是否在按照序号接收数据。最后检查端口号，确定具体的应用程序。数据被完整地接收以后，会传给由端口号识别的应用程序。
3. 应用程序的处理  
    接收端应用程序会直接接收发送端发送的数据。通过解析数据，展示相应的内容。

# 传输层中的 TCP 和 UDP

TCP/IP 中有两个具有代表性的传输层协议，分别是 TCP 和 UDP。

TCP 是面向连接的、可靠的流协议。流就是指不间断的数据结构，当应用程序采用 TCP 发送消息时，虽然可以保证发送的顺序，但还是犹如没有任何间隔的数据流发送给接收端。TCP 为提供可靠性传输，实行“顺序控制”或“重发控制”机制。此外还具备“流控制（流量控制）”、“拥塞控制”、提高网络利用率等众多功能。

UDP 是不具有可靠性的数据报协议。细微的处理它会交给上层的应用去完成。在 UDP 的情况下，虽然可以确保发送消息的大小，却不能保证消息一定会到达。因此，应用有时会根据自己的需要进行重发处理。

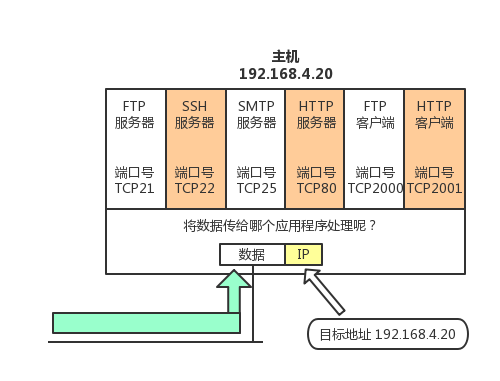
TCP 和 UDP 的优缺点无法简单地、绝对地去做比较：TCP 用于在传输层有必要实现可靠传输的情况；而在一方面，UDP 主要用于那些对高速传输和实时性有较高要求的通信或广播通信。TCP 和 UDP 应该根据应用的目的按需使用。

## 端口号

数据链路和 IP 中的地址，分别指的是 MAC 地址和 IP 地址。前者用来识别同一链路中不同的计算机，后者用来识别 TCP/IP 网络中互连的主机和路由器。在传输层也有这种类似于地址的概念，那就是端口号。端口号用来识别同一台计算机中进行通信的不同应用程序。因此，它也被称为程序地址。

### 根据端口号识别应用

一台计算机上同时可以运行多个程序。传输层协议正是利用这些端口号识别本机中正在进行通信的应用程序，并准确地将数据传输。



通过端口号识别应用

### 通过IP地址、端口号、协议号进行通信识别

仅凭目标端口号识别某一个通信是远远不够的。

通过端口号、IP地址、协议号进行通信识别

① 和② 的通信是在两台计算机上进行的。它们的目标端口号相同，都是80。这里可以根据源端口号加以区分。

③ 和 ① 的目标端口号和源端口号完全相同，但它们各自的源 IP 地址不同。

此外，当 IP 地址和端口号全都一样时，我们还可以通过协议号来区分（TCP 和 UDP）。

### 端口号的确定

标准既定的端口号：这种方法也叫静态方法。它是指每个应用程序都有其指定的端口号。但并不是说可以随意使用任何一个端口号。例如 HTTP、FTP、TELNET 等广为使用的应用协议中所使用的端口号就是固定的。这些端口号被称为知名端口号，分布在 0~1023 之间；除知名端口号之外，还有一些端口号被正式注册，它们分布在 1024~49151 之间，不过这些端口号可用于任何通信用途。

时序分配法：服务器有必要确定监听端口号，但是接受服务的客户端没必要确定端口号。在这种方法下，客户端应用程序完全可以不用自己设置端口号，而全权交给操作系统进行分配。动态分配的端口号范围在 49152~65535 之间。

### 端口号与协议

端口号由其使用的传输层协议决定。因此，不同的传输层协议可以使用相同的端口号。

此外，那些知名端口号与传输层协议并无关系。只要端口一致都将分配同一种应用程序进行处理。

## UDP

UDP 不提供复杂的控制机制，利用 IP 提供面向无连接的通信服务。

并且它是将应用程序发来的数据在收到的那一刻，立即按照原样发送到网络上的一种机制。即使是出现网络拥堵的情况，UDP 也无法进行流量控制等避免网络拥塞行为。

此外，传输途中出现丢包，UDP 也不负责重发。

甚至当包的到达顺序出现乱序时也没有纠正的功能。

如果需要以上的细节控制，不得不交由采用 UDP 的应用程序去处理。

UDP 常用于一下几个方面：1.包总量较少的通信（DNS、SNMP等）；2.视频、音频等多媒体通信（即时通信）；3.限定于 LAN 等特定网络中的应用通信；4.广播通信（广播、多播）。

## TCP

TCP 与 UDP 的区别相当大。它充分地实现了数据传输时各种控制功能，可以进行丢包时的重发控制，还可以对次序乱掉的分包进行顺序控制。而这些在 UDP 中都没有。

此外，TCP 作为一种面向有连接的协议，只有在确认通信对端存在时才会发送数据，从而可以控制通信流量的浪费。

根据 TCP 的这些机制，在 IP 这种无连接的网络上也能够实现高可靠性的通信（ 主要通过检验和、序列号、确认应答、重发控制、连接管理以及窗口控制等机制实现）。

### 三次握手（重点）

TCP 提供面向有连接的通信传输。面向有连接是指在数据通信开始之前先做好两端之间的准备工作。

所谓三次握手是指建立一个 TCP 连接时需要客户端和服务器端总共发送三个包以确认连接的建立。在socket编程中，这一过程由客户端执行connect来触发。

下面来看看三次握手的流程图：



三次握手

第一次握手：客户端将标志位SYN置为1，随机产生一个值seq=J，并将该数据包发送给服务器端，客户端进入SYN\_SENT状态，等待服务器端确认。

第二次握手：服务器端收到数据包后由标志位SYN=1知道客户端请求建立连接，服务器端将标志位SYN和ACK都置为1，ack=J+1，随机产生一个值seq=K，并将该数据包发送给客户端以确认连接请求，服务器端进入SYN\_RCVD状态。

第三次握手：客户端收到确认后，检查ack是否为J+1，ACK是否为1，如果正确则将标志位ACK置为1，ack=K+1，并将该数据包发送给服务器端，服务器端检查ack是否为K+1，ACK是否为1，如果正确则连接建立成功，客户端和服务器端进入ESTABLISHED状态，完成三次握手，随后客户端与服务器端之间可以开始传输数据了。

### 四次挥手（重点）

四次挥手即终止TCP连接，就是指断开一个TCP连接时，需要客户端和服务端总共发送4个包以确认连接的断开。在socket编程中，这一过程由客户端或服务端任一方执行close来触发。

由于TCP连接是全双工的，因此，每个方向都必须要单独进行关闭，这一原则是当一方完成数据发送任务后，发送一个FIN来终止这一方向的连接，收到一个FIN只是意味着这一方向上没有数据流动了，即不会再收到数据了，但是在这个TCP连接上仍然能够发送数据，直到这一方向也发送了FIN。首先进行关闭的一方将执行主动关闭，而另一方则执行被动关闭。

下面来看看四次挥手的流程图：



四次挥手

中断连接端可以是客户端，也可以是服务器端。

第一次挥手：客户端发送一个FIN=M，用来关闭客户端到服务器端的数据传送，客户端进入FIN\_WAIT\_1状态。意思是说"我客户端没有数据要发给你了"，但是如果你服务器端还有数据没有发送完成，则不必急着关闭连接，可以继续发送数据。

第二次挥手：服务器端收到FIN后，先发送ack=M+1，告诉客户端，你的请求我收到了，但是我还没准备好，请继续你等我的消息。这个时候客户端就进入FIN\_WAIT\_2 状态，继续等待服务器端的FIN报文。

第三次挥手：当服务器端确定数据已发送完成，则向客户端发送FIN=N报文，告诉客户端，好了，我这边数据发完了，准备好关闭连接了。服务器端进入LAST\_ACK状态。

第四次挥手：客户端收到FIN=N报文后，就知道可以关闭连接了，但是他还是不相信网络，怕服务器端不知道要关闭，所以发送ack=N+1后进入TIME\_WAIT状态，如果Server端没有收到ACK则可以重传。服务器端收到ACK后，就知道可以断开连接了。客户端等待了2MSL后依然没有收到回复，则证明服务器端已正常关闭，那好，我客户端也可以关闭连接了。最终完成了四次握手。

上面是一方主动关闭，另一方被动关闭的情况，实际中还会出现同时发起主动关闭的情况，  
具体流程如下图：



同时挥手

### 通过序列号与确认应答提高可靠性

在 TCP 中，当发送端的数据到达接收主机时，接收端主机会返回一个已收到消息的通知。这个消息叫做确认应答（ACK）。当发送端将数据发出之后会等待对端的确认应答。如果有确认应答，说明数据已经成功到达对端。反之，则数据丢失的可能性很大。

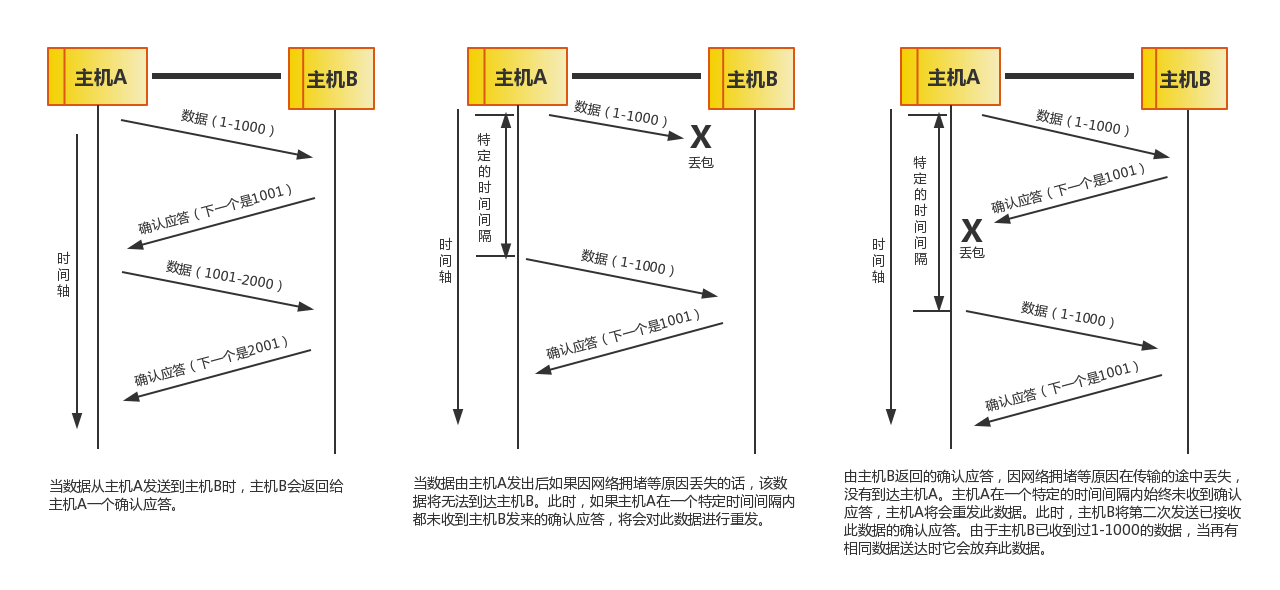
在一定时间内没有等待到确认应答，发送端就可以认为数据已经丢失，并进行重发。由此，即使产生了丢包，仍然能够保证数据能够到达对端，实现可靠传输。

未收到确认应答并不意味着数据一定丢失。也有可能是数据对方已经收到，只是返回的确认应答在途中丢失。这种情况也会导致发送端误以为数据没有到达目的地而重发数据。

此外，也有可能因为一些其他原因导致确认应答延迟到达，在源主机重发数据以后才到达的情况也屡见不鲜。此时，源主机只要按照机制重发数据即可。

对于目标主机来说，反复收到相同的数据是不可取的。为了对上层应用提供可靠的传输，目标主机必须放弃重复的数据包。为此我们引入了序列号。

序列号是按照顺序给发送数据的每一个字节（8位字节）都标上号码的编号。接收端查询接收数据 TCP 首部中的序列号和数据的长度，将自己下一步应该接收的序列号作为确认应答返送回去。通过序列号和确认应答号，TCP 能够识别是否已经接收数据，又能够判断是否需要接收，从而实现可靠传输。



序列号和确认应答

### 重发超时的确定

重发超时是指在重发数据之前，等待确认应答到来的那个特定时间间隔。如果超过这个时间仍未收到确认应答，发送端将进行数据重发。最理想的是，找到一个最小时间，它能保证“确认应答一定能在这个时间内返回”。

TCP 要求不论处在何种网络环境下都要提供高性能通信，并且无论网络拥堵情况发生何种变化，都必须保持这一特性。为此，它在每次发包时都会计算往返时间及其偏差。将这个往返时间和偏差时间相加，重发超时的时间就是比这个总和要稍大一点的值。

在 BSD 的 Unix 以及 Windows 系统中，超时都以0.5秒为单位进行控制，因此重发超时都是0.5秒的整数倍。不过，最初其重发超时的默认值一般设置为6秒左右。

数据被重发之后若还是收不到确认应答，则进行再次发送。此时，等待确认应答的时间将会以2倍、4倍的指数函数延长。

此外，数据也不会被无限、反复地重发。达到一定重发次数之后，如果仍没有任何确认应答返回，就会判断为网络或对端主机发生了异常，强制关闭连接。并且通知应用通信异常强行终止。

### 以段为单位发送数据

在建立 TCP 连接的同时，也可以确定发送数据包的单位，我们也可以称其为“最大消息长度”（MSS）。最理想的情况是，最大消息长度正好是 IP 中不会被分片处理的最大数据长度。

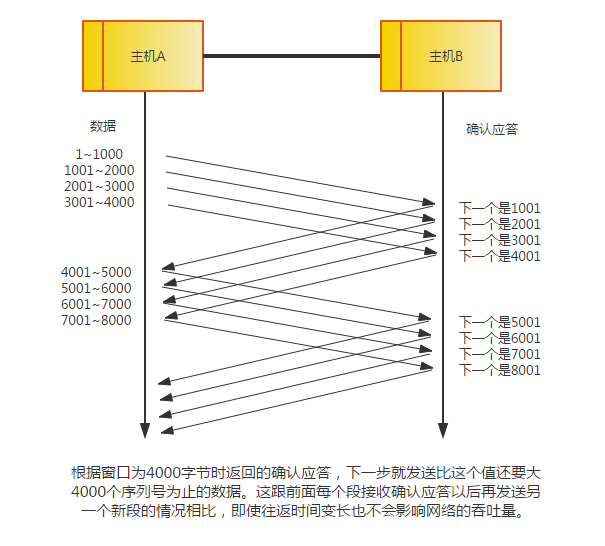
TCP 在传送大量数据时，是以 MSS 的大小将数据进行分割发送。进行重发时也是以 MSS 为单位。

MSS 在三次握手的时候，在两端主机之间被计算得出。两端的主机在发出建立连接的请求时，会在 TCP 首部中写入 MSS 选项，告诉对方自己的接口能够适应的 MSS 的大小。然后会在两者之间选择一个较小的值投入使用。

### 利用窗口控制提高速度

TCP 以1个段为单位，每发送一个段进行一次确认应答的处理。这样的传输方式有一个缺点，就是包的往返时间越长通信性能就越低。

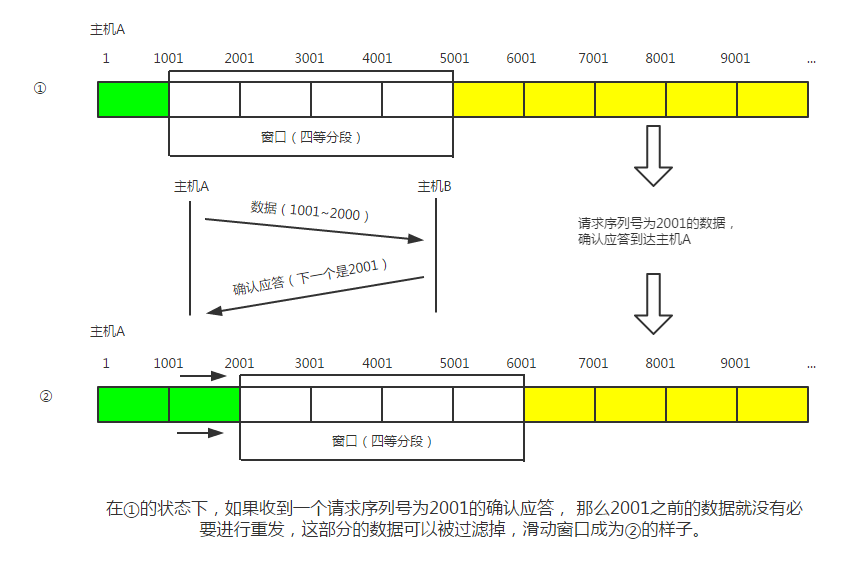
为解决这个问题，TCP 引入了窗口这个概念。确认应答不再是以每个分段，而是以更大的单位进行确认，转发时间将会被大幅地缩短。也就是说，发送端主机，在发送了一个段以后不必要一直等待确认应答，而是继续发送。如下图所示：



窗口控制

窗口大小就是指无需等待确认应答而可以继续发送数据的最大值。上图中窗口大小为4个段。这个机制实现了使用大量的缓冲区，通过对多个段同时进行确认应答的功能。

### 滑动窗口控



滑动窗口

上图中的窗口内的数据即便没有收到确认应答也可以被发送出去。不过，在整个窗口的确认应答没有到达之前，如果其中部分数据出现丢包，那么发送端仍然要负责重传。为此，发送端主机需要设置缓存保留这些待被重传的数据，直到收到他们的确认应答。

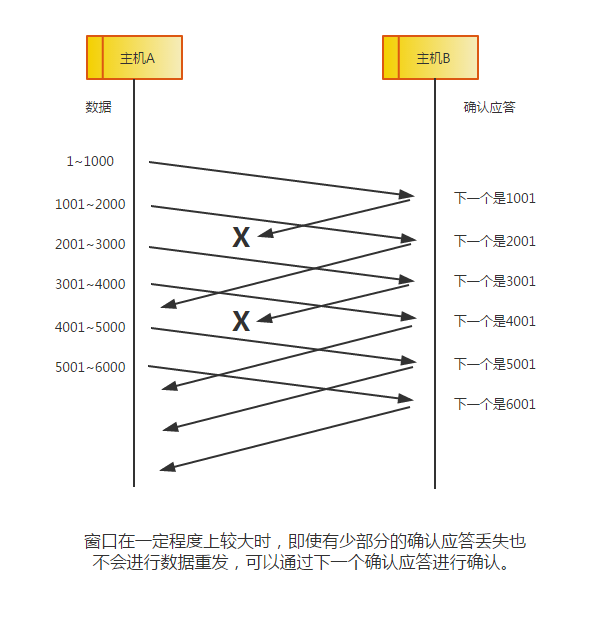
在滑动窗口以外的部分包括未发送的数据以及已经确认对端已收到的数据。当数据发出后若如期收到确认应答就可以不用再进行重发，此时数据就可以从缓存区清除。

收到确认应答的情况下，将窗口滑动到确认应答中的序列号的位置。这样可以顺序地将多个段同时发送提高通信性能。这种机制也别称为滑动窗口控制。

### 窗口控制中的重发控制

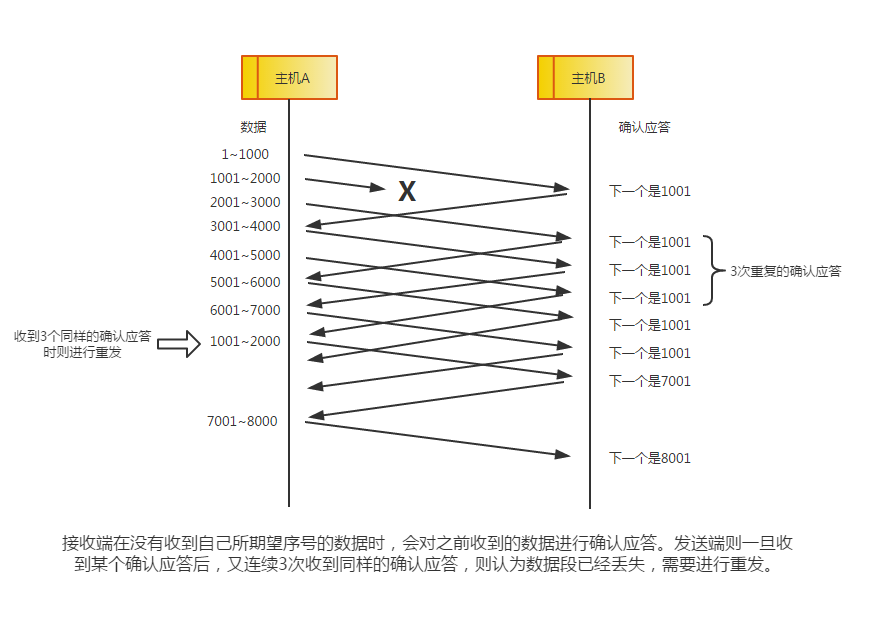
在使用窗口控制中， 出现丢包一般分为两种情况：

① 确认应答未能返回的情况。在这种情况下，数据已经到达对端，是不需要再进行重发的，如下图：



部分确认应答丢失

② 某个报文段丢失的情况。接收主机如果收到一个自己应该接收的序列号以外的数据时，会针对当前为止收到数据返回确认应答。如下图所示，当某一报文段丢失后，发送端会一直收到序号为1001的确认应答，因此，在窗口比较大，又出现报文段丢失的情况下，同一个序列号的确认应答将会被重复不断地返回。而发送端主机如果连续3次收到同一个确认应答，就会将其对应的数据进行重发。这种机制比之前提到的超时管理更加高效，因此也被称为高速重发控制。



高速重发控制

# 网络层中的 IP 协议

IP（IPv4、IPv6）相当于 OSI 参考模型中的第3层——网络层。网络层的主要作用是“实现终端节点之间的通信”。这种终端节点之间的通信也叫“点对点通信”。

网络的下一层——数据链路层的主要作用是在互连同一种数据链路的节点之间进行包传递。而一旦跨越多种数据链路，就需要借助网络层。网络层可以跨越不同的数据链路，即使是在不同的数据链路上也能实现两端节点之间的数据包传输。

IP 大致分为三大作用模块，它们是 IP 寻址、路由（最终节点为止的转发）以及 IP 分包与组包。

## IP 地址

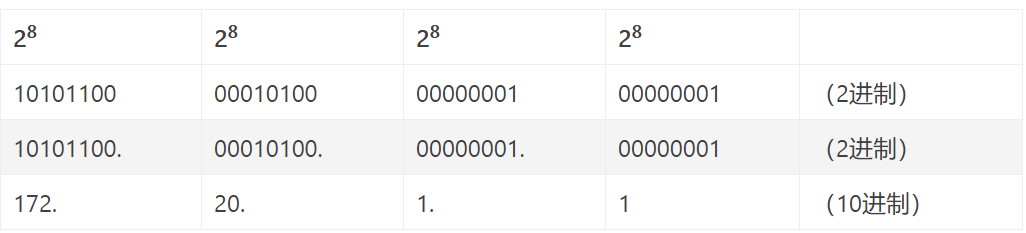
### IP 地址概述

在计算机通信中，为了识别通信对端，必须要有一个类似于地址的识别码进行标识。在数据链路中的 MAC 地址正是用来标识同一个链路中不同计算机的一种识别码。

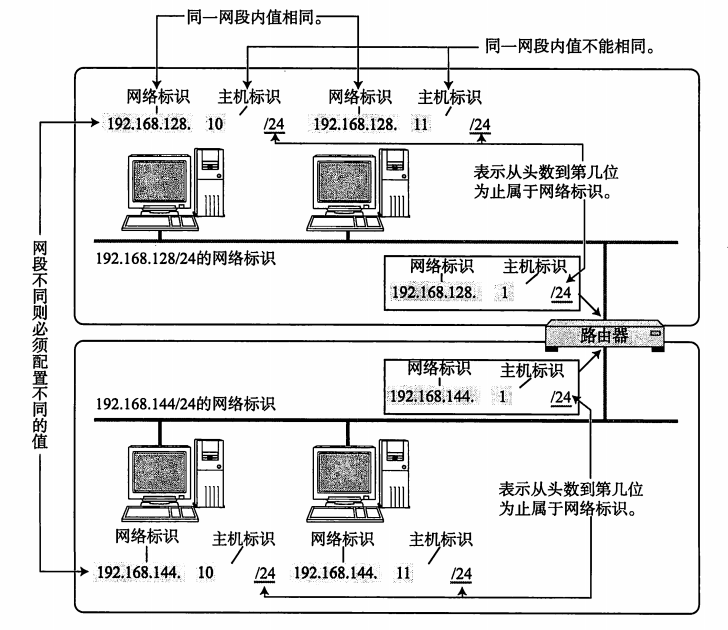
作为网络层的 IP ,也有这种地址信息，一般叫做 IP 地址。IP 地址用于在“连接到网络中的所有主机中识别出进行通信的目标地址”。因此，在 TCP/IP 通信中所有主机或路由器必须设定自己的 IP 地址。

不论一台主机与哪种数据链路连接，其 IP 地址的形式都保持不变。

IP 地址（IPv4 地址）由32位正整数来表示。IP 地址在计算机内部以二进制方式被处理。然而，由于我们并不习惯于采用二进制方式，我们将32位的 IP 地址以每8位为一组，分成4组，每组以 “.” 隔开，再将每组数转换成十进制数。如下：

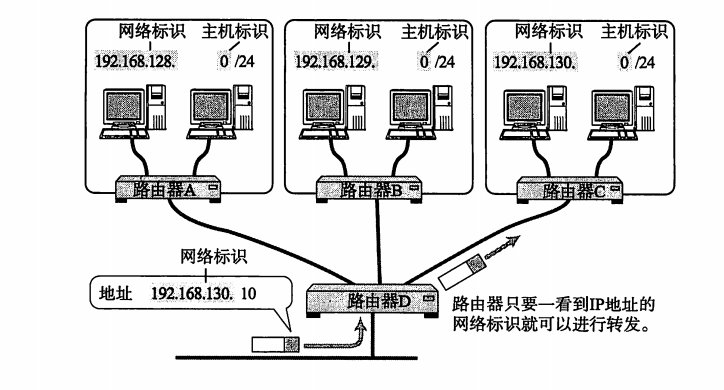


### IP 地址由网络和主机两部分标识组成

如下图，网络标识在数据链路的每个段配置不同的值。网络标识必须保证相互连接的每个段的地址不相重复。而相同段内相连的主机必须有相同的网络地址。IP 地址的“主机标识”则不允许在同一个网段内重复出现。由此，可以通过设置网络地址和主机地址，在相互连接的整个网络中保证每台主机的 IP 地址都不会相互重叠。即 IP 地址具有了唯一性。

IP地址的主机标识

如下图，IP 包被转发到途中某个路由器时，正是利用目标 IP 地址的网络标识进行路由。因为即使不看主机标识，只要一见到网络标识就能判断出是否为该网段内的主机。



IP地址的网络标识

### IP 地址的分类

IP 地址分为四个级别，分别为A类、B类、C类、D类。它根据 IP 地址中从第 1 位到第 4 位的比特列对其网络标识和主机标识进行区分。

A 类 IP 地址是首位以 “0” 开头的地址。从第 1 位到第 8 位是它的网络标识。用十进制表示的话，0.0.0.0~127.0.0.0 是 A 类的网络地址。A 类地址的后 24 位相当于主机标识。因此，一个网段内可容纳的主机地址上限为16,777,214个。

B 类 IP 地址是前两位 “10” 的地址。从第 1 位到第 16 位是它的网络标识。用十进制表示的话，128.0.0.0~191.255.0.0 是 B 类的网络地址。B 类地址的后 16 位相当于主机标识。因此，一个网段内可容纳的主机地址上限为65,534个。

C 类 IP 地址是前三位为 “110” 的地址。从第 1 位到第 24 位是它的网络标识。用十进制表示的话，192.0.0.0~223.255.255.0 是 C 类的网络地址。C 类地址的后 8 位相当于主机标识。因此，一个网段内可容纳的主机地址上限为254个。

D 类 IP 地址是前四位为 “1110” 的地址。从第 1 位到第 32 位是它的网络标识。用十进制表示的话，224.0.0.0~239.255.255.255 是 D 类的网络地址。D 类地址没有主机标识，常用于多播。

在分配 IP 地址时关于主机标识有一点需要注意。即要用比特位表示主机地址时，不可以全部为 0 或全部为 1。因为全部为 0 只有在表示对应的网络地址或 IP 地址不可以获知的情况下才使用。而全部为 1 的主机通常作为广播地址。因此，在分配过程中，应该去掉这两种情况。这也是为什么 C 类地址每个网段最多只能有 254（ 28 - 2 = 254）个主机地址的原因。

### 广播地址

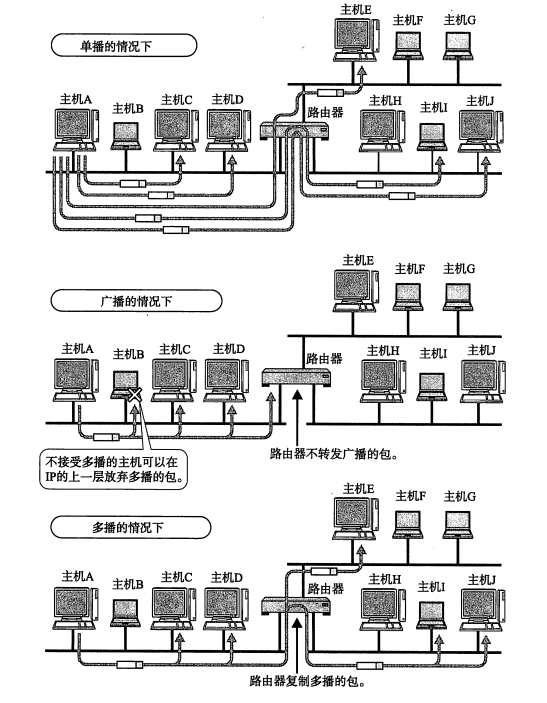
广播地址用于在同一个链路中相互连接的主机之间发送数据包。将 IP 地址中的主机地址部分全部设置为 1，就成了广播地址。

广播分为本地广播和直接广播两种。在本网络内的广播叫做本地广播；在不同网络之间的广播叫做直接广播。

### IP 多播

多播用于将包发送给特定组内的所有主机。由于其直接使用 IP 地址，因此也不存在可靠传输。

相比于广播，多播既可以穿透路由器，又可以实现只给那些必要的组发送数据包。请看下图：



IP 多播

多播使用 D 类地址。因此，如果从首位开始到第 4 位是 “1110”，就可以认为是多播地址。而剩下的 28 位可以成为多播的组编号。

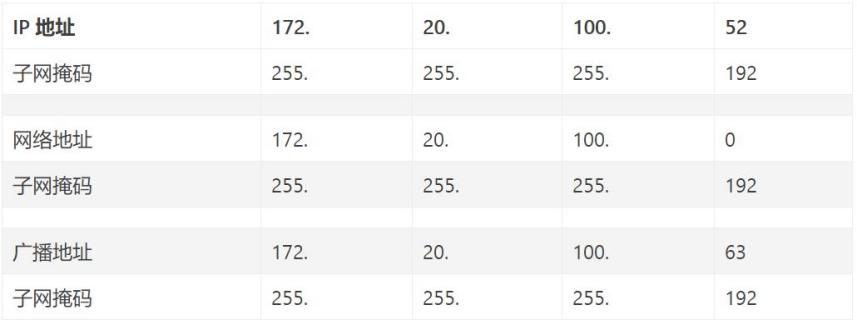
此外， 对于多播，所有的主机（路由器以外的主机和终端主机）必须属于 224.0.0.1 的组，所有的路由器必须属于 224.0.0.2 的组。

### 子网掩码

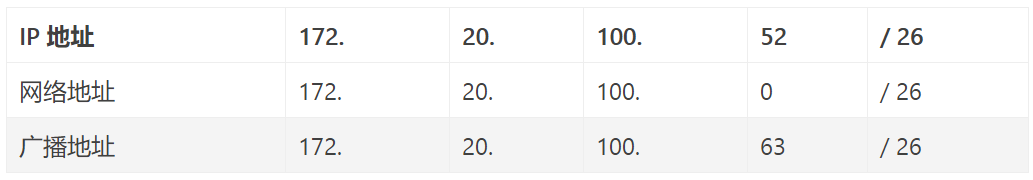
现在一个 IP 地址的网络标识和主机标识已不再受限于该地址的类别，而是由一个叫做“子网掩码”的识别码通过子网网络地址细分出比 A 类、B 类、C 类更小粒度的网络。这种方式实际上就是将原来 A 类、B 类、C 类等分类中的主机地址部分用作子网地址，可以将原网络分为多个物理网络的一种机制。

子网掩码用二进制方式表示的话，也是一个 32 位的数字。它对应 IP 地址网络标识部分的位全部为 “1”，对应 IP 地址主机标识的部分则全部为 “0”。由此，一个 IP 地址可以不再受限于自己的类别，而是可以用这样的子网掩码自由地定位自己的网络标识长度。当然，子网掩码必须是 IP 地址的首位开始连续的 “1”。

对于子网掩码，目前有两种表示方式。第一种是，将 IP 地址与子网掩码的地址分别用两行来表示。以 172.20.100.52 的前 26 位是网络地址的情况为例，如下：



第二种表示方式是，在每个 IP 地址后面追加网络地址的位数用 “/ ” 隔开，如下：



另外，在第二种方式下记述网络地址时可以省略后面的 “0” 。例如：172.20.0.0/26 跟 172.20/26 其实是一个意思。

## 路由

发送数据包时所使用的地址是网络层的地址，即 IP 地址。然而仅仅有 IP 地址还不足以实现将数据包发送到对端目标地址，在数据发送过程中还需要类似于“指明路由器或主机”的信息，以便真正发往目标地址。保存这种信息的就是路由控制表。

该路由控制表的形成方式有两种：一种是管理员手动设置，另一种是路由器与其他路由器相互交换信息时自动刷新。前者也叫做静态路由控制，而后者叫做动态路由控制。

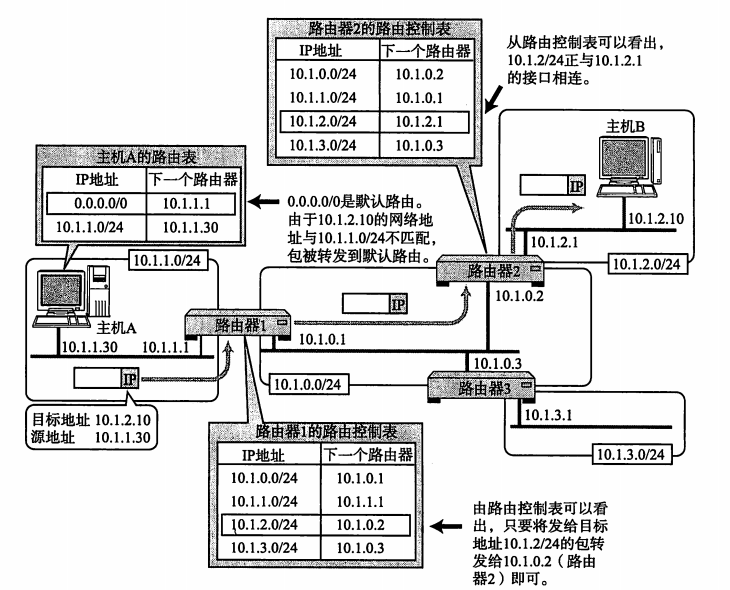
IP 协议始终认为路由表是正确的。然后，IP 本身并没有定义制作路由控制表的协议。即 IP 没有制作路由控制表的机制。该表示由一个叫做“路由协议”的协议制作而成。

### IP 地址与路由控制

IP 地址的网络地址部分用于进行路由控制。

路由控制表中记录着网络地址与下一步应该发送至路由器的地址。

在发送 IP 包时，首先要确定 IP 包首部中的目标地址，再从路由控制表中找到与该地址具有相同网络地址的记录，根据该记录将 IP 包转发给相应的下一个路由器。如果路由控制表中存在多条相同网络地址的记录，就选择一个最为吻合的网络地址。



路由控制表与 IP 包发送

## IP 分包与组包

每种数据链路的最大传输单元（MTU）都不尽相同，因为每个不同类型的数据链路的使用目的不同。使用目的不同，可承载的 MTU 也就不同。

任何一台主机都有必要对 IP 分片进行相应的处理。分片往往在网络上遇到比较大的报文无法一下子发送出去时才会进行处理。

经过分片之后的 IP 数据报在被重组的时候，只能由目标主机进行。路由器虽然做分片但不会进行重组。

3.1 路径 MTU 发现

分片机制也有它的不足。如路由器的处理负荷加重之类。因此，只要允许，是不希望由路由器进行 IP 数据包的分片处理的。

为了应对分片机制的不足，“路径 MTU 发现” 技术应运而生。路径 MTU 指的是，从发送端主机到接收端主机之间不需要分片是最大 MTU 的大小。即路径中存在的所有数据链路中最小的 MTU 。

进行路径 MTU 发现，就可以避免在中途的路由器上进行分片处理，也可以在 TCP 中发送更大的包。

## IPv6

IPv6（IP version 6）是为了根本解决 IPv4 地址耗尽的问题而被标准化的网际协议。IPv4 的地址长度为 4 个 8 位字节，即 32 比特。而 IPv6 的地址长度则是原来的 4 倍，即 128 比特，一般写成 8 个 16 位字节。

### IPv6 的特点

IP 得知的扩大与路由控制表的聚合。

性能提升。包首部长度采用固定的值（40字节），不再采用首部检验码。简化首部结构，减轻路由器负担。路由器不再做分片处理。

支持即插即用功能。即使没有DHCP服务器也可以实现自动分配 IP 地址。

采用认证与加密功能。应对伪造 IP 地址的网络安全功能以及防止线路窃听的功能。

多播、Mobile IP 成为扩展功能。

### IPv6 中 IP 地址的标记方法

一般人们将 128 比特 IP 地址以每 16 比特为一组，每组用冒号（“：”）隔开进行标记。

而且如果出现连续的 0 时还可以将这些 0 省略，并用两个冒号（“：：”）隔开。但是，一个 IP 地址中只允许出现一次两个连续的冒号。

### IPv6 地址的结构

IPv6 类似 IPv4，也是通过 IP 地址的前几位标识 IP 地址的种类。

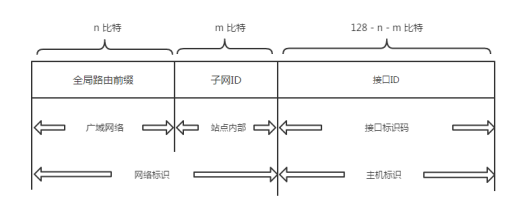
在互联网通信中，使用一种全局的单播地址。它是互联网中唯一的一个地址，不需要正式分配 IP 地址。



### 全局单播地址

全局单播地址是指世界上唯一的一个地址。它是互联网通信以及各个域内部通信中最为常用的一个 IPv6 地址。

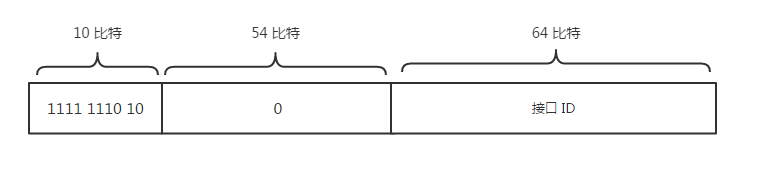
格式如下图所示，现在 IPv6 的网络中所使用的格式为，n = 48，m = 16 以及 128 - n - m = 64。即前 64 比特为网络标识，后 64 比特为主机标识。



全局单播地址

### 链路本地单播地址

链路本地单播地址是指在同一个数据链路内唯一的地址。它用于不经过路由器，在同一个链路中的通信。通常接口 ID 保存 64 比特版的 MAC 地址。



链路本地单播地址

### 唯一本地地址

唯一本地地址是不进行互联网通信时所用的地址。

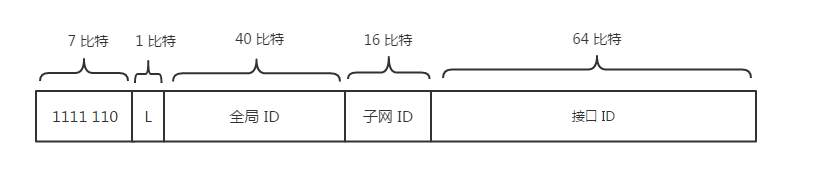
唯一本地地址虽然不会与互联网连接，但是也会尽可能地随机生成一个唯一的全局 ID。

L 通常被置为 1

全局 ID 的值随机决定

子网 ID 是指该域子网地址

接口 ID 即为接口的 ID



唯一本地地址

### IPv6 分段处理

IPv6 的分片处理只在作为起点的发送端主机上进行，路由器不参与分片。

IPv6 中最小 MTU 为 1280 字节，因此，在嵌入式系统中对于那些有一定系统资源限制的设备来说，不需要进行“路径 MTU 发现”，而是在发送 IP 包时直接以 1280 字节为单位分片送出。

### IP 首部（暂略）

## IP 协议相关技术

IP 旨在让最终目标主机收到数据包，但是在这一过程中仅仅有 IP 是无法实现通信的。必须还有能够解析主机名称和 MAC 地址的功能，以及数据包在发送过程中异常情况处理的功能。

### DNS

我们平常在访问某个网站时不适用 IP 地址，而是用一串由罗马字和点号组成的字符串。而一般用户在使用 TCP/IP 进行通信时也不使用 IP 地址。能够这样做是因为有了 DNS （Domain Name System）功能的支持。DNS 可以将那串字符串自动转换为具体的 IP 地址。

这种 DNS 不仅适用于 IPv4，还适用于 IPv6。

### ARP

只要确定了 IP 地址，就可以向这个目标地址发送 IP 数据报。然而，在底层数据链路层，进行实际通信时却有必要了解每个 IP 地址所对应的 MAC 地址。

ARP 是一种解决地址问题的协议。以目标 IP 地址为线索，用来定位下一个应该接收数据分包的网络设备对应的 MAC 地址。不过 ARP 只适用于 IPv4，不能用于 IPv6。IPv6 中可以用 ICMPv6 替代 ARP 发送邻居探索消息。

RARP 是将 ARP 反过来，从 MAC 地址定位 IP 地址的一种协议。

### ICMP

ICMP 的主要功能包括，确认 IP 包是否成功送达目标地址，通知在发送过程当中 IP 包被废弃的具体原因，改善网络设置等。

IPv4 中 ICMP 仅作为一个辅助作用支持 IPv4。也就是说，在 IPv4 时期，即使没有 ICMP，仍然可以实现 IP 通信。然而，在 IPv6 中，ICMP 的作用被扩大，如果没有 ICMPv6，IPv6 就无法进行正常通信。

### DHCP

如果逐一为每一台主机设置 IP 地址会是非常繁琐的事情。特别是在移动使用笔记本电脑、只能终端以及平板电脑等设备时，每移动到一个新的地方，都要重新设置 IP 地址。

于是，为了实现自动设置 IP 地址、统一管理 IP 地址分配，就产生了 DHCP（Dynamic Host Configuration Protocol）协议。有了 DHCP，计算机只要连接到网络，就可以进行 TCP/IP 通信。也就是说，DHCP 让即插即用变得可能。

DHCP 不仅在 IPv4 中，在 IPv6 中也可以使用。

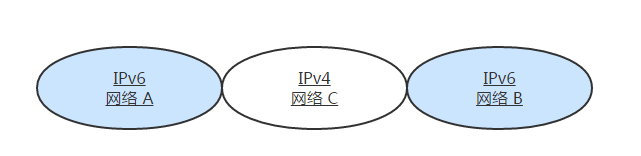
### NAT

NAT（Network Address Translator）是用于在本地网络中使用私有地址，在连接互联网时转而使用全局 IP 地址的技术。

除转换 IP 地址外，还出现了可以转换 TCP、UDP 端口号的 NAPT（Network Address Ports Translator）技术，由此可以实现用一个全局 IP 地址与多个主机的通信。

NAT（NAPT）实际上是为正在面临地址枯竭的 IPv4 而开发的技术。不过，在 IPv6 中为了提高网络安全也在使用 NAT，在 IPv4 和 IPv6 之间的相互通信当中常常使用 NAT-PT。

### IP 隧道



夹着 IPv4 网络的两个 IPv6 网络

如上图的网络环境中，网络 A 与网络 B 之间无法直接进行通信，为了让它们之间正常通信，这时必须得采用 IP 隧道的功能。

IP 隧道可以将那些从网络 A 发过来的 IPv6 的包统合为一个数据，再为之追加一个 IPv4 的首部以后转发给网络 C。

一般情况下，紧接着 IP 首部的是 TCP 或 UDP 的首部。然而，现在的应用当中“ IP 首部的后面还是 IP 首部”或者“ IP 首部的后面是 IPv6 的首部”等情况与日俱增。这种在网络层的首部后面追加网络层首部的通信方法就叫做“ IP 隧道”。

# ****经典课后题****

3.1 简述数据链路层的功能。

答：数据链路层是在物理层提供的比特流传送服务的基础上，通过一系列的控制和管理，构成透明的、相对无差错的数据链路，向网络层提供可靠、有效的数据帧传送的服务。

其主要功能包括：链路管理，帧定界，流量控制，差错控制，数据和控制信息的识别，透明传输，寻址。

3.2 试解释以下名词：数据电路，数据链路，主站，从站，复合站。

答：数据电路是一条点到点的，由传输信道及其两端的DCE构成的物理电路段，中间没有交换节点。数据电路又称为物理链路，或简称为链路。

数据链路是在数据电路的基础上增加传输控制的功能构成的。一般来说，通信的收发双方只有建立了一条数据链路，通信才能够有效地进行。

在链路中，所连接的节点称为“站”。发送命令或信息的站称为“主站”，在通信过程中一般起控制作用；接收数据或命令并做出响应的站称为“从站”，在通信过程中处于受控地位。同时具有主站和从站功能的，能够发出命令和响应信息的站称为复合站。

3.3 数据链路层流量控制的作用和主要功能是什么？

答：流量控制简称“流控”，是协调链路两端的发送站、接收站之间的数据流量，以保证双方的数据发送和接收达到平衡的一种技术。

在计算机网络中，由于接收方往往需要对接收的信息进行识别和处理，需要较多的时间，通常发送方的发送速率要大于接收方的接收能力。当接收方的接收处理能力小于发送方的发送能力时，必须限制发送方的发送速率，否则会造成数据的丢失。流量控制就是一种反馈机制，接收方随时向发送方报告自己的接收情况，限制发送方的发送速率。保证接收方能够正常、有序地接收数据。

3.4 在停止-等待协议中，确认帧是否需要序号？为什么？

答：在停止-等待协议中，由于每次只确认一个已经发送的帧，确认帧可以不需要序号。但在一些特殊情况下会出现问题。如果发送方在超时重发一个帧后又收到了迟到的确认，就不能确定该应答是对哪一个帧的确认，并可能导致随后的传送过程重新差错。

3.5 解释为什么要从停止-等待协议发展到连续ARQ协议。

答：停止—等待协议的优点是控制比较简单；缺点是由于发送方一次只能发送一帧，在信号传播过程中发送方必须处于等待状态，这使得信道的利用率不高，尤其是当信号的传播时延比较长时，传输效率会更低。

导致停止—等待协议信道利用率低的原因，是因为发送方每发送一帧都需要等待接收方的应答，才可以继续发送。如果能允许发送方在等待应答的同时能够连续不断地发送数据帧，而不必每一帧都是接收到应答后才可以发送下一帧，则可以提高传输效率。允许发送方在收到接收方的应答之前可以连续发送多个帧的策略，就是滑动窗口协议。滑动窗口流量控制包括连续ARQ和选择ARQ方式。

3.6 对于使用3比特序号的停止-等待协议、连续ARQ协议和选择ARQ协议，发送窗口和接收窗口的最大尺寸分别是多少？

答：使用3比特对帧进行编号，可以有0～7，共8种编码。

停止-等待协议：发送窗口＝1，接收窗口＝1；

连续ARQ协议：最大发送窗口＝7，接收窗口＝1；

选择ARQ协议：最大发送窗口＝4，最大接收窗口＝4。

3.7 信道速率为4kb/s，采用停止等待协议，单向传播时延tp为20ms，确认帧长度和处理时间均可忽略，问帧长为多少才能使信道利用率达到至少50%？

答：不考虑确认帧发送时间和双方的处理时间，则信道利用率＝tF/(2tp+tF)

tF=L/v，其中L为帧长度，v=4kb/s

要使信道利用率达到50％，则 tF >= 40 ms

可以得到 L >= 160 bit

3.8 假设卫星信道的数据率为1Mb/s，取卫星信道的单程传播时延为250ms，每一个数据帧长度是1000bit。忽略误码率、确认帧长和处理时间。试计算下列情况下的卫星信道可能达到的最大的信道利用率分别是多少？

1) 停止-等待协议；

2）连续ARQ协议，WT=7；

3）连续ARQ协议，WT=127。

答：不考虑差错情况，确认帧发送时间和双方的处理时间，则信道利用率＝tF/(2tp+tF)

tF=L/v， 其中L为一个帧长度，v=1Mb/s，则tF=1000/1000000＝0.001s＝1ms

1) 停止-等待协议：每次只发送一个帧，信道利用率＝1 /（250×2＋1）＝1/501

2）连续ARQ协议，WT=7：可以连续发送7个帧，但后面的6个帧是在等待的同时发送，

信道利用率＝7 /（250×2＋1）＝7/501

3）连续ARQ协议，WT=127：可以连续发送127个帧，但后面的126个帧是在等待的同时发送，

而且，当127个帧全部发送完毕使用了127ms，确认应答还没有到达，

信道利用率＝127 /（250×2＋1）＝127/501

3.9 简述PPP协议的组成。

答：PPP由以下三个部分组成：

（1）在串行链路上封装IP数据报的方法：PPP既支持异步链路(无奇偶校验的8比特数据)，也支持面向比特的同步链路。

(2) 链路控制协议(Link Control Protocol ，LCP)：用于建立、配置和测试数据链路连接，通信的双方可协商一些选项。

(3) 网络控制协议(Network Control Protocol，NCP)：用于建立、配置多种不同网络层协议，如IP，OSI的网络层，DECnet以及AppleTalk等，每种网络层协议需要一个NCP来进行配置，在单个PPP链路上可支持同时运行多种网络协议。

3.10 简述PPP链路的建立过程。

答：目前大部分家庭上网都是通过PPP在用户端和运营商的接入服务器之间建立通信链路。当用户拨号接入网络服务提供商ISP时，路由器的调制解调器对拨号做出应答，并建立一条物理连接。这时，PC机向路由器发送一系列的LCP分组(封装成多个PPP帧)。这些分组及其响应选择了将要使用的一些PPP参数。接着就进行网络层配置，NCP给新接人的PC机分配一个临时的IP地址。这样，计算机就和网络建立了一个PPP连接，成为Internet上的一个主机了。

3.11 简述HDLC信息帧控制字段中的N（S）和N（R）的含义。要保证HDLC数据的透明传输，需要采用哪种方法？

答：HDLC信息帧控制字段中的N（S）表示当前发送的帧的编号，使接收方能够正确识别所接收的帧及帧的顺序；

N（R）表示N(R)以前的各帧已正确接收，通知发送方希望接收下一帧为第N(R)帧。

要保证HDLC数据的透明传输，需要避免数据和控制序列中出现类似帧标志的比特组合，保证标志F的唯一性，HDLC采用“0”比特插入／删除法。采用这种方法，在F以后出现5个连续的1，其后额外插入一个“0”，这样就不会出现连续6个或6个以上“1”的情况。在接收方，在F之后每出现连续5个“1”后跟随“0”，就自动将其后的“0”删除，还原成原来的比特流，

3.12 若窗口序号位数为3，发送窗口尺寸为2，采用Go back N(出错全部重发)协议，试画出由初始状态出发相继发生下列事件时的发送及接收窗口图示：发送0号帧；发送1号帧；接收0号帧；接收确认0号帧；发送2号帧；接收1号帧；接收确认1号帧。

答：



3.13 试用HDLC协议，若主站A与从站B以异步平衡方式，采用选择ARQ流量控制方案，按以下要求实现链路通信过程：  
1）A站有6帧要发送给B站，A站可连续发3帧；  
2）A站向B站发的第2、4帧出错；  
帧表示形式规定为：（帧类型：地址，命令，发送帧序号N（S），接收帧序号N（R），探询/终止位P/F）

答：



3.14 在面向比特同步协议的帧数据字段中，出现如下信息：1010011111010111101（高位在左低位在右），则采用“0”比特填充后的输出是什么？

答：“0”比特自动插入/删除技术是在信息序列中连续5个“1”后自动加入一个“0”比特，则以下信息序列采用“0”比特插入后为：

信息序列： 1010011111010111101

“0”比特插入后：10100111110010111101

3.15 HDLC协议中的控制字段从高位到低位排列为11010001，试说明该帧是什么帧，该控制段表示什么含义？

答：HDLC协议中的控制字段从高位到低位排列为11010001，即最低两位（b1b0）为“01”，表示是监督帧。其控制字段b3b2为“00”，表示是“RR”，接收准备好，可以继续发送。P/F＝1，N（R）＝110，表示对第5号帧及以前各帧确认，希望下一次接收第6号帧。

3.16 HDLC协议的帧格式中的第三字段是什么字段？若该字段的第一比特为“0”，则该帧为什么帧？

答：HDLC协议的帧格式中的第三字段是控制（C）字段。若该字段的第一比特（最低位LSB）为“0”，则该帧为信息帧。

3.17 常用的差错控制的方法有哪些？各有什么特点？

答：（1）检错重发（ARQ）：接收端检测到接收信息有错时，通过自动要求发送端重发保存的副本以达到纠错的目的，这种方式需要在发送端把所要发送的数据序列编成能够检测错误的码，在后面的数据链路层中将会详细介绍这种差错控制的方法。

（2）前向纠错（FEC）：接收端检测到接收信息有错后，通过计算，确定差错的位置，并自动加以纠正，这种方式需要发送端将输入的数据序列变换成能够纠正错误的码。

（3）混合方式：接收端采取纠检错混合（在ATM中应用），即对少量差错予以自动纠正，而超过其纠正能力的差错则通过重发的方法加以纠正。

（4）信息反馈（IRQ）：接收端把收到的数据序列全部由反向信道送回给发送端，发送端比较其发送的数据序列与送回的数据序列，从而发现是否有错误，并把认为错误的数据序列的原始数据再次发送，直到发送端没有发现错误为止，这种方式不需要发送端进行差错控制编码。

3.18 一码长为n=15的汉明码，监督位应为多少？编码效率为多少？

答：因为对于汉明码来说，应满足2 r -1≥n

又因为n=15，所以监督位r至少应为4。

编码效率=73.3%

3.19 简述（7，4）汉明码中7和4的含义。

答：7是指一个码组的总长度是7位，4是指一个码组中信息位的长度是4位。

3.20 已知（7，4）汉明码接收码组为0100100，计算其校正子并确定错码在哪一位。

答：因为校正子

S1= c6 ⊕ c5 ⊕ c4 ⊕c2=0，

S2= c6 ⊕ c5 ⊕ c3 ⊕c1=1，

S3= c6 ⊕ c4 ⊕ c3 ⊕c0=0，

因为三个校正因子不全为0，说明码字有错。

S=S1S2S3=010，说明信息位c1有错，将c1上的0变为1，即可纠正错误。

3.21 在循环冗余校验系统中，利用生成多项式g（x）= x 5 + x 4 +x+1判断接收到的报文1010110001101是否正确？并计算100110001的冗余校验码。

答：若收到的报文是1010110001101，则用其去除以生成多项式对应的码组110011，

1 1 0 0 0 1 0 0

110011⌡1 0 1 0 1 1 0 0 0 1 1 0 1

1 1 0 0 1 1

1 1 0 0 0 0

1 1 0 0 1 1

1 1 0 0 1 1

1 1 0 0 1 1

0 1 ≠0

可知结果不是全零，所以肯定是有错的。

当要发送的数据是100110001，根据生成多项式，可知所对应的冗余校验码为5位，则在100110001后添加00000，用10011000100000/110011后，所得余数为110，则冗余校验码为00110。

# 真题解析：

**OSI七层架构**

1. 下面哪个说法正确描述了在OSI参考模型中数据的封装过程? ( B ) （2007选择题1）

A. 数据链路层在数据分组上增加了源物理地址和目的物理地址

B. 网络层将高层协议产生的数据封装成分组，并增加了第三层的地址信息和控制信息

C. 传输层将数据流封装成数据帧，并增加了可靠性和流量控制信息

D. 表示层将高层协议产生的数据分割成数据段，并增加相应的源端口和目的端口信息

**物理层**



1. 在无噪声的情况下，若某通信链路的带宽为 3kHz， 所采用的调制方法支持 32 种信号状态， 则该通信链路的 最大数据传输速率为\_\_\_\_\_\_\_\_\_\_\_\_kbps。（2012年填空1）【答案】30 （2\*3\*5）
2. 一条线路每1/16 秒采样一次，传输信号共有16 种状态，问传输速率是（ C ） （2004选择1）

A. 16bps B. 48bps C. 64bps D. 256bps

解析： 16种状态可以用4bit二进制数表示，每秒采样16次，所以每秒需要传的数据量就是64bit。如果不考虑信道

编码需要增加的冗余比特，传输速率就是64bit/s。（每次采样4 比特，每秒采样16 次，传输速率为64bps。）

1. 传统以太网发送的数据采用曼彻斯特（Manchester）编码，所占的频带宽度（ C ）。 （2009选择题2）

A．与原始基带信号相同 B．是原始基带信号的一半 C．是原始基带信号的两倍 D．是原始基带信号的四倍

解析：曼彻斯特编码是将每一个码元再分成两个相等的间隔。码元 1 是在前一个间隔为高电平而后一个间隔为低电平。

码元 0 则正好相反，从低电平变到高电平。这种编码的好处是可以保证在每一个码元的正中间出现一次电平的转换，这

对接收端的提取位同步信号是非常有利的。缺点是它所占的频带宽度比原始的基带信号增加了一倍。

1. 用 PCM 对语音进行数字化，如果将声音分为 128 个量化级，采样频率为 8000 次/秒。 那么一路话音需要的数据传输率为( A )Kbit/s。 （2006选择题1）

A．56 B．64 C．128 D．1024

解释：PCM 代表 Pulse Code Modulation(脉冲编码调制)。它通常用在电话系统，对模拟数据进行采样。一般都把 PCM

采样时间设置成 125 微秒，125µs 的采样时间对应于每秒 8000 次采样。一个典型的电话通道是 4KHz。根据奈奎斯

特定理，为获取在一个 4KHz 通道中的全部信息需要每秒 8000 次的采样频率。

1. 相关试题（大纲样卷）：数据通信中，频带传输时可采用（A）技术的调制解调器；基带传输的编码方式可采用（B）;

脉冲编码调制可采用（C）技术；多路复用时可采用（D）方法。

可供选择的答案：A、B、C、D：1.差分 PCM；2. 相移键控法 PSK；3 差分曼彻斯特编码；4. CRC；5. FDM；

参考答案： A(2. 相移键控法 PSK); B(3 差分曼彻斯特编码); C(1.差分 PCM ); D(5. FDM )。

解析：由于 =128，每个信号需要 7bit 表示，采样率为 8K/s。数据传输率为 56Kbit/s.

注：PCM 分为 n 个量化级，则需要lg 为来表示出来。

1. 下面关于千兆以太网的说法哪个是错误的( A ) （2007年选择题4）

A. 采用曼彻斯特编码利用光纤进行数据传输 B. 千兆以太网同时支持全双工模式和半双工模式

C. 数据的传输时间主要受到线路传播时延的制约 D. 支持流量控制机制

解析：8B/10B编码是千兆以太网主要采用的数据编码方法。它的编码效率大约是曼彻斯特编码的1.6倍，并且它可使用光缆或铜缆，所以A错

1. 集线器(HUB)和路由器分别工作于 OSI 参考模型的( B )层。 (2006选择题2)

A．第一和第二 B．第一和第三 C．第二和第三 D．第二和第四

解释：集线器（HUB）是物理层连网设备，路由器是网络层连网设备

1. 要控制网络上的广播风暴，可以采用的手段为( C ) (2006选择题5)

**A．**用集线器将网络分段 B．用网桥将网络分段 C．用路由器将网络分段 D．用交换机将网络分段

解释：集线器、网桥和 LAN 交换机都不隔离广播，路由器可以隔离广播，所以要控制网络上的广播风暴，可以采用

的手段为用路由器将网络分段。

解析：传统的交换机只能分割冲突域，不能分割广播域；而路由器可以分割广播域 。由交换机连接的网段仍属于

同一个广播域，广播数据包会在交换机连接的所有网段上传播，在某些情况下会导致通信拥挤和安全漏洞。连接到

路由器上的网段会被分配成不同的广播域，广播数据不会穿过路由器。 虽然第三层以上交换机具有 VLAN 功能，

也可以分割广播域，但是各子广播域之间是不能通信交流的，它们之间的交流仍然需要路由器。

注：交换机有几个端口就有几个冲突域,但是只要在一个局域网就属于同一个广播域，只有通过路由器才能将局域网划分

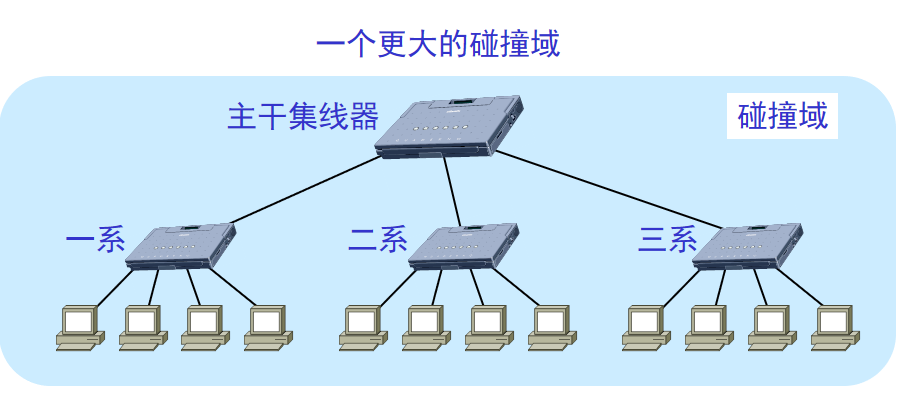
为多个广播域。

1. 一个 16 端口的二层以太网交换机，冲突域和广播域的个数分别是( D )。 (2006选择题6)

A．1，1 B．16，16 C．1，16 D．16，1

解释：2 层以太网交换机的每个端口都是冲突域的终止点，但 LAN 交换机都不隔离广播，所以本题中，冲突域和广 播域的个数分别是 16 和 1。

解析：交换机是一个端口对应一个冲突域，这样，交换机就划分了冲突域，但是所有的端口都是属于同一个广播域。



1. 使用10Mb/s 以太网,已知集线器的端口数为N,共享媒体集线器的总量为10Mb/s； 交换式以太网的总容量为 (10\*N)Mb/s 。

1. 采用二层以太网交换机扩展局域网，（ B ）是错误的。

A.二层以太网交换机的各个端口可以支持不同的速率 B.二层以太网交换机可以隔离广播帧

C.二层以太网交换机需要对收到的数据帧进行处理，增加了传输时延 D.二层以太网交换机在转发帧时不改变帧的源地址。

1. 采用12个10 Mbps端口的半双工以太网交换机互连局域网， 每个站点可获得的平均带宽为 ( D ).

A.0.83Mbps B.0.083Mbps C.8.3 Mbps D．10Mbps

解析：因为交换机的每个端口都是独立带宽

1. 一个广域网传输比特率是4Kbps，传播时延为20ms，若采用停-等协议效率是50%，帧长至少为（160）位（2019年填空）

[解析] 当发送一帧的时间等于信道传播延迟的2倍时，信道利用率是50%。或者说，当发送一帧的时间等于来回路程的传播延迟时，效率将是50%。本题中，往返传播时间为20ms×2=40ms，发送速率是每秒4000位，即发送1位需0.25ms。40ms/0.25ms/位=160位。所以，帧大于160位时，采用停一等协议才有至少50%的效率.

1. 下列不属于数据链路层的功能是（ C ）。（2009选择题3）

A.使用滑动窗口协议进行流量控制 B.提供数据的透明传输机制

C.为应用进程之间提供端到端的可靠通信 D.将IP分组封装成帧

1. 不属于数据链路层的功能是（ ）。 （2014年选择题1）

A．使用滑动窗口协议进行流量控制 B．为应用进程之间提供端到端的可靠通信

C．提供数据的透明传输机制 D．提供差错检测机制

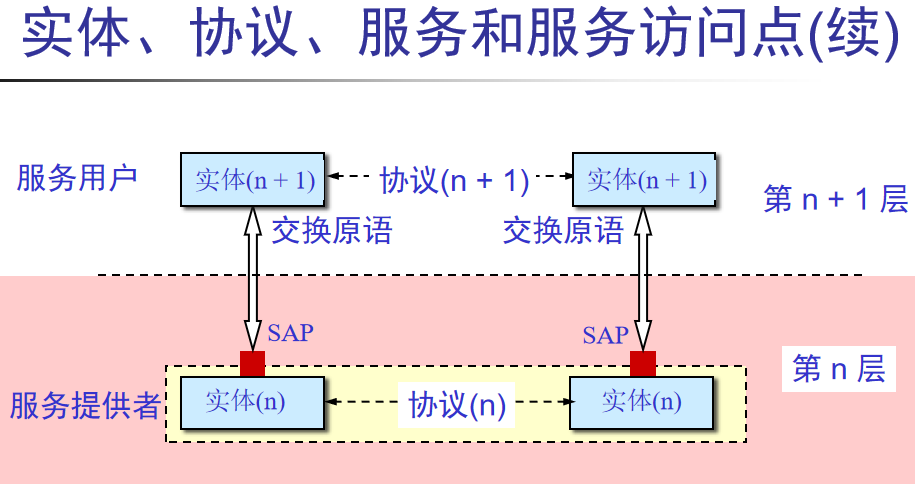
【答案】 B

【解析】数据链路层有三个基本问题，分别是：封装成帧、透明传输和差错检测，因此 C、D 两项属于数据链路层的功能。使用滑动窗口协议进行流量控制和为应用进程之间提供端到端的可靠通信均为传输层的功能。

以太网的争用期是指（两倍的端到端的传播时延），以太网发送数据使用（曼切斯特）编码。（2019网络）

1. 在数字通信中，以字节为单位进行封装，每个字节增加一个起始比特和停止比特, 每个字节中所有比特的发送时间间隔是固定的。这种通信方式为 ( B ). （2007选择题5）

同步通信 B．异步通信 C. 并行通信 D．串行通信



1. 网络协议的三要素为（ C ） （2008选择题1）

A.数据格式、编码、信号电平 B.数据格式、流量控制、拥塞控制

C.语法、语义、同步 D.编码、控制信息、同步

解释：通信双方在通信时需要遵循的一组规则和约定就是协议。协议主要由语义、语法和定时三部分组成，语义规定通 信双方准备“讲什么”，亦即确定协议元素的种类；语法规定通信双方“如何讲”，确定数据的信息格式、信号电平等； 定时则包括速度匹配和排序等。

1. 以下各项中，数据报服务是（ B ）。 （2005选择题7）

A．面向连接的、可靠的、保证分组顺利到达的网络服务 B．面向无连接的、不可靠的、不保证分组顺利到达的网络服务

C．面向连接的、不可靠的、保证分组顺利到达的网络服务 D．面向无连接的、可靠的、不保证分组顺利到达的网络服务

1. 下面对计算机网络体系结构中协议所做的描述，（ C ）是错误的。 （2008选择题1）

A．网络协议的三要素是语法、语义和同步 B．协议是控制两个对等层实体之间通信的规则的集合

C．在 OSI 参考模型中，要实现第 N 层的协议，需要使用 N＋1 层提供的服务

D．协议规定了对等层实体之间所交换的信息的格式和含义

1. 两个网段在物理层进行互连时要求( B )。 （2006选择题3）

A．数据传输率和数据链路层协议都不相同 B．数据传输率和数据链路层协议都相同

C．数据传输率相同，数据链路层协议可不同 D．数据传输率可不同，数据链路层协议相同

解释：在 N 层互连，为了让在两个网段上的计算机能够正常通信，要求 N 层以上的协议也相同。所以在本题中要求

数据传输率和数据链路层协议都相同。

1. 在网络协议的三要素中，\_\_\_\_\_\_表示事件实现顺序的详细说明；\_\_\_\_\_\_说明需要发出何种控制信息及如何响应。（2013填空）

【答案】时序；语义

【解析】网络协议的三要素为语法、语义和时序（亦可称为同步），其中，

语法是用户数据与控制信息的结构与格式，以及数据出现的顺序；语义是解释控制信息每个部分的意义，它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；时序是对事件发生顺序的详细说明。

1. 在 OSI 参考模型中，上层使用下层所提供的服务必须与下层交换命令，这些命令称为服务原语 ； 相邻层之间的接口称为 服务访问点（SAP） ；对等层之间传送的数据单位称为 协议数据单元（PDU） 。
2. 下列关于虚拟局域网（VLAN）的描述，错误的是（ D ）。

A．IEEE 802.1Q 协议定义了虚拟局域网的概念 B．虚拟局域网可以隔离广播风暴

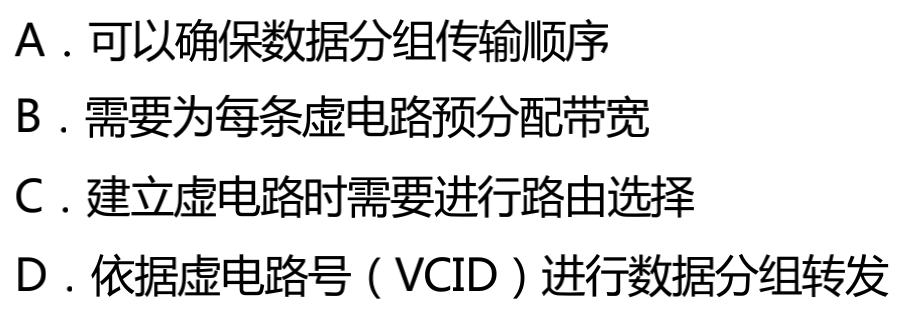
C．虚拟局域网的帧格式与传统以太网的帧格式不同 D．虚拟局域网是由一些局域网段组成的、与物理位置相关的结点集合

1. 在采用（ C ）的传输方式下，由网络负责差错控制和流量控制，分组按顺序被交付。（2008年选择5）

A．电路交换 B．报文交换 C．虚电路分组交换 D．数据报分组交换

[解析] 本题考查电路交换，报文交换，虚电路和数据报的基本概念和特点，注意电路交换不采用分组技术，报文交换也不划分分组，因此选项A和B错误。数据报传输方式没有差错控制和流量控制机制，也不保证分组按顺序被递交，因此选项D不正确。虚电路分组交换提供面向连接的、可靠的、保证分组按顺序到达的网络服务，因此答案是C。

1. 下列关于虚电路网络的叙述中，说法错误的是(D)



解析：分组交换技术可以分为两类：数据报与虚电路，请简述虚电路方式的特点  
（1）在每次分组传输之前，需要在源结点与目的结点之间建立一条逻辑连接。由于连接源结点与目的结点的物理链路已经存在，因此不需要真正去建立一条物理链路。  
（2）一次通信的所有分组都通过虚电路顺序传送，因此分组不必带目的地址、源地址等信息。分组到达目的结点时不会出现丢失、重复与乱序的现象。  
（3）分组通过虚电路上的每个结点时，结点只需要进行差错检测，而不需要进行路由选择。  
（4）通信子网中每个结点可以与任何结点建立多条虚电路连接。

1. GO\_BACK\_N和选择性重传



滑动窗口协议，是TCP使用的一种流量控制方法。该协议允许发送方在停止并等待确认前可以连续发送多个分组。由于发送方不必每发一个分组就停下来等待确认，因此该协议可以加速数据的传输。

 自动重传请求（Automatic Repeat-reQuest，ARQ）是OSI模型中数据链路层的错误纠正协议之一。它通过使用确认和超时这两个机制，在不可靠服务的基础上实现可靠的信息传输。如果发送方在发送后一段时间之内没有收到确认帧，它通常会重新发送。ARQ可能包括停止等待ARQ协议、回退ARQ和连续ARQ协议，错误检测（Error Detection）、正面确认（Positive Acknowledgment）、超时重传（Retransmission after Timeout）和 负面确认及重传（Negative Acknowledgment and Retransmission）等机制。

他们的概念是差不多的只是作用于不同的网络层。数据链路层的滑动窗口是“个数固定”的。而TCP的滑动窗口是“个数可变”的，可以由接收端设置WIN字段来修改。

传统自动重传请求分成为三种，

即停等式(stop-and-wait）ARQ: 当发送窗口和接收窗口的大小都等于 1时，就是停止等待协议。

回退n帧（go-back-n）ARQ: 当发送窗口大于1，接收窗口等于1时，就是回退N步协议。

以及选择性重传（selective repeat）ARQ: 当发送窗口和接收窗口的大小均大于1时，就是选择重发协议

后两种协议是滑动窗口技术与请求重发技术的结合，由于窗口尺寸开到足够大时，帧在线路上可以连续地流动，因此又称其为连续ARQ协议。三者的区别在于对于出错的数据报文的处理机制不同。三种ARQ协议中，复杂性递增，效率也递增。除了传统的ARQ，还有混合ARQ（Hybrid-ARQ）。

1. 在停止-等待协议中，确认帧是否需要序号？为什么？

答：在停止-等待协议中，由于每次只确认一个已经发送的帧，确认帧可以不需要序号。但在一些特殊情况下会出现问题。如果发送方在超时重发一个帧后又收到了迟到的确认，就不能确定该应答是对哪一个帧的确认，并可能导致随后的传送过程重新差错。

1. 数据链链路层采用后退N帧协议，若发送窗口大小是16，那至少需要（）位序号才能保证不出错（2019年选1）

A. 7  B.6   C.5  D.4

对应GO\_BACK\_N的窗口大小为 

答案：C

[解析] 本题考查后退N帧协议的原理。数据链路层的停止-等待协议、后退N帧协议、选择重传协议，以及TCP协议对发送窗口和接收窗口的要求，是理解协议工作原理精髓所在。后退N帧协议的最大发送窗口为2^n-1(其中n为帧号的位数)，题目中已经说明发送窗口的大小为16，也就是说如果要使得协议不出错，必须满足16≤2^n-1，所以n至少要等于5，因此答案是B。

1. 一个使用选择性重传协议的数据链路层协议，如果采用了6位的帧序号，那么可以使用的最大发送窗口是（）（2018年选择题2）

A. 31           B. 32           C. 63                D. 64

解析：在选择性重传协议中，为了保证没有重叠，那么最大窗口尺寸不应该超过序列号范围的一半。在题目中采用了5位的序列号，序列号的范围就是0～31共32个，所以最大窗口尺寸应该是16。

选择性重传

1. 对于选择性重发滑动窗口协议，若序号为 n 为，则接收窗口的最大尺寸为  （2017填空3）
2. 对于选择重传ARQ 协议，若序号位数为3，则最大发送窗口Wt 为（C ）。 （2004选择题2）

A. 7 B. 8 C. 4 D. 5

1. 若数据链路层采用回退 N（go-back-N）滑动窗口协议，发送帧的序号用 7bit 表示，发送窗口的最大值为（ C ）。（2008选择）

A．7 B．64 C．127 D．128

解析：go-back-n的对应窗口大小为 

1. 数据链路层采用 go-back—N 方式进行流量和差错控制，发送方已经发送了编号 0～6 的帧。当计时器超时， 除 1 号帧外，其他各帧的确认均已返回时，发送方需要重发( D )帧。 （2007选择题6）

A．1 B.2 C．5 D.6

解释：1 号帧尚未返回确认，当计时器超时，1 号帧及其后面的帧都要重发。因此共有 6 个帧需要重发。

1. 数据链路层采用选择重传(SR)协议，发送方已经发送了编号为0～3的帧。当计时器超时时．若发送方只收到0．2．3号帧的确认，则发送方此时需要重发的帧数是\_\_\_A\_\_\_。  
   A．1  
   B．2  
   C．3  
   D．4

解析：本题目主要考查了“多帧滑动窗口与选择重传协议(SR)”。  
当管道化技术建立在不可靠的信道上时会有一些问题。比如，如果位于帧流中的某个帧丢失或损坏了，另外在发送进程发现出错前，大量的后继帧会到达接收方；也可能当一个坏帧到达接收方时，会被接收方丢弃，这些又如何处理呢处理以上问题，其中一种方法称之为“GO-BACK-N”协议，即GBN，接收进程丢弃所有的后继帧，并且不通知发送进程。该策略对应接收窗口为l的情况，即只能按顺序接收帧，当发送进程超时后，必须按顺序重传所有未被确认的帧。如果错误率高的话，这种方法会浪费很多带宽，但对内存需求不大。为了进一步提高信道的利用率，可设法只重传出现差错的数据帧或是计时器超时的数据帧。但这时必须加大接收窗口，以便先收下发送序号不连续但仍处在接收窗口中的那些数据帧。等到所缺序号的数据帧收到后再一并送交主机。这就是选择重传协议。  
题目告知已经发送了编号为0～3的帧，当计时器超时时，发送方只收到0.2.3号帧的确认。这表示，对方已经正确接收到了0、2、3号帧，只有1号帧没有被正确接收，此时，发生了超时问题，所以发送方需要重发的帧数是1。

1. 以太网采用二进制指数退避算法来确定碰撞后重传的时间，当第四次发生碰撞后, 节点随机从   中间选择一个值。（2018年填空1）
2. 对每个数据帧，当第一次发生冲突时，设置一个参数L=2；
3. 退避间隔取1到L个时间片中的一个随机数，一个时间片等于两个节点之间最大传播时延的两倍；
4. 当数据帧再次发生冲突，则将参量L加倍；
5. 设置一个最大重传次数，超过该次数，则不再重传，并报告出错；

二进制指数退避算法是按后进先出的次序控制的，即未发生冲突或很少发生冲突的数据帧，具有优先发送的概率；而发生过多次冲突的数据帧，发送成功的概率就更小

1. 设信道的码元速率为600波特，采用4相DPSK调制，则其数据速率为\_\_\_D\_\_\_bps。  
   A．300  
   B．600  
   C．1000  
   D．1200

[解析] 根据奈奎斯特定理，码元携带的信息量由码元取的离散值个数决定。若采用4相DPSK调制，则码元可取4种离散值，一个码元携带两位信息。根据公式  
R=Blog2N =》则有Blog2N=600波特×2=1200(bps)

1. 对于10Mbps以太网，在CSMA/CD过程中，若经过4次碰撞后，节点从离散的整数集合中随机选取的整数为3，则节点选择的重传推迟时间是\_\_\_A\_\_\_。  
   A．153.6μs  
   B．76.8μs  
   C．307.2μs  
   D．38.4μs

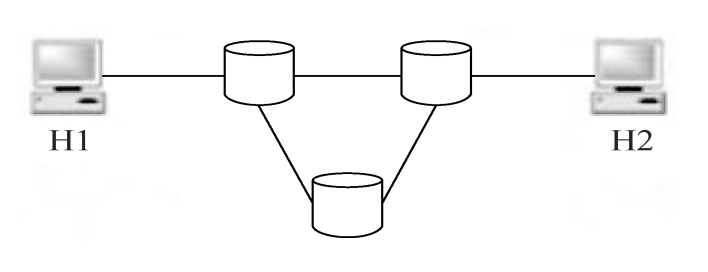
在CSMA/CD执行过程中，当检测到碰撞时，以太网使用截断二进制指数类型的退避算法来确定重传推迟时间：设参数k等于重传次数，k=Min[重传次数，10]。从离散的整数集合[0，1，…，(2^k-1)]中随机选取一个数，记为r。则重传所需的时延就是r倍的基本退避时间(以太网的基本退避时间为传送512bit所需时间)。故当选取整数为3时，重传推迟时间为：3\*512(bit)/10(Mbps)=153.6μs。

注意512bit=64\*8（以太网最短帧长64个字节）

最小帧长/数据传输速率 = 2倍的传播时延

1. 如图所示的采用“存储-转发”方式分组的交换网络中，所有的链路的数据传输速率是100Mbit/s，分组大小为1000B，其中分组头大小为20B。若主机H1向主机H2发送一个大小为980,000B的文件，则在不考虑分组拆装时间和传播延迟的情况下，从H1发送到H2接受完为止，需要的时间至少是（D）

A. 80ms B. 80.08ms C. 80.16ms D. 80.24ms



分组大小为1000B，头大小为20B，因此每个分组最大载荷980B。因此980000B的文件需要1000个1000B的分组才能传输完成，传输时间为1000\*1000\*8÷100M = 80ms。H1到H2之间的最短路径为3个链路，分组延时为1000\*8÷100M = 0.08ms，因此链路物理延迟(需要三次转发)为0.08×3 = 0.24ms

综上，从H1开始发送首个比特到H2接收完最后一个比特，总共至少需要80.24ms。

1. 主机甲通过1个路由器(存储转发方式)与主机乙互联，两段链路的数据传输速率均为10Mbps，主机甲分别采用报文交换和分组大小为10kb的分组交换向主机乙发送1个大小为8Mb(1M=106)的报文。若忽略链路传播延迟、分组头开销和分组拆装时间，则两种交换方式完成该报文传输所需的总时间分别为（D）  
   A．800ms、1600ms  
   B．801ms、1600ms  
   C．1600ms、800ms  
   D．1600ms、801ms

解析：不进行分组时，发送一个报文的时延是8Mb/10Mb/s=800ms，在接收端接收此报文的时延也是800ms，共计1600ms。进行分组后，发送一个报文的时延是10kb/10Mb/s=1ms，接收一个报文的时延也是1ms，但是在发送第二个报文时，第一个报文已经开始接收。共计有800个分组，总时间为801ms。

1. 某单位建立了一个由 30 台计算机组成的通信网络，网络中任意两个计算机之间的往返时延是 20ms，它们之间的通信采用 UDP 协议进行请求和响应。如果在 40ms 内没有收到响应，该计算机就重传请求。但很快该网络就发生了拥塞崩溃。下列选项中能解决这个问题的方法是（ ）。 （2019年选择题）

A. 增加超时计时器的超时时间 B．增加路由器中队列长度

C．接收方使用滑动窗口机制防止缓冲区溢出 D．在超时后重传请求时，使用二进制指数后退算法

【答案】D

【解析】AB 两项只是延缓了阻塞发生的时间，无法解决问题：C 项是 TCP 协议用来实现可靠传输的方法； D 项是以太网用来确定碰撞后重传的时机的算法．

1. 以太网中采用二进制指数后退算法处理发送冲突问题，下列数据帧中重传时再次发生冲突概率最低的是（ D ）。

A．首次重传的帧 B．发生两次冲突的帧 C．发生三次冲突的帧 D．发生四次冲突的帧

解析：根据 IEEE 802．3 标准的规定，以太网采用二进制指数后退算法处理冲突 问题。在由于检测到冲突而停止发送后，

一个站必须等待一个随机时间段，才能重新尝试 发送。这一随机等待时间是为了减少再次发生冲突的可能性。

等待的时间长度按下列步骤计算： 1)取均匀分布在 0 至 2min(k m)之间的一个随机整数 r、k 是冲突发生的次数。

2)发送站等待 r×2t 长度的时间才能尝试重新发送，其中 t 为以太网的端到端延迟。 从这个计算步骤可以看出，k 值

越大，帧重传时再次发生冲突的概率越低。

1. 生成树（spanning tree）算法的作用是（ B ）。 （2009选择题1）

A.发现网络中允许通过帧的最大长度 B.避免转发的帧在网络中死循环

C.减小重新传输帧时再次发生冲突的概率 D.逆向地址学习

1. 若HDLC 帧的数据域中出现比特串“ 010111110101”，为解决透明传输，则比特填充后的输出为：（ D ）。 （2004选择4 选项D有修改过）

A. 0100111110101 B. 010111110101 C. 01001111010101 D. 0101111010101

解析： HDLC 完全独立于被传送的数据，它把数据看成一个透明的位流。所有的帧都必须以标志段开头和结尾。

标志序列由01111110 构成。为了保证标志序列的惟一性，发送站将不断监视正在被发送的除标志段以外的位流，

每当有5 个连续的1 被发送时， 就插入一个附加的0（位）

1. 主机A向主机B发送IP分组,途中经过了4个路由器,那么,在IP分组的发送过程中,共使用了（ D ）次 ARP 协议。 （2013选择题）

A．1 B．3 C．4 D．5

解析：（前提，理论上，当前主机路由器 arp 表中都没有下一跳路由器 MAC） 共需 5 次，主机 A 先通过 arp 得到第一个路由器的 MAC，之后每一个路由器转发前都通过 ARP 得到下一跳路由器的 MAC，最后一条路由器将 IP 包发给 B 前仍要通过 ARP 得到 B 的 MAC，共 5 次。

1. 主机 A 向主机 B 发送 IP 分组，途中经过 6 个新路由，那么，在 IP 分组的发送过程中，共使用了 7 次 ARP 协议。（2017填空1）

解析：（前提，理论上，当前主机路由器 arp 表中都没有下一跳路由器 MAC） 共需 7 次，主机 A 先通过 arp 得到第一个路由器的 MAC，之后每一个路由器转发前都通过 ARP 得到下一跳路由器的 MAC，最后一条路由器将 IP 包发给 B 前仍要通过 ARP 得到 B 的 MAC，共 7 次。

1. 不属于路由选择协议的功能是（ A ）。 （2017年选择题4）

A.发现下一跳的物理地址 B.获得网络拓扑结构信息 C.将路由信息在互连网络内扩散 D.创建链路状态数据库

解析：在 IP 数据报进行路由转发时，ARP 协议用来发现“下一跳”物理地址，即 ARP 协议完成 IP 地址到 MAC 地址的映射

1. 以太网交换机在收到一帧后先进行\_\_\_\_\_\_；在转发帧时，对于未知目的地的帧，可以采用\_\_\_\_\_\_方式转发。（2014填空1）

【答案】存储；广播

【解析】交换机是按照存储转发方式工作的，在收到一帧后，一定是先将它存储再进行处理，而不管其目的地址是什么； 在转发顿时，如果该帧的目的地址不存在于交换机的转发表中，则交换机除接收该帧的接口以外的所有接口转发该帧。 也就是采用广播的方式转发。

1. 以太网交换机从某一个端口接收到正确的数据帧后，在转发表中查找该帧要到达的目的站点,若查不到,则交换机

向除该端口外的所有端口转发（扩散、广播）此帧（原答案 洪泛） ；若该帧的目的站点在同一端口，则交换机转发此帧 （2010填空2）

解析：注意：区别路由器找不到目的地址就丢弃，而交换机则广播。

1. 当以太网交换机收到一个帧时，若帧的目的地址在转发表中找不到对应的表项，交换机将（）（2018年选择题1）

A．丢弃      B. 洪泛

C转发给网关          D. 转发给其他主机

解析：B

1. 以太网交换机按照 自学习 算法建立转发表，并通过帧中的 **源MAC地址** 进行地址学习。 （2017填空1）

解析：一个全新的交换机的 MAC 地址表是空的， 这个表是一点一点学习到的， 接受数据帧的时候是根据源 MAC 地址去

查交换机本身的 MAC 地址表如果没有就会泛洪给除发送口外的所有接口。总之建立 MAC 地址表是根据数据帧的源 MAC 地址去学习 。

1. 要控制网络上的广播风暴，可以采用的方法为（ D ）。 （2017年选择题1）
2. 用集线器将网络分段 B.用网桥将网络分段 C.用交换机将网络分段 D.用路由器将网络分段
3. ARP 协议通过广播方式完成（ C ）的映射。 （2005选择题9）

A ．从域名到IP 地址 B．从网卡地址到IP 地址 C．从IP 地址到网卡地址 D．从IP 地址到域名

解释：地址解析协议（ARP）用来在局域网上从目的地IP地址得到目的地MAC地址。

1. 位于不同子网中的主机之间进行相互通信，下面哪个说法是正确的?( C ) (2007年选择题5)

A. 路由器在转发IP数据报时，重新封装源IP地址和目的IP地址

B. 路由器在转发IP数据报时，重新封装目的IP地址和目的硬件地址

C. 路由器在转发IP数据报时，重新封装源硬件地址和目的硬件地址

D. 源站点可以直接进行ARP广播得到目的站的硬件地址

1. 针对不同自治系统之间的路由选择协议，目前最常用的外部网关协议为\_\_\_\_\_\_\_\_。 （2017年填3）

【答案】BGP 协议

【解析】BGP 协议属于外部网关路由协议,可以实现自治系统间无环路的域间路由,是沟通 Internet 广域网的主要路由协议。



1. 关于 BGP 协议的描述正确的是（ ）。 （2013年选择3）

A. BGP 协议总是选择最短路径进行分组路由 B. BGP 不支持无分类域间路由选择 CIDR

C. BGP 采用距离向量算法计算路由表 D. BGP 协议交换路由信息的结点数量级是自治系统个数的量级

【答案】D

【解析】A 项，BGP 协议中 AS 之间的路由选择必须考虑有关策略，因而网关协议 BGP 只能力求寻找一条能够到达目的网络且比较好的路由，而并非要寻找一条最佳路由；

B 项，BGP 支持 CIDR，因此 BGP 的路由表也就包括目的网络前缀,下一跳路由器,以及到达该目的网络所要经过的 AS 序列；

C 项，BGP 采用了路径向量路由选择协议，它与距离向量协议有很大的区别；

D 项，每个 AS 中 BGP 发言人（即交换路由信息的结点）的个数是很少的，也就是在自治系统个数的量级，这样就使得 AS 之间的路由选择不致过分复杂。

1. BGP协议交换的网络可达性信息是( D ). （2007选择题7）

A ．到达某个网络的链路状态的摘要信息 B ．到达某个网络的最短距离以及下一跳路由器

C ．到达某个网络的下一跳路由器 D ．到达某个网络所经过的路径

1. 下面关于 OSPF 协议的描述，错误的是（ B ）。

A. OSPF协议直接用 IP 分组传送 OSPF 报文 B. OSPF协议中，相邻路由器定期交换整个路由表信息

C. OSPF协议中,所有路由器最终都能建立一个全网的拓扑结构图 D.OSPF协议可以将一个自治系统划分成若干区域。

解析：ospf是和采用洪泛的方式发送路由信息，不仅限于相邻路由器

1. 下一代互联网核心协议Ipv6 的地址长度为（ D ）比特。 （2005选择题3）

A ．32 B．48 C．64 D．128

解释：IPv6有比IPv4长得多的地址。IPv6的地址用16个字节表示，地址空间是IPv4的倍。

1. 关于IPv6的叙述，错误的是（）（2018年选择题）

A．IPv6数据报取消了选项字段，采用扩展首部实现选项功能 B．IPv6数据报只能在源点进行分片，路由器不进行分片操作

C．IPv6的本地链路单播地址可以和互联网上的其他主机进行通信 D．IPv6支持按流标号进行资源预分配。

解析：C。

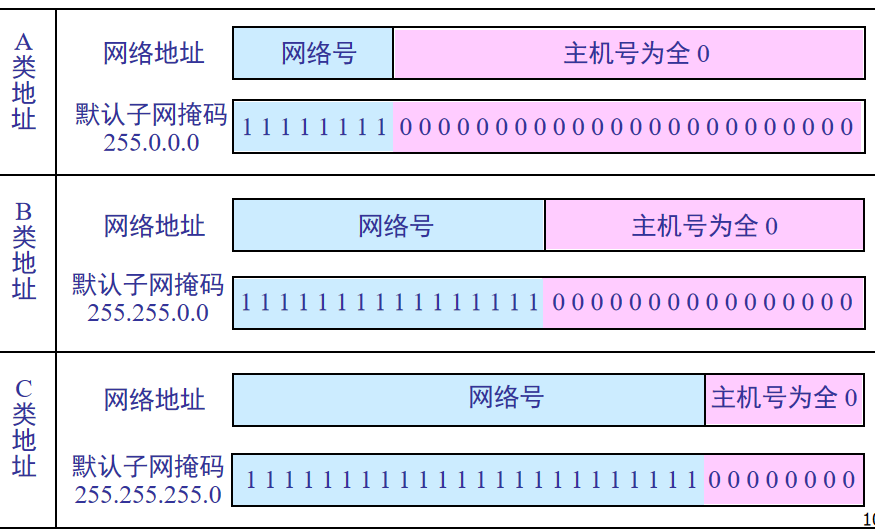
A：IPv6取消了选项字段，而用扩展首部来实现选项功能。

B：IPv6把分片限制为由源节点来完成。源点可以采用保证的最小MTU或者在发送数据前完成路径最大传送单元发现(PathMTU Discovery) ，以确定该路径到终点的最小MTU。当需要分片时源点在发送数据报前先把数据报分片，保证每个数据报片都小于此路径的MTU。因此分片是端到端的，路径途中的路由器不允许进行分片。

C：本地链路单播地址 (Link-LocalUnicast Address) 有些组织的网络使用TCP/IP协议，但并没有连接到因特网上。连接在这样的网络上的主机都可以使用这种本地地址进行通信，但不能和因特网上的其它主机通信。

D：IPv6流标号 (flow label) 占20位。支持资源的预分配。IPv6支持实时视像等要求，保证一定的带宽和时延的应用。

子网掩码知识点



0-127 128-191 192-223 224-239 240-255.

255.xx 255.255.0.0 255.255.255.0

1. 一个网段的网络号为130.10.3.0/21，子网掩码可以写为（255.255.248.0）（2019年填空题3） 21个1（16+5）

21对应255.255.248=11111000

1000000=128

248=11111000

240 = 11110000

224 = 11100000

192 =11000000

1. 一台主机的IPv4地址为16.29.4.3，子网掩码为255.248.0.0，该主机所在网络共有   32   个不同子网，该主机子网地址为    16.24.0.0       ，子网掩码对应的网络前缀有   13       位。（2018年填空3）

[注意]:首先16.29.4.3为A类地址，默认掩码为255.0.0.0，现在为255.248.0.0: 其中248=11111000，也就是占用前五位作为子网的掩码，也就是有2^5个子网，每个子网的主机号为：2^(3+8)-2=2^11-2

1. 从 212.115.32.0 开始有连续可用的 IP 地址。若某个单位需要申请 800 个地址，掩码的前缀长度为 24 位， 相当于 4 个连续的 C 类地址块。 （2017年填空3）



0XXXXXX (A) 0-127

10XXXXX （B）128--191

110XXXXX（C）192.0.0.0-223.255.255.255

解析:首先要明确该地址为C类地址，通过主机位来推导网络前缀位数： −2 ≥ 800 n=10

掩码长度:C类ip地址的掩码为24位

1. 某计算机的 lP 地址为 130.35.110.2，子网掩码为 255.255.224.0，则该计算机的子网地址为\_\_\_\_\_\_\_；与掩码对应的网络前缀有\_\_\_19\_\_\_\_位。 （2014年填空题2） 11100000(224)

【答案】130.35.96.0 ； 19 【解析】IP 地址转换成二进制为 10000010 00100011 01101110 00000010，子网掩码转换成二进制为 11111111 11111111 11100000 00000000。将 IP 地址与子网掩码按位与可得该计算机的子网地址为 10000010 00100011 01100000 00000000，即130.35.96.0，由子网掩码可知与子网掩码对应的网络前缀有 19 位。

224 = 128+64+32 = 11100000

1. 119.26.100.93 是一个\_\_A\_\_ 类 IP 地址，若子网掩码为 255.255.224.0，则该 IP 地址所在子网的广播地址为 \_\_\_。 （2012年填空2）

A ； 119.26.127.255

100=01100100

224=11100000

子网的广播地址为，除了网络号的主机号部分为全1

所以广播地址为：192.26.{01111111}.{11111111}=119.26.127.255

1. 某计算机的 IP 地址为 210.23.65.122，子网掩码为 255.255.255.240，则该计算机的子网地址为 210.23.65.112 ； 与掩码对应的网络前缀有 28 位。 （2011年填空2）

【解析】IP：210.23.65.01111010 255.255.255. 11110000 210.23.65.01110000=210.23.65.112

C 类地址默认掩码 24 位，借了 4 位，（240=11110000）网络前缀共 24+4=28 位

另，C 类地址默认掩码 24 位，借了 4 位， =16，故能分 16 个子网，有效主机有 3 8 -2= 4-2=14 个

注：

A 1.0.0.0 到 126.0.0.0 有效 0.0.0.0 和 127.0.0.0 保留

B 128.1.0.0 到 191.254.0.0 有效 128.0.0.0 和 191.255.0.0 保留

C 192.0.1.0 到 223.255.254.0 有效 192.0.0.0 和 223.255.255.0 保留

D 224.0.0.0 到 239.255.255.255 用于多点广播

E 240.0.0.0 到 255.255.255.254 保留 255.255.255.255 用于广播

1. IP 地址 10.224.12.1 的子网掩码为 255.240.0.0，和该地址在同一子网中的地址是（ C ）。 （2009选择题6）

A．10.223.21.121 B．10.240.46.23 C．10.236.23.171 D．10.242.23.120

解析：224 = 11100000 网络 ID=10.224.0.0 下一个子网 ID=10.240.0.0

240 = 11110000 通过子网掩码我们算出每个子网所含有的主机（IP）个数：16 个 256/16 = 16 0-15/16-31/32-47/48-64/(224-239)

1. 访问Internet的每台主机都需要分配IP地址（假定采用缺省子网掩码），IP地址（ B ）分配给主机是正确的。 （2004选择题5）

A. 192.46.10.0 B. 110.47.10.0 C. 127.10.10.17 D. 211.60.256.21

解析： A 是C类网络号，不是主机地址。C是为回环测试保留的地址。D是语法错误的地址，不允许有256。

选项B可以分配给主机，其A 类网络号是110，主机号是47.10.0。

127开头的ip地址是保留回环地址,不可能出现在网络上

1. 一个B 类地址的子网掩码是255.255.255.224，可以得出（ D ）个子网？（不考虑特殊地址）。 （2004选择题7）

A. 8 B. 32 C. 1024 D. 2048 -2

解析： 224 是11100000，（ 8+3）=11 位，可以有2048 个子网号。

1. 一台主机的 IP 地址为 130.72.80.12，子网掩码为 255.255.192.0 下列选项中可不经过路由器直接与该主机进行通信的

是（ ）。 （2014选择题3）

A．130.72.58.67 B．130.72.60.12 C．130.72.120.25 D．130.72.130.62

【答案】C 192=128+64 =11000000 分为 256/4 = 64 0-63/64-127

【解析】根据该主机的 IP 地址与子网掩码，计算出该主机所在的网络号为 130.72.64.0。要想不经过路由器直接与该主机

进行通信，需与该主机在同一网络中，计算 ABCD 四项的网络号分别为：130.72.0.0、130.72.0.0、130.72.64.0、130.72.128.0，

只有 C 项符合条件。

1. 一台主机的IP地址为152.68.70.3，子网掩码为255.255.224.0，必须经过路由器才能与该主机通信的是（）（2019年选择2）

A.152.68.62.23 B.152.68.67.15 C.152.68.85.220 D.152.68.90.30

答案：A

0-127 A （默认网关 255.0.0.0） 128--191 B （255.255.0.0） 224 =128+64+32 = 11100000 借位3位一共分为

256/8 = 32 0-31/32-63/64-95

1. CIDR地址块192.168.10.0/20所包含的IP地址范围是（D）（2019年选择4）

A．192.168.10.0-192.168.12.255 B．192.168.10.0-192.168.13.255

C．192.168.10.0-192.168.14.255 D．192.168.10.0-192.168.15.255

[解析] CIDR地址由网络前缀和主机号两部分构成。CIDR将网络前缀都相同的连续的IP地址组成“CIDR地址块”。本试题中，网络前缀的长度为20位，主机号为12位，因此192.168.10.0/20地址块中的地址数为2他个。其中，当主机号全为0时，得该CIDR地址块的最小地址为192.168.10.0；当主机号全为1时，该CIDR地址块的二进制表示为1100 0000.1010 1000.0000 1111.1111 1111，得最大地址为192.168.15.255。

[注意] CIDR表示法的意义与计算

1. 四个地址块172.18.129.0/24，172.18.130.0/24，172.18.132.0/24，172.18.133.0/24，如果进行路由汇聚，覆盖这4个地址块的是（）（2018选择题3）

A. 172.18.132.0/23            B. 172.18.128.0/22            C. 172.18.130.0/22                D 172.18.128.0/21

解析：D

129===》10000001

130===》10000010

132===》10000011

133===》10000100

（均包含） 10000000 =172.18.128.0/21

1. 若 IP 地址是 10.12.100.2，子网掩码是 255.255.224.0，则该子网的地址是（ C ）。 （2017选择题3）

A.10.12.0.0 B.10.12.32.0 C.10.12.96.0 D.10.12.128.0

解析： 10 . 12 . 01100100.2 255.255.11100000.0 10 . 12 .01100000.0 =10.12.96.0

1. 在某一个子网中给以下四台主机分配IP 地址（子网掩码均为255.255.255.244） ,其中一台因IP地址分配不当 而存在通信故障，这台主机IP 地址为（ A ） （201选择题3）

A． 200.10.1.60 B． 200.10.1.65 C． 200.10.1.70 D． 200.10.1.75

解释：[解析] 子网掩码255.255.255.244的最后一个字节“224”的二进制数表示为1111 0100。而4个选项IP地址的最后一个字节的二进制数表示分别为：60=(0011 1100)2，65=(0100 0001)2，70=(0100 0110)2，75=(0100 1011)2。其中，被子网掩码中的比特1所覆盖的部分中共有3个“010”、1个“001”，因此IP地址为192.168.3.60/27的主机无法与其他3台主机进行数据通信；而其他3台主机处于同一个逻辑子网，它们相互之间可以进行数据通信。

注意看最长匹配前缀

1. 类似例题：在某一个子网中，分别给4台主机分配了各自的IP地址，这4台主机的子网掩码均设置为255.255.255.224。其 中一台主机因IP地址分配不当而不能与其他3台主机进行数据通信。这一台主机的IP地址可能是 ( ) 。

A．192．168．3．60 B．192．168．3．65 C．192．168．3．70 D．192．168．3．75

解：子网掩码255．255．255．224的最后一个字节“224”的二进制数表示为11100000。而4个选项IP地址的最后一个字节的二 进制数表示分别为：60=(00l1 ll00)2，65=(0100 0001)2，70=(0100 0110)2，75=(0100 1011)2。其中，阴影部分表示被子网 掩码中比特l所覆盖的部分。对比这4处阴影部分的比特值，共有3个“010”、1个“001”，因此IP地址为192.168.3.60/27的主 机无法与其他3台主机进行数据通信；而其他3台主机处于同一个逻辑子网，它们相互之间可以进行数据通信。

1. 一个网段的网络号为 198．90．10．0/27，子网掩码固定为 255．255．255．224，最多可以分成( A )个子网， 而每个子网最多具有( A )个有效的 IP 地址。 （2006选择题6）

A．8，30 B．4．62 C． 16．14 D．32，6

解析：198．90．10．0 为 C 类地址，前 24 位形成网络号，又因为198．90．10．0/27，所以子网号占用3位. 由于十进制 224 的二进制编码为 11100000，因此最多可以划分 2^3=8 个子网，每个子网有 个 IP 地址，除去全 0 和全 1 的两个 IP 地址，还有 30 个有效的 IP 地址。

注：划分子网只与 IP 地址的类型和子网掩码有关。

1. 某单位分配了B类地址, 计划将内部网络分成35个子网，将来要增加16子网,每个子网的主机数接近800台，可行的掩码方案是( B ) 。 （2007选择题6）

A.255.255.248.0 B．255.255.252.0 C.255.255.254.0 D．255.255.255.0

解析： B地址为255.255.0.0 要求每个子网含800以上。对应10位，对应的网络号为22位。 子网数为35+16=51按照64取值。需要借位6位对应252（11111100）

248=11111000 252=11111100 254=11111110 255=11111111

1. 假定一台主机的 IP 地址是 180.120.74.56，子网掩码为 255.255.240.0，则该子网地址为（ B ）。

A．180.120.0.0 B．180.120.64.0

C．180.120.72.0 D．180.120.74.0

解析：74 =01001010 240=11110000 64 =01000000

子网地址计算方式 子网数计算方式（先判断哪一类的地址）

TCP和UDP数据有效率计算

1. 长度为 500 位的应用层数据递交给传输层处理，需加上 20 字节的 TCP 头部。再递交给网络层处理，需加上 20 字节的 IP 头部。最后递交给数据链路层的以太网传送，还需加上 18 字节的头部和尾部。 假设不计其他开销， 该数据的传输效率为 约 51.9% 。

解析：注意tcp是面向字节的因此，因此tcp发送的是整数个字节，

数据长度为：500/8=62.5=63 字节 传输效率=63(63+20+20+18)=62.5/120.5≈52.06%

1. TCP 协议是面向字节流的协议，其特点是（ A ）。 （2009选择题8）

A．接收方收到的数据块和发送方发出的数据块大小可能不相同 B．接收方的 TCP 每次向应用层交付一个完整的报文

C．TCP 协议知道所传输的数据块的含义 D．TCP 协议不要求主机维护复杂的状态表

1. 对分片后的数据进行重组的是（B）（2019选择题3）
2. 中间主机 B. 目的主机 C. 核心路由器 D.下一跳路由器
3. 对于 IP 分组的分段和重组，（ B ）是正确的。 （2008选择题6）
4. IP 分组可以被源主机分段，并在中间路由器进行重
5. IP分组可以被路径中的路由器分段，并在目的主机进行重组

C. IP 分组可以被路径中的路由器分段，并在中间路由器上进行重组

D. IP分组可以被路径中的路由器分段，并在最后一跳的路由器进行重组

答案：B

TCP滑动窗口和三次握手

1. 设主机A通过TCP连接向主机B连续发送两个TCP报文段。现已知第一个报文段的序号为1000，且该报文段中有1000字节数据，则第二个报文段序号为（ ）。  
   A. 1001 B. 2000 C. 1999 D. 2001

答案是B。  
TCP是面向连接的字节流，每个字节按顺序编号。  
第一个报文起始为1000，长度为1000，该报文最后一个字节的编号为1999，则下一个报文的第一个字节编号为2000.

1. 若主机A通过一个TCP链接向主机B连续发送两个相邻的TCP报文段, 第一个报文段的序号为750，第二个序号为1100，那么第一个报文段中有     350      字节数据。（2018年填空2）
2. 假设主机A通过TCP连接向主机B连续发送两个TCP报文段,序号分别为90和110,若第一个报文段丢失而第二个报文段到达主机B,则主机B发给A的确认报文的确认号为是多少? 90
3. 判断是非并说明原因.假设主机A 通过TCP连接向主机B发送一个序号为38的4字节报文段,则主机B对这一报文段的确认号必定是42.

错  
反例如上题,如果这个是重传的,而下一个报文段已经到达并确认.

1. 在源主机A和目的主机B之间的数据报被限制为500字节（包括首部）.假定A向B发送一个3000字节的数据报,初始数据报具有标识号422,则A将会产生多少个报文段?它们的特征是什么?（包括标识、报文段长、报文段的偏移、标志）
2. 对（3000-20）/(500-20)取整得7,可以得知要7个报文段.  
   特征分别为：包括标识、报文段长、报文段的偏移、标志）  
   422 500 0 1  
   422 500 60 1  
   422 500 120 1  
   422 500 180 1  
   422 500 240 1  
   422 500 300 1  
   422 120 360 0
3. 考虑在主机 A 和主机 B 之间建立一个 TCP 连接，若主机 A 向主机 B 连续发送两个 TCP 报文段，第一个报文段的序号为 200，第二个报文段的序号是 1100，则第一个报文段中的数据为\_\_\_\_\_\_\_\_\_\_\_\_字节。若第一个报文段丢失， 第二个报文段到达主机 B，那么主机 B 发送的报文中确认号为\_\_\_\_\_\_\_\_\_\_\_\_\_。（2013年填空题3）

【答案】900；200

【解析】第二个报文段的序号减去第一个报文段的序号即可得到第一个报文段的大小，即 1100-200=900 字节； TCP 是可靠的传输协议，第一个报文段丢失后，主机 B 收不到该报文， 仍希望收到第一个报文， 则发送的报文的 确认号仍为第一个报文的序号，即 200。

1. TCP 报文中，确认号为1000 表示（ A ）。 （2003选择题8）

A. 已收到999 字节 B. 已收到1000 字节 C. 报文段999 已收到 D. 报文段1000 已收到

解析：确认号为1000 表示期待接收的下一个字节号是1000，因此已收到999 号字节。

1. 主机甲和主机乙之间已建立 TCP 连接，主机甲向主机乙发送了三个 TCP 段。其中有效载荷长度分别为 400、500、600 字节，第一 个段的序号为 200，传输过程中第二个段丢失，主机乙收到第一和第三个段后分别返回确认，分别返回的两个确认号是（ C ）。 （2017年选4）

A.600 和 900 B.600 和 1500 C.600 和 600 D.600 和 1100

答：TCP 协议是可靠的传输协议，200+400=600，第一段返回确认为 600，第二段丢失，故返回确认还是 600。

TCP协议中发送窗口的大小应该由（拥塞）窗口和（接收）窗口中较小的一个决定（2019年填空4）

1. 在TCP协议中，发送方的窗口大小是由( C ) 的大小决定的。 （2007年选择题8）

A ．仅接收方允许的窗口 B ．接收方允许的窗口和发送方允许的窗口

C ．接收方允许的窗口和拥塞窗口 D ．发送方允许的窗口和拥塞窗口

1. 在采用 TCP 连接的数据传输阶段，如果发送端的发送窗口值由 1000 变为 2000， 那么发送端在收到一个确认之前可以发送( B ). （2006选择题9）

A．2000 个 TCP 报文段 B.2000 个字节

C．1000 个字节 D.1000 个 TCP 报文段

解释：在 TCP 的连接中，数据“流”必须以正确的顺序送达对方。TCP 的可靠性是通过顺序编号和 ACK 来实现的。TCP

是面向字节流的，数据“流”上的各字节都有自己的编号，各段第 1 个数据的顺序编号和该段一起传送，我们称它为 段顺序编号。而且，在送回的 ACK 信息中，含有指示下一个应该发送的顺序编号。为控制流量，TCP 模块间通信采 用了窗口机制。这里，窗口是接收方接收字节数量能力的表示。在 ACK 应答信息中，TCP 把 ACK 加上接收方允许接 收数据范围的信息回送给发送方。发送方除非以后又收到来自接收方的最大数据允许接收范围信息，否则总是使用由接收方提供的这一范围发送数据。 S 解：TCP 的 WINDOW SIZE 是以字节数为单位的，窗口值是 2000，因此可以发送 2000 字节。

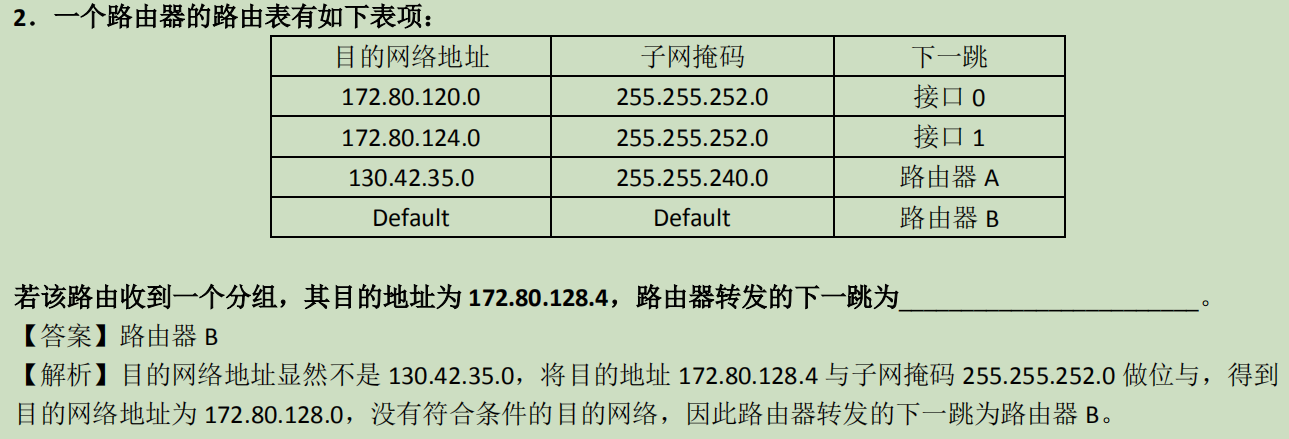
注：TCP 发送窗口以字节单位。

1. 主机 A 和主机 B 要建立 TCP 连接，A 的初始序号为 X，B 的初始序号为 Y，在建立连接过程中，共交换了 3 个报文； 其中每一端的确认序号的含义是 指示下一个应该发送的顺序编号 。 （2011年填空题）

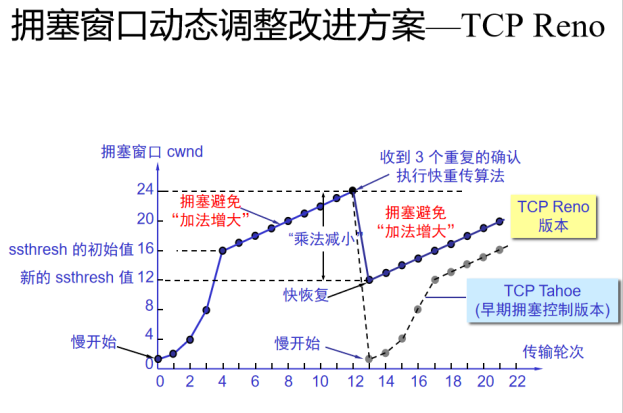
S 解：TCP 三次握手



1. 路由转发



慢启动和快速恢复



1. 假设使用 TCP 协议传送文件。TCP 的报文段大小为 1K 字节（假设无拥塞，无丢失分组），接收方通告窗口为 1M 字节。当慢启动打开发送窗口达到 32K 字节时，用了 5 个往返时延（RTT）。

解：慢启动，是传输控制协议使用的一种拥塞控制机制。慢启动也叫做指数增长期。慢启动是指每次 TCP 接收窗口收到 确认时都会增长。发送方开始时发送一个报文段，然后等待 ACK。当收到该 ACK 时，拥塞窗口从 1 增加为 2，即可以发送 两个报文段。当收到这两个报文段的 ACK 时，拥塞窗口就增加为 4，故第 n 次后为 =32，则 n=5，指数增加关系。

注： TCP 缓存区与窗口关系结论

1 发送窗口不是发送方通告的窗口，而是接收方通告的窗口。

2 接收方通告的窗口大小=发送方窗口大小。

3 接收方通告的窗口大小也=自己的窗口大小（即接收方窗口大小）

4 发送缓存>发送方窗口>已发送字节

5 接收缓存>接收窗口>接收未确认字节

6 TCP通信过程中，发送缓存和接收缓存大小不变，发送窗口和接收窗口可能会改变。

1. 在 TCP 协议的慢启动（Slow Start）中，若初始发送方设置拥塞窗口（cwnd）大小为 1，在经过三个往返时延（也称为传输轮次）后，拥塞窗口变为（ D ）。 （2009选择题9）

A．3 B．4 C．6 D．8

解析：慢启动，是传输控制协议使用的一种拥塞控制机制。慢启动也叫做指数增长期。慢启动是指每次 TCP 接收窗口收到 确认时都会增长。发送方开始时发送一个报文段，然后等待 ACK。当收到该 ACK 时，拥塞窗口从 1 增加为 2，即可以发送两个报文段。当收到这两个报文段的 ACK 时，拥塞窗口就增加为 4，故第 3 次后为，指数增加关系。

传输层

表示层

1. 下列功能中，属于表示层提供的功能是（ D ）

A．拥塞控制 B． 透明传输 C．死锁处理 D．文本压缩

解释：表示层涉及在应用层进程之间传送的数据表示。这可以包括加密、正文压缩或者两个端点系统使用的语法或数据格式之间的转换（例如EBCDIC和ASCII码之间的转换），也可以包括为了建立适当的语法与远方对等表示层进行的协商过程。它不关心数据媒介，只关心其表示。

注：表示层：定义数据表达的格式，比如加密，解密，压缩，解压缩等。

会话层：用来进行会话的建立，维护，断开的管理和数据的同步、也同来保证高层数据之间的区分。

其中死锁处理属于应用层的处理范畴

应用层

1. TCP 的连接端点称为\_\_\_\_\_\_\_\_\_\_\_，由\_\_\_\_\_\_\_\_\_\_\_\_拼接而成。

【答案】套接字； lP 地址和端口号

【解析】TCP 连接的端点称作套接字（socket）或插口。根据 RFC793 的定义：端口号拼接到 lP 地址即构成了套接字。

套接字的表示方法是点分十进制的 IP 地址后面写上端口号，中间用冒号或逗号隔开。

1. 下列关于客户／服务器方式的说法，错误的是（ B ）。 （2009选择题10）

A．客户端在通信时主动向服务器发起通信请求 B．服务器必须事先知道客户端的地址才能通信

C．客户端系统通常使用随机的传输层端口号 D．客户端和服务器之间的通信是双向的，都可以发送和接收数据

域名解析

1. 域名解析两种方式分别是（）（2018选1）

A. 直接解析和间接解析           B. 直接解析和递归解析

C. 间接解析和迭代解析           D. 迭代解析和递归解析

解析：D

1. 在解析域名时， 客户端向本地域名服务器发出查询请求， 如果服务器不能回答该请求，就向其他域名服务器发出查询请求，直到最终将查询结果返回给客户端。这种方式可称之为 递归 查询。 （2014年填空4）

【答案】递归

【解析】在进行域名解析时，IP 地址的查询方式主要有递归查询和迭代查询两种。

递归查询是 DNS 服务器在收到递归查询请求后，必须由它将最终的查询结果返回给请求发送方,即便该 DNS 服务器 无法从本地数据库返回查询结果，它也必须查询其他 DNS 服务器，直到得到确认的查询结果，如本题所述；

迭代查询 则是 DNS 服务器在收到迭代查询的请求后，如无法从本地数据库返回查询结果，它会返回一个可能知道 查询结果的 DNS 服务器地址给请求者，由请求者自行查询该 DNS 服务器，以此类推，请求者最终将得到查询结果。

递归有结果，迭代只转播

1. 下面哪个协议中，客户端和服务器之间采用面向连接的协议进行通信? ( B ) （2007选择9）

A ．DNS B．SMTP C ．SNMP D. DHCP

DNS/DHCP/SNMP 传输层基于UDP，只有SMTP基于TCP

1. 使用www浏览器浏览网页时,用户可用鼠标点击某个超链接,从协议分析的角度看,此时,浏览器首先需要进行 ( C ) 。 （2007选择10）

A ．IP地址到MAC地址的解析

B ．建立TCP连接

C ．域名到IP地址的解析

D ．建立会话连接，发出获取某个文件的命令

各种协议汇总



1. 下列协议中使用 UDP 协议传送的是（ B ）。 （2017选择题5）

A.FTP B.DNS C.HTTP D.OSPF

基于面向连接的 TCP 协议， 如 FTP(21 连接，20 传输)、Telnet(23)、HTTP(80)、SMTP(25)、POP3(110)

基于无连接的使用 UDP 协议，如 DNS(53)、SNMP(161)、QQ(4000) 、OSPF 基于 IP 协议，端口号为 89

1. FTP 采用的传输层协议为\_\_\_\_\_\_\_\_\_\_\_ ，建立连接时服务器的缺省端口号为\_\_\_\_\_\_\_\_。 （2012填空3）

【答案】TCP 协议；21

【解析】TCP 协议是面向连接的协议，可以保证数据的正确性，适合用于传输大量数据，相对来说速度较慢，建立

连接需要的开销较多。FTP 是文件传输协议，因而对数据的正确性要求较高，需要可靠的传输，而对速度要求相对

较低，因而在传输层采用 TCP 协议。FTP 协议在建立连接时服务器的缺省端口号为 21，用于传输数据的端口号为 20。

1. FTP 协议在使用时需要建立两个连接：控制连接和数据传输连接，并用不同的端口号标识两个连接，其中用于数据传输连接的端口号是( D )。 （2006选择题8）

A．25 B． 23 C．21 D．20

解析：21 端口是状态连接端口，20 端口是数据传输连接端口。注：FTP 服务中：20 端口用于数据连接，21 端口用于状态连接。

1. 协议（ C ）采用无连接方式进行工作。 （2004选择题6）

A. FTP B. Telnet C. SNMP D. SMTP

解析：SNMP是无连接的协议,它使用的运输层协议UDP也是无连接的。FTP、Telnet 和SMTP都是因特网上面向连接的应用协议。

1. 在因特网电子邮件系统中，电子邮件应用程序（ B ）。 （2005选择题6）

A．发送邮件和接受邮件通常都使用SMTP 协议 B．发送邮件通常使用SMTP协议，而接收邮件通常使用POP3 协议

C．发送邮件通常使用POP3 协议，而接收邮件通常使用SMTP协议 D．发送邮件和接受邮件通常都使用POP3 协议

1. 在 Internet 上，主机采用（ ）标识，运行在主机上的应用程序用（ D ）标识。（2008 选择题8）
2. 端口号 主机地址 B．主机地址 IP 地址 C．IP 地址 主机地址 D．IP 地址 端口号
3. 当客户端请求域名解析时，如果本地 DNS 服务器不能完成解析，就把请求发送给其他服务器，依次进行查询，直到把域名解析结果返回给请求的客户端。这种方式称为（ B ）。 （2008年选择题9）

A．迭代解析 B．递归解析 C．迭代与递归相结合的解析 D．高速缓存解析

网络安全

1. 用户甲发送消息给用户乙，如果既需要提供认证功能，又要保证被发送消息的保密性，可采用的方法是（ ）。 （2013年选3）

A．发送方先用接收方的公钥进行数字签名．然后再用自己的私钥进行加密

B．发送方先用其私钥对消息进行数字签名，然后再用接收方的公钥加密

C．发送方用其私钥对消息进行数字签名和加密 D．发送方用接收方的公钥进行数字签名和加密

【答案】B

【解析】A 项，发送方先用接收方的公钥进行数字签名，接收方不能验证发送方身份， 无法提供认证功能， 然后 再用自己的私钥进行加密，则消息会被他人获得，亦无法保证被发送消息的保密性；

B 项，发送方先用其私钥对消息进行数字签名，则接收方可验证消息发送方的身份， 提供了认证功能， 然后再用 接收方的公钥加密，则他人无法获取该消息的内容，保证了被发送消息的保密性；

C 项，发送方用其私钥对消息进行数字签名和加密，可提供认证功能，但是不能保证被发送消息的保密性；

D 项，发送方用接收方的公钥进行数字签名和加密，能保证被发送消息的保密性，但是不能提供认证功能。

1. 防火墙的安全架构基于( C )技术. (2006选择题10)

A．用户管理和认证 B.数据加密 C．访问控制 D.流量控制

解析：防火墙是一个或一组系统，它在网络之间执行访问控制策略。 注：防火墙基于访问控制的原理。

1. 在信息安全领域，使用（ A ）方法可以使通信的接收方验证收到报文是否受到篡改和伪造。（2008选择题10）

A．数字签名 B．数据加密 C．防火墙 D．身份认证

题型1-----UDP\TCP IP分包，计算中

1. 一台路由器收到一个1500字节的IPv4分组，IP头部为20字节，如果需要将该分组转发到一个MTU为500字节的链路上，（2019-1）

该IP分组共分成几个分片，有效数据长度分别为多少字节。

最后一个分片的片偏移是多少字节。

解析： 

①、数据+IP头 = MTU，MTU=500,所以1500字节数据分分成4片，第一、二、三片数据长度为480字节，第四片长度为60字节

②、最后一个分片的片偏移是前三片的有效数据长度480\*3 = 1440字节。

1. 一个UDP用户的数据报的数据部分长为8192字节。那么通过以太网来传播该UDP数据报时，最后一个IP分片的数据长度是(C )。  
   A．1500 B．1480 C．800 D．600

UDP头部长为8字节，因此该UDP数据报总长度为8200字节，以太网帧的最大数据域为1500，再减去20的IP头部，得到每个IP分片的最大数据域长度应该是1480，则最后一个数据分片的长度应该是(8200-5×1480=)800字节.

1. (共5分) UDP用户数据报的数据部分长度是8000字节，通过以太网来传输UDP数据报，若UDP头部为8字节，IP分组头部为20字节，以太网MTU为1500字节。(2018-2)

(1)能分几个IP分片？

(2)最后一个IP分片的长度是多少？片偏移字段值是多少？

解析 

UDP数据报长度：8000+8=8008字节 MTU为1500字节= IP头部20字节+ IP数据部分1480字节。

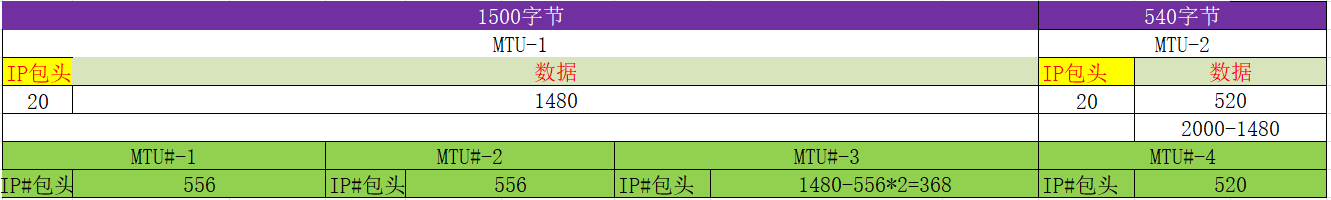
(1)8008=1480\*5+608，所以共需要6个IP分片

(2)8008=1480\*5+608，最后一个IP分片的数据长度是608+20=628字节，故最后一个片偏移字段的值为1480\*5-8。

[注意]该题不同于上面的ip分组，ip分组在每个分片上都有头部，但是对于UDP、TCP来说，头部只在第一个包的分片的上面才有，所以做此类题时需要区分是ip包还是udp、tcp包

1. 某一网络的一台主机产生了一个 IP 数据报，头部长度为 20 字节，数据部分长度为 2000 字节。 该数据报需要经过两个网络到达目的主机，这两个网络所允许的最大传输单元 MTU 分别为 1500 字节和 576 字节。 请问原 IP 数据报到达目的主机时分成了几个 IP 小报文? 每个报文的数据部分长度分别是多少? （2006-5）

解析



1、因为第一个网络的 MTU 为 1500 字节<2000+20 字节,因此在第一个网络传输时 IP 数据报被分成两个 IP 小报 文，第一个小报文的数据部分长度为 1480，第二个小报文数据部分长度为 520 字节。当传输到第二个网络时，由 于其 MTU=576<1480，因此第一个小报文还要再分成三片，第一片和第二片的数据部分长度为 556， 第三片的数据 部分长度为 1480-556\*2=368。当原 IP 数据报到达目的主机时分成了四个 IP 小报文，第一个第二个小报文数据部分 长度为 556，第三个数据部分长度为 368，第四个数据部分长度为 520 字节。

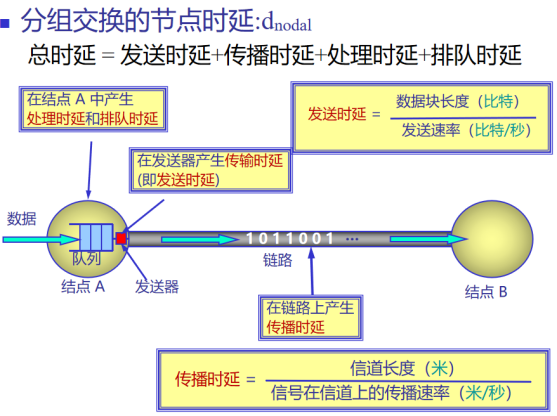
2、在 IP 层下面的每一种数据链路层都有自己的帧格式，其中包括帧格式中的数据字段的最大长度，这称为最 大传输单元 MTU 1500-20=1480，2000-1480=520，520+20=540，540<576。所以原 IP 数据报到达目的主机时分成 了两个 IP 小报文，第一个报文的数据部分长度是 1480 字节，第一个报文的数据部分长度是 520 字节。

[注意]数据包分片既可以在终点组装也可以在每通过一个网络组装，通常为前者

1. 长度为 200 字节的应用层数据交给传输层传送，需加上 20 字节的 TCP 头部。再交给网络层传送，需加上 20 字节 的 IP 头部。最后交给数据链路层的以太网传送，还需加上 18 字节的头部和尾部。假设不计其他开销，试求该数据的传输效率。 （2006年-题4-3分）

解析：该数据的传输率为 

题型2-------TCP发送窗口、吞吐率。





1. 一个TCP连接使用256Kbps链路，其端到端的传输时延为128ms，实际吞吐量是128Kbps，若忽略数据封装开销及接收方响应分组的发送时间，发送窗口大小是多少字节。（2019年题2）

答案：实际吞吐量为128Kbps，说明利用率只有50%

设窗口大小为x字节，



1. (共4分) 主机A通过一条带宽为100Mbps的网络链路向主机B传输数据帧，假设每帧携带的数据是1K字节，链路单向时延为50ms，若设计一个滑动窗口协议，使得发送窗口和接收窗口大小相同：（2018年）

(1)窗口大小是多少？

(2)最少需要多少位作为序号？

答： 传输延时：  往返传播延时：RTT= 50ms\*2 = 100ms



。

1. 假设地球到某个行星的距离约为 米。在一条 128Mbps 的点到点链路上传输数据帧。帧大小为 64K 字节，光速为米/秒。 （2017年-题2-4分）

（1）若采用简单停-等协议，信道利用率是多少？

（2）若使链路利用率达到 100%，发送窗口是多少字节？（忽略协议处理时延）

解析：（1）地球到星行的传播时延为 = 300s

发送一帧的传输时延为 4ms = 0.004s，若采用等-停协议，信道利用率为

若链路利用率为 100%，则发送窗口为x,  x= (300+300+0.004)/0.004=150001，共 9.6G 字节.

1. 假设一个 4Mbps 点到点链路，节点间距离为 5000km，数据帧大小为 1KB，设计一个选择性重传的滑动窗口协议（Selective Repeat, SR)，在管道满载的情况下，最少需要多少位作为序号？（信号的传播速率为 ） 注：时延带宽积=传播时延×带宽，是以比特为单位的链路长度，是在某时链路上可容纳的最大比特数。 （2014年1）

解析：传播时延=，在管道满载的情况下，发送窗口的最大取值为，需要的序号最小值为。（5/3\*10^-2 \* 4\*10^6）= (20/3)\*10^4=2/3 \* 10^5

[注意]:时延带宽积=带宽\*传播时间(单程)， 除了题目中特别说明的外，我们都只乘以单程的传播时延

1. 假设要在网络上传送 1MB 的文件。设分组长度为 1KB，往返时延为 40ms，网络带宽为 10Mbps。

数据发送前与接收方建立连接的时间为两倍的往返时延。试计算以下两种情况下传输文件所需的时间 （即接收方收到该文件的最后一个比特所需的时间）。 （2014年-题2-6分）

（1）数据可以被连续发送；

（2）每发送完一个分组后等待一个往返时延的时间才能再次发送下一个分组。

答：(1) 发送文件需要的时延(传输时延)＝1M\*8bit/10Mbps＝0.8s＝800ms；

最后一个分组分组需要的传播时延=40ms/2 = 20ms

传输文件所需时间＝2\*40ms＋800ms＋20ms=900ms。

因为在发送文件的时候，发送完就会进入链路，因为是连续的，所以，这段时间的传播和传输是同时进行的，因此两个是overlap的，所以不用算，但是最后一个分组，传输完后，交给了传播，两个却不是overlap的所以需要算一个传播时延

(2)该文件的分组数＝1MB/1KB=1000；

每发送完一个分组后等待一个往返时延的时间才能再次发送下一个分组，则 1000 个分组要等待 999 次，这种情况 需要的时间比数据连续发送需要时间多 999x40ms=39960ms；

传输文件所需的时间＝900ms＋39960ms=40860ms。

1. 两台主机之间通过长距离网络通信，彼此之间通过一条传输速率为 1Gbps 的信道相连。 线路的单向传播时延为 10ms。分组（包括头部和数据字段）长度为 1500 字节。 如果 ACK 分组很小，接收方收到一个分组后立即发送 ACK，试计算： （2013年-题1-5分）

（1）如果采用停等协议，信道的利用率是多少？

（2）若使信道的利用率达到 80%，窗口长度应设为多少？最少需要多少位表示序号？

解析：每个分组的发送时延

（1）如采用停等协议，信道的利用率 

（2）设窗口长度为 x 时，信道利用率达到 80%，则有：

1. 考虑一个城域网，若源和目的主机之间的平均距离为 10km，信号在传输介质中的传播速率为 m/s。 （2011年-题2-5分）

试回答问题：

① 当数据的传输速率为多大时，2K 字节分组的传输时延等于链路的往返传播时延？

② 若线路带宽为 1Gbps，线路长度为 2000km，数据传输采用停等协议，传输一个 100K 字节的文件,能否通过增加 带宽来显著缩短成功传输该文件所需的时间？试简要说明理由。

解析：1)一个分组传播时延 往返传播时延=   ，

2)一个分组传播时延 往返传播时延2\*0.01=0.02s 传输时延

一个分组发送周期 T=0.02+0.000016 (s) 100K 字节的分组有 50 个 

如采用停等协议，100K 字节的文件成功传输所需时间为=50\*（0.02+0.000016） 因链路较长导致往返传播时延占比较大，上式中，将带宽增加效果并不明显，建议采用流水线传输方式的滑动窗口机制，来提高链路利用率，从而缩短传输文件总时间。

1. 主机 A 通过一条带宽为 100Mbps 的网络链路向主机 B 传输数据帧，假设每帧携带的数据是 1K 字节， 链路的单向时延为 15ms。若设计一个滑动窗口协议,使得发送窗口和接收窗口的大小相同,最少需要多少位表示序号？ （2011年-题1-3分）

答：发送一帧所需时间：

若使用滑动窗口协议，

滑动窗口需要n位则：2^(n-1) > 376 => n-1 = 9 => n = 10

1. 两台主机之间的数据链路层采用后退N帧协议(GBN)传输数据，数据传输速率为16kbps，单向传播时延为270ms，数据帧长度范围是128～512字节，接收方总是以与数据帧等长的帧进行确认。为使信道利用率达到最高，帧序号的比特数至少为（C）  
   A．5 B．4 C．3 D．2

解析：在一个来回的2×270ms时间内，发送方可以发送至少9个128字节的数据帧，其中一个用于确认帧，8个用于发送的数据帧，帧序号8需要用4位二进制数表示（GBN：2^n - 1）

信道利用率为：T/(T+RSS) 其中T为总的传输时延，RSS为2倍的传播时延， T/(T+RSS) = 1/(1 + RSS/T) 要这个最高则要求RSS/T最小，因为RSS固定，则要求T最大, 我们知道T是总的传输时延，我们要求T越大，那就是要求发送的时长越大，用于确认的越小越好，及当帧长为128的时候最好，此时消耗的确认时长最短，留给实际发送的最长，那么信道利用率就越大。因为如果没有确认浪费的时间，你可以在T的时间内一直发一直发，而不需要考虑帧长。

1. 一个局域网采用 CSMA/CD 协议，网段长度为 2km，数据传输速率为 1Gbps，电磁信号的传播速率为 200m/μs，

问能够支持此协议的最短帧长应为多少字节？ （2010年题1-4分）



解析：

1. 网络时延带宽积可以由带宽和往返时延相乘得到。考虑两个网络： 一个是无线网络，带宽为 54Mbps，RTT 为 0.33μs；另一个是远距离的光纤网络，带宽为 10Gbps，RTT 为 40ms。 （2010年题2--5分）

①分别计算两个网络的时延带宽积；

②说明该乘积值对于分析网络性能的意义；

③若传输一个 1MB 的文件，试比较两个网络的有效利用率。

解析：时延带宽积=带宽\*RTT=

②、时延带宽积表示从发送方到接收方的管道容量，单位为bit，即所能容纳的bit数。由于有往返时间的要求，在收到来自接收方的确认信号之前(ACK)，发送方可以最多发送两个这样的时延带宽积。如果传送的信息量不能填满这样的“管道”，则链路未被充分利用。

③、无线的通道利用率为,光纤的利用率为

特别注意：除了题目特别说明的或定义的外，时延带宽积是带宽\*传播时延（非两倍的传播时延）

1. 假定卫星信道的数据率为100kbps，卫星信道的单程(发送方通过卫星到接受方)传播延时为250ms，每个数据帧长均为2000bit，并且不考虑误码、确认帧长、头部和处理时间等开销，为达到传输的最大效率，试问帧的顺序号应为多少位？此时信道利用率是多少？ （2004-5-5分）

解析：RTT=250\*2= 500ms=0.5s，传输时延=,

假设窗口大小为x。则

1. 考虑一条带宽为 1.6Mbps 的链路，往返传播时延为 45ms，假设数据帧的大小为 1KB。 若采用滑动窗口协议来保证链路的利用率，允许发送方在收到应答之前尽量连续发送多帧。 那么，至少需要多少位作为序号？（忽略确认帧大小和接收处理开销） （2009年-题3-4分）

答：发送一帧所需时间 t1 = 1KB\*8/1.6Mbps = 5ms ，RTT=45ms ,若使用滑动窗口协议，可连续发送帧数：

1. 一个采用 CSMA/CD 介质访问控制方式的局域网，总线是一条完整的同轴电缆， 数据传输率为 10Mbps（1M=），信号在总线传输介质中的传播速度为 。试计算： （2012年-题1-4分）

（1）如果最小帧长为 600bit，那么最远的两台主机之间的距离为多少米？

（2）假如最小帧长保持不变，当数据传输率提高到 100Mbps 时，为满足 CSMA/CD 要求，该局域网需做哪些调整？

解析： CSMA/CD为了避免在发送完毕后才检测到碰撞，规定最小帧长所需要的的时间即为端到端往返时间。因此最小传播延迟=最小帧长所需时间/2。因为RTT=

②、最小帧长保持不变，当数据传输率提高到 100Mbps 时，传输时延



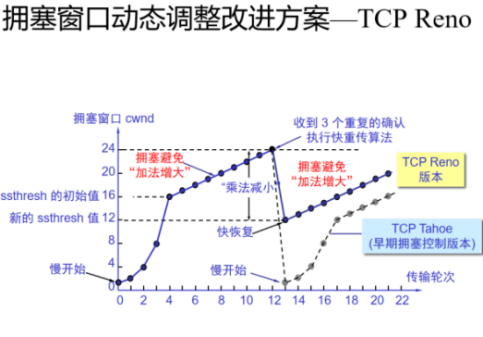
1. 考虑一条带宽为1Mbps的链路，往返时延为45ms，假设数据帧的大小为1000字节。 若采用停等协议，实际的数据率是多少? 信道利用率是多少? （2007年-题4-3分）

答：实际的数据率：（1000\*8）/（45ms+1000\*8/1Mbps）=8000/(45ms+8ms)=8/53Mbps 信道利用率：（1000\*8/1Mbps）/ （1000\*8/1Mbps+45ms）=8/53

1. 长度为1 公里、数据传输率为10Mbps 的CSMA/CD 以太网，信号传播速度为200m/us . 试求能够使该网络正常运行的最小帧长。 （2005年-题3-3分）

解答：对于1公里电缆，单程传播时间为s 往返传播时间为了够按照CSMA/CD工作，最小帧的发射时间不能小于 。 帧长=速率\*时间，故，以10Mbps速率工作， 可以发送的比特数等于：=100比特。

题型3--------拥塞机制和重传



1. 客户端C和S之间建立一个TCP连接，该连接总是以1KB的最大段长发送TCP段，C有足够数据发送，当拥塞窗口为32KB时，收到了三个重复的ACK报文，如果接下来4个RTT时间内TCP段的传输是成功的，那么在当四个RTT时间内发送的TCP段都得到ACK，拥塞窗口大小是多少？采用了怎样的拥塞机制？（2019年题3-5分）

答案：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| RTT | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 拥塞窗口 | 1 | 2 | 4 | 8 | 16 | 32 | 16 | 17 | 18 | 19 | 20 |

拥塞窗口大小为20KB

慢启动、拥塞避免（ssthrelod为窗口大小的一半）、快重传（收到3个以上的重复的ACK即开始重传）、快恢复）

[注意] 此题和接下来的两道题是不同的地方是，这里碰到的是三个重复的ACK，此时执行的是快重传或快恢复，而非超时或拥塞的慢启动从1开始，此时的快恢复从当前的一半开始

1. 一个TCP连接总是以1KB的最大段发送TCP段，发送方有足够多的数据要发送。当拥塞窗口为16KB时发生了超时，如果接下来的4个RTT(往返时间)时间内的TCP段的传输都是成功的，那么当第4个RTT时间内发送的所有TCP段都得到肯定应答时，拥塞窗口大小是(C )

A．7KB B．8KB C．9KB D．16KB

解析：  
考查TCP的拥塞控制方法。  
无论在慢开始阶段还是在拥塞避免阶段，只要发送方判断网络出现拥塞(其根据就是没有按时收到确认)，就要把慢开始门ssthresh设置为出现拥塞时的发送方窗口值的一半(但不能小于2)。把拥塞窗口cwnd重新设置为1，执行慢开始算法。这样做的目的就是要迅速减少主机发送到网络中的分组数，使得发生拥塞的路由器有足够时间把队列中积压的分组处理完毕。  
在发送拥塞后，慢开始门限ssthresh变为16/2=8KB，发送窗口变为1KB。  
在接下来的3个RTT内，拥塞窗口执行慢开始算法，呈指数形式增加到8KB，此时由于慢开始门限ssthresh为8KB，因此转而执行拥塞避免算法，即拥塞窗口开始加法增大。因此第4个RTT结束后，拥塞窗口的大小为9KB

1. 设TCP的慢启动窗口大小从1开始，拥塞窗口阈值初始为16（报文段），当拥塞窗口上升到20时发生超时，TCP开始慢启动和拥塞避免。（2018年-题3-5分）

(1)简要说明该过程中经过的拥塞控制阶段。

(2)第15轮次传输时，拥塞窗口大小为多少？

(3)在哪个传输轮次中发送第35个报文段？

解析：(1)开始慢启动,拥塞窗口达到慢开始阈值前,呈指数增长；达到阈值16后,开始拥塞避免每一轮加1；直到达到20发生拥塞，慢开始阈值变为1，拥塞窗口阈值变为10，开始拥塞避免每一轮加1。

(2)建立连接后，第1轮到第15轮次的拥塞窗口cwnd大小如下表所示（横屏看）：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 传输轮次 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 拥塞窗口大小 | 1 | 2 | 4 | 8 | 16 | 17 | 18 | 19 | 20 | 1 | 2 | 4 | 8 | 10 | 11 |

故第15轮次传输时，拥塞窗口大小为：11

1. 如上表，前5次传输轮次发送报文段个数共有：1+2+4+8+16=31个，第6次共发送16个报文段，故第6个传输轮次中才发送第35个报文段。
2. 若使用 TCP 协议传送文件,TCP 的报文段大小为 1K 字节(假设无拥塞，无丢失分组),接收方通告窗口为 1M 字节。 （2017年题3）

（1）简要说明 TCP 慢启动算法。

（2）当慢启动阶段发送窗口达到 1M 字节时，用了多少个往返时延（RTT）？

解析： 1）慢启动算法(slow start)，是传输控制协议使用的一种拥塞控制机制。

工作原理：在主机刚刚开始发送报文段时，可先设置拥塞窗口 cwnd=1，即设置为一个最大报文段 MSS 的数值。 在每收到一个对新的报文段的确认后,将拥塞窗口加倍，即成倍增加MSS 的数值。 用这样的方法逐步增大发送端的拥塞窗口 cwnd，可以使分组注入到网络的速率更加合理。其实慢启动一点也不慢只是起点比较低，是指数增长。

2）假设当慢启动阶段发送窗口达到 1M 字节时，用了 x 个往返时延，则

开始 ---> cwnd = 1 个 MSS=1K=

经过 1 个 RTT 后 ---> cwnd = MSS= 

经过 2 个 RTT 后 ---> cwnd = MSS= 

经过 3 个 RTT 后 ---> cwnd =  MSS= 

经过 x 个 RTT 后 ---> cwnd = MS=

，用了 11 个 RTT

1. 图 1 给出了 TCP 的拥塞控制过程。横坐标为时间轴，纵坐标为发送方的拥塞窗口大小。 （2013年-题3-7分）

（1）（2 分）假设最大段长 MSS 为 1000 字节。如图 1 所示，当拥塞窗口大小达到 A 点时发送方共向网络中传输了

15000 字节。试计算 A 点对应的拥塞窗口大小（假设发送方在 t=0 时刻建立 TCP 连接，数据的发送时延可以忽略不计）。

（2）（3 分）根据 TCP 的拥塞控制机制说明图 1 中 A、B 和 E 点拥塞窗口变化的原因。

（3）（2 分）图 1 中 C、D 处分别是由于什么原因导致拥塞窗口减小的？

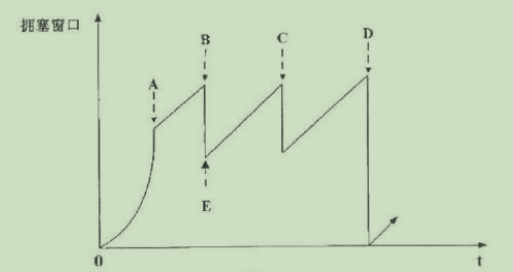


图1

答：（1）从开始到拥塞窗口达到 A 点，共传输了 15000/1000=15 个数据包，发送了，

则 A 点对应的拥塞窗口大小为 。

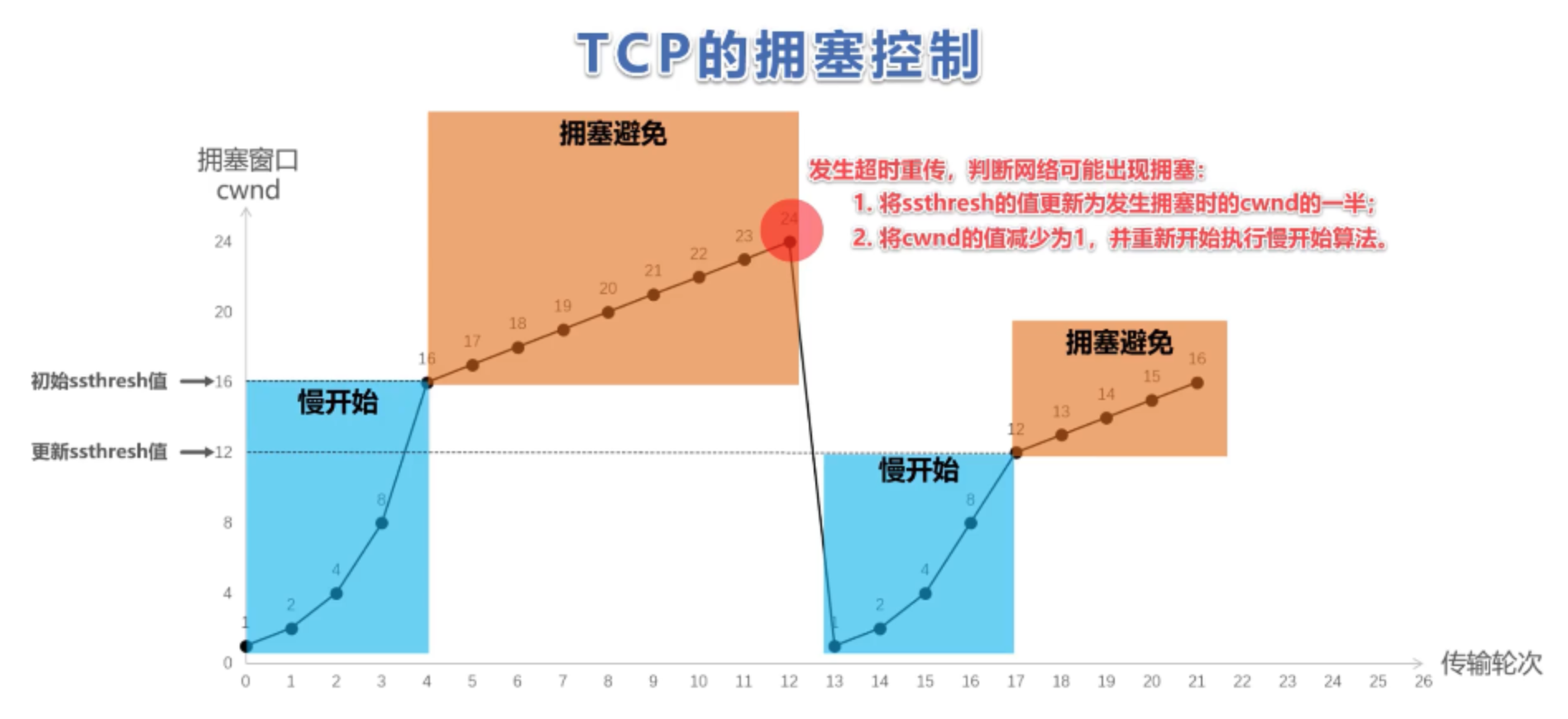
（2）A 点拥塞窗口变化是因为达到了慢开始门限 ssthresh，之后停止使用慢开始算法而采用拥塞避免算法； B 处收到了 3 个重复的确认，接下来执行快恢复算法；E点拥塞窗口变化是因为启动了快恢复算法。

（3）在 C 处收到了 3 个重复的确认，为预防网络出现拥塞，将拥塞窗口减小为原来的一半；在 D发生了超时，发送方设置的超时计时器时限己到但还没有收到确认，很可能是网络出现了拥塞,致使报文段在网络中的某处被丢弃， 因此拥塞窗口减小到 1，重新开始慢启动算法

1. 设 TCP 拥塞控制算法中，拥塞窗口的初始值为 1（报文段），慢开始阈值 ssthresh 的初始值为 8（报文段）。 当拥塞窗口 cwnd 上升到 14（报文段），网络发生超时，TCP 启用拥塞避免过程。 试分别计算 TCP 建立连接后第 1 轮到第 15 轮次的拥塞窗口 cwnd 大小（报文段），并要求写出计算过程。 （2012年-题3-6分）

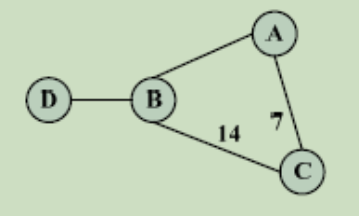
答：拥塞窗口达到慢开始阈值前，呈指数增长，达到阈值后，每一轮加 1，直到达到 14，发生拥塞， 慢开始阈值变为 7，拥塞窗口从1开始慢速增长，则建立连接后，第 1 轮到第 15 轮次的拥塞窗口 cwnd 大小如下表所示：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 传输轮次 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 拥塞窗口大小 | 1 | 2 | 4 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 1 | 2 | 4 | 7 | 8 |



题型4----路由选择和路由算法

1. 如下图所示的网络中，采用距离向量路由算法进行路由选择。假设路由器 C 在启动时，测得与相邻路由器 A、B 的时延分别为 7，14。此后，路由器 C 分别收到来自相邻路由器发出的路由向量： B(15，0，4，6)，A(0，3，12，16)。上述向量表示发送该向量的路由器分别与网络中路由器 A、B、C、D 之间的时 延。计算路由器 C 在收到相邻路由器发出的向量后，更新的路由表是什么？ （2008年-题4-4分）



解析：收到路由向量：A（0，3，12，16） B（15，0，4，6）， C 更新后的路由表（分别到 A,B,C,D 的路由向量）：（（7，A），（10，A），（0，－），（20，B））

|  |  |  |
| --- | --- | --- |
| C的路由表 | 距离 | 下一跳 |
| A | 7 | A |
| B | 14 | B |
| C | 0 | 直连 |
| D |  | - |

|  |  |
| --- | --- |
| B的数据 | 距离 |
| A | 15 |
| B | 0 |
| C | 4 |
| D | 6 |

|  |  |
| --- | --- |
| A的数据 | 距离 |
| A | 0 |
| B | 3 |
| C | 12 |
| D | 16 |

更新策略为，将C->A的距离加到A的数据的每一数据上，将C->B的距离加到B的每一个数据上

|  |  |
| --- | --- |
| B的数据 | 距离 |
| A | 15+14 |
| B | 0+14 |
| C | 4+14 |
| D | 6+14 |

|  |  |
| --- | --- |
| A的数据 | 距离 |
| A | 0+7 |
| B | 3+7 |
| C | 12+7 |
| D | 16+7 |

依次用原路由表和节点数据比较到某个节点的距离，如果新的距离比原来的距离近，则更新该条记录，并把下一跳改为该节点，否则不更新

C

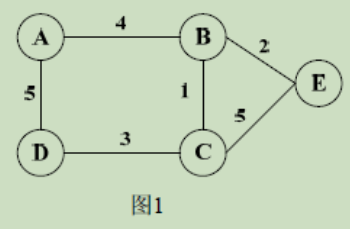
|  |  |  |
| --- | --- | --- |
|  | 距离 | 下一跳 |
| A | 7 | A |
| B | 10 | A（通过A的数据更新的） |
| C | 0 | 0 |
| D | 20 | B（通过B的数据更新的） |

评分说明：每答对到一个节点的路由的时延值得 0.5 分，答对输出线路得 0.5 分；若答案为（7，10，0，20）得 2 分

1. 如图 1 所示的网络中，每条链路边上的数字表示链路的开销。若采用距离向量算法进行路由选择， 第一次交换距离向量时，每个节点仅将初始的路由表告知其邻居节点，试写出：（2010年-题3-6分）

①节点 C 的初始路由表；

②第一次相邻节点之间交换距离向量后,节点 C 的路由表。(提示:路由表的基本信息包括目的节点,链路开销和下一跳节点)



C路由，初始距离向量表

|  |  |  |
| --- | --- | --- |
| 目标 | 开销 | 下一跳 |
| A |  | - |
| B | 1 | B |
| C | 0 | C |
| D | 3 | D |
| E | 5 | E |

C路由和相邻的B/D/E交互后。对应的相邻边变更为

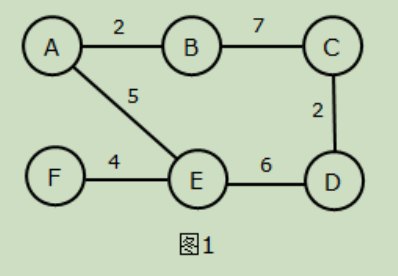
|  |  |  |
| --- | --- | --- |
| 目标 | 开销 | 下一跳 |
| A | 5 | B |
| B | 1 | B |
| C | 0 | C |
| D | 3 | D |
| E | 3 | B |

1. 如图 1 所示的网络中，采用距离向量算法进行路由选择。 (2017年-题3-6分)

（1）初始时，每个节点只知道到达相邻节点的距离，写出节点 E 的距离向量表（目标，开销，下一跳）

（2）第一次交换距离向量时，每个节点仅将初始时的路由表告知其相邻节点，试写出更新后节点 E 的距离向量表。

（3）当节点 F 到节点 E 的链路出现故障后，试分析距离向量算法可能出现的慢收敛问题。



解析：

①、E路由初始为

|  |  |  |
| --- | --- | --- |
| 目标 | 开销 | 下一跳 |
| A | 5 | A |
| B |  | - |
| C |  | - |
| D | 6 | D |
| E | 0 | 直连 |
| F | 4 | F |

②、交换一次后E的路由表信息如下：

|  |  |  |
| --- | --- | --- |
| 目标 | 开销 | 下一跳 |
| A | 5 | A |
| B | 7 | A |
| C | 8 | D |
| D | 6 | D |
| E | 0 | 直连 |
| F | 4 | F |

(3)网络阻碍，导致慢收敛问题：RIP 存在的一个问题是当网络出现故障时，要经过较长的时间才能将此信息传送到所有的路由器。

E 在收到 F 的报文更新之前，给（A 和 D）还发送原来的报文，我们拿 A 来看，因为此时 A 也不知道 F 也出了故障，

E 收到 A 的更新报文后，误认为经过 A 可以到 F，于是更新自己的路由表说，我到 F 的距离为 10，下一跳经过 A；

然后将此更新送给 A，A 又更新路由表说我到 F 距离 11，下一跳经过 E；就这样不断更新下去，直到 E 和 A 到 F 的

距离都增大到 16 时，E 和 A 才知道 F 是不可达的。于是这样好消息传播的快，坏消息传播的慢，网络出故障的传播

时间要经过较长的时间。这就是 RIP 协议的慢收敛问题。

解决方法：水平分割、毒性逆转、触发更新、抑制计时等（注：现在的路由器中都采用 OSPF 链路状态路由协议技术了）

（注 1：路由收敛：指从网络的拓扑结构发生变化到网络中所有路由设备中路由表重新保持一致的状态转换过程。

注 2路由环路，就是数据包不断在这个网络传输，始终到达不了目的地，导致掉线或者网络瘫痪。）

1. 假定网络中的路由器B的路由表有如下的项目（这三列分别表示“目的网络”、“距离”和“下一跳路由器”）

                 N1       7        A

                 N2       2        B

                 N6       8        F

                 N8       4        E

                 N9       4        F

现在B收到从C发来的路由信息（这两列分别表示“目的网络”“距离”）：

                 N2        4

                 N3        8

                 N6        4

                 N8        3

                 N9        5

试求出路由器B更新后的路由表（详细说明每一个步骤）。

 答：先把收到的路由信息中的“距离”加1：

N2        5

                N3        9

                N6        5

                N8        4

                N9        6

 路由器B更新后的路由表如下：

N1 7 A　　　　无新信息，不改变

N2 5 C　　　　相同的下一跳，更新

N3 9 C　　　　新的项目，添加进来

N6 5 C　　　　不同的下一跳，距离更短，更新

N8 4 E　　　　不同的下一跳，距离一样，不改变

N9 4 F　　　　不同的下一跳，距离更大，不改变

1. 假定网络中的路由器A的路由表有如下的项目（格式同上题）：

           N1         4          B

           N2         2          C

           N3         1          F

           N4          5         G

   现将A收到从C发来的路由信息（格式同上题）：

           N1          2

           N2          1

           N3          3

           N4          7

试求出路由器A更新后的路由表（详细说明每一个步骤）。

 答：先把收到的路由信息中的“距离”加1：

N1          3

           N2          2

           N3          4

           N4          8

路由器A更新后的路由表如下：

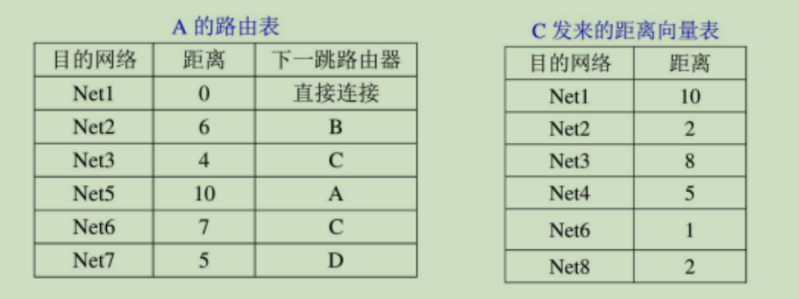
N1 3 C　　　　不同的下一跳，距离更短，改变

N2 2 C　　　　不同的下一跳，距离一样，不变

N3 1 F　　　　不同的下一跳，距离更大，不改变

N4 5 G　　　　不同的下一跳，距离更大，不改变

1. 某网络采用 RIP 路由协议，当路由器 A 收到从路由器 C 发来的距离向量时，试问 A 的路由表将发生怎样的变化？试画出路由器 A 新的路由表。 （2014年题3）



解析：首先，将 A 的路由表中下一跳路由器为 C 的目的网络的距离更新为 C 发来的距离向量表中的距离加 1，

如 C 发来的距离向量表中没有该目的网络，则删除该项；然后，从 C 发来的距离向量表中找出 A 的路由表中没有的

目的网络，并将其添加到 A 的路由表中，距离为 C 发来的距离向量表中相应的距离加 1，下一跳路由器设置为 C；

最后，将 C 发来的距离向量表中剩下的目的网络的距离加 1 后与 A 的路由表中相应目的网络的距离比较， 如小于

原 A 的路由表中的距离， 则将 A 的路由表中此目的网络的距离改为 C 发来的距离向量表中该网络的距离加 1，并

将 A 的路由表中该目的网络的下一跳路由器设置为 C，否则不作修改；A 的路由表中的其他项不作修改。

经上述操作，A 的路由表如下：

|  |  |  |
| --- | --- | --- |
| 目的网络 | 距离 | 下一跳路由器 |
| NET1 | 0 | 直接连接 |
| NET2 | 3 | C |
| NET3 | 9 | C |
| NET4 | 6 | C |
| NET5 | 10 | A |
| NET6 | 2 | C |
| NET7 | 5 | D |
| NET8 | 3 | C |

1. 某网络采用 RIP 路由协议，当路由器 A 收到从路由器 C 发来的距离向量时，试问： （2012年-题2-5分）

（1）A 的路由表将发生怎样的变化？试画出路由器 A 新的路由表。

（2）随后 A 收到两个分别发往 Net4 和 Net6 的数据报，A 将怎样转发？



解析（1）RIP 路由协议，当路由器 A 收到从路由器 C 发来的距离向量时，将 C 发来的距离向量路由表中与目的网络 的距离加 1，然后与路由器 A 原来的路由表中相应目的网络的举例进行比较，如原路由表中目的网络的下一条为 C， 则将其距离改为计算得到的距离，对于原来下一条路由器不是 C 的，如计算得到的距离小于原路由表中的距离，则 将该目的网络对应的下一条地址改为 C，并对距离进行替换，如原路由表中没有该目的网络，则将其添加进路由表， 并将下一条地址设为 C，对路由表中的其他项不做修改，得到的路由表如下：

|  |  |  |
| --- | --- | --- |
| 目的网络 | 距离 | 下一跳路由器 |
| NET1 | 0 | 直接连接 |
| NET2 | 3 | C |
| NET3 | 1 | C |
| NET4 | 4 | C |
| NET5 | 4 | C |
| NET6 | 5 | D |
| NET7 | 6 | B |
| NET8 | 2 | D |

②、当路由器 A 收到发往 Net4 的数据报后，将其转发给路由器 C，收到发往 Net6 的数据报后，将其转发给路由器 D。

1. 在图 1 所示的网络中，主机 H\_A、主机 H\_B、路由器 R\_1 和路由器 R\_2 的各端口的 IP 地址和 MAC 地址

分别表示为(MAC 地址，IP 地址)的形式，即有：H\_A(MAC\_A ,IP\_A),H\_B(MAC\_B, IP\_B), R\_1 的端口11（MAC\_11,IP\_11）

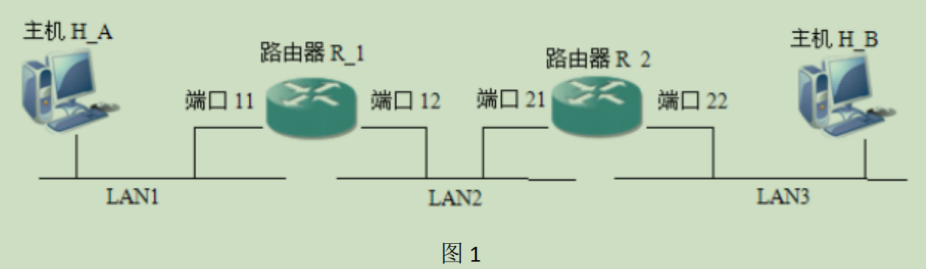
, R\_1 的端口 12（MAC\_12，IP\_12）,R\_2 的端口 21（MAC\_21，IP\_21），R\_2 的端口 22（MAC\_22，IP\_22）。 （2013年题4-6分）

试回答问题：

① 主机 H\_A 向主机 H\_B 发送数据，最多需要使用多少次 ARP 协议？简要说明理由。

② 主机 H\_A 向主机 H\_B 发送数据，试分别写出路由器 R\_1 的端口 11 收到的数据单元以及路由器 R\_2 的端口 22

转发的数据单元中，数据链路层协议首部的地址字段和网络层协议首部的地址字段内容。



答：（1）共需 3 次，主机 A 先通过 arp 得到第 1 个路由器的 MAC，第 1 个路由器通过 arp 得到第 2 个路由器的 MAC，

第 2 个路由器将 IP 包发给主机 B 前仍要通过 ARP 得到主机 B 的 MAC，共 3 次。

在整个传输中，IP 数据报报头的源和目的 IP 地址都不会发生变化，只要跨网段了（跨广播域）源和目的 MAC 地址 肯定是要变化的，且目的 MAC 地址是下一跳的 MAC 地址。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 网络层报头 | | 链路层MAC报头 | |
|  | 源IP地址 | 目的 IP 地址 | 源 MAC 地址 | 目的 MAC 地址 |
| 主机 H\_A 到端口 11 | IP\_A | IP\_B | MAC\_A | MAC\_11 |
| 端口 12 到端口 21 | IP\_A | IP\_B | MAC\_12 | MAC\_21 |
| 端口 22 到主机 H\_B | IP\_A | IP\_B | MAC\_22 | MAC\_B |

题型5---------TTL计算（段的最大生命周期）

1. 设计一个传输层的协议，其序号为 4 位，最大报文段长度为 512 字节，段的最大生存期为 60 秒。 试问每个连接的最大数据率是多少？（2013年题3）

解：序号为 4 位，则每个连接最多发送 4=16 个报文段，则每次连接可传送的最大数据量为 16x512B=8192B=8KB，

则每个连接的最大数据率为 8KB/60s=0.13KB/s.

1. 假设一台主机将500字节的应用层数据给传输层进行处理，序列号为4位，最大的TPDU 生存周期是30秒。 (考虑传输层头部20字节) 若使序列号不回绕，该线路的最大数据率是多少? （2007题5）

答：序列号4 位，不回绕可以编号16 个TPDU ，在30 秒内16 个TPDU 共：（500+20）\*16=8320Byte ，

数据率： 8320\*8/30=2.2kbps

注：TPDU,全称 Transport Protocol Data Unit，是指传送协议数据单元。代表从一个传输实体发送至另一个传输实体的消息。

题型6---子网划分（选择填空题常考）

1. 某单位内有4 个局域网通过一台四个端口的路由器（支持可变长子网掩码VLSM）连接， 一个端口连接 一个局域网， 每个局域网的主机数分别是120 台、60 台、26 台、25 台。该单位已拥有一个C 类IP 地址 198.101.116.0/255.255.255.0, 试合理分配IP 地址并给出每一个局域网的IP 地址范围和子网掩码。 （2005-5题-4分）

答：每个部门分配一个子网，名义上部门A 、B、C、D 的子网大小分别是：

（=128）， （=64）， （=32）和 （=32）

IP 地址的最高位是0表示子网A，最高两位是10表示子网B，最高三位是110表示子网C，最高三位是111 表示子网D。

显然这里采用了可变长子网掩码,涉及3 种子网掩码,分别是255.255.255.128;255.255.255.192; 255.255.255.224

因此IP 地址范围和子网掩码分配方式如下：

192.101.116.1~126 /255.255.255.128

192.101.116.129~190 /255.255.255.192

192.101.116.193~222 /255.255.255.224

192.101.116.225~254 /255.255.255.224

题型7---其他类型简答题

1. (3 分）试说明以太网规定的最短帧长是多少？为什么要限制最短帧长？ （2009年-题1-3分）

答：以太网定义最短帧长为 64 字节（1 分）。 最短长度的限制与以太网 MAC 层的CSMA/CD 协议有关（1 分）。

以太网在发送数据帧时能够检测到冲突并停止发送。如果帧长度过短，在检测到冲突之前帧已经发送完毕，则协议无法进行有效冲突检测（1 分）。

1. 试说明 TCP 协议是如何提供端到端可靠的传输服务的？ （2009年-题2-3分）

答：TCP 协议是面向连接的协议（1 分）；

可靠建立连接（也可答三次握手建立连接）和终止连接（1 分）；

采用滑动窗口协议进行流量控制和差错控制（1 分）。

1. 以太网交换机在初次使用时， 其转发表是空的， 试说明交换机如何建立自己的转发表。（2007年-题1-3分）

S答：交换机初始状态下的转发表示空的（一个全新的交换机的MAC地址表是空的），这个表是通过自学习，一点一点学习到的，当端口1收到一个要求转发MAC地址为A的帧的时候，交换机将广播到出端口1以外的所有端口。当MAC地址为A 的设备响应了这个包以后，交换机会记录下这个设备的MAC和端口的对应关系（所以这个时候就是学习的过程，得到的响应的包的源mac地址和相应的端口去记录mac地址表）。等到下一次再接收到请求MAC地址为A的帧的时候，交换机不再广播，直接转发到对应端口上去。交换机每次接受数据帧的时候是根据源MAC地址去查交换机本身的MAC地址表，如果没有就会泛洪给出发送口的所有接口，总之建立MAC地址表是根据数据帧的源MAC地址去学习。

以太网交换机的主要功能：

  1、学习：以太网交换机了解每一端口相连设备的MAC地址，并将地址同相应的端口映射起来存放在交换机缓存中的MAC地址表中。

2、转发/过滤：当一个数据帧的目的地址在MAC地址表中有映射时，它被转发到连接目的节点的端口而不是所有端口(如该数据帧为广播/组播帧则转发至所有端口)。

3、消除回路：当交换机包括一个冗余回路时，以太网交换机通过生成树协议避免回路的产生，同时允许存在后备路径。

注意：这里以太网交换机学习的时候是通过的源mac和相应的端口去建立映射地址表，但是转发是通过目的mac地址，去查找mac地址表去转发，这两个需要区别对待

1. 试说明防火墙的工作原理。 （2007年-题2-3分）

答：防火墙是由软件、硬件构成的系统，是一种特殊编程的路由，用来在两个网络之间实施接入控制策略。 接入控制策略是由使用防火墙的单位自行制订的，为的是可以最适合本单位的需要。防火墙系统决定了哪些内部服务可以被外界访问；外界的哪些人可以访问内部的服务以及哪些外部服务可以被内部人员访问。防火墙必须只允许授权的数据通过。 https ftp

1. 网络中拥塞产生的原因是什么? 如何进行拥塞控制? （2007年-题3-3分）

S答：1）发生拥塞的原因：资源(带宽、交换节点的缓存、处理机)的需求大于可用资源。

2）拥塞控制：处理网络拥塞现象，考虑网络能够承受现有的网络负荷，防止过多的数据注入到网络，使网络中的

路由器或链路不致过载，确保通信子网可以有效为主机传递分组。

3）因特网建议标准RFC2581定义了拥塞控制的四种算法：慢开始（Slow-start)，拥塞避免（Congestion Avoidance)，

快重传（Fast Restrangsmit)和快恢复（Fast Recovery）。

注：对比流量控制和拥塞控制（（Flow Control & Congestion Control）

相同：提高网络性能。

不同：1）流量控制：在TCP连接上实现对发送流量的控制，考虑点对点之间对通信量的控制，端到端，即：控制发送端 的数据发送速率，使接收端可以来得及接收，保证网络高效稳定运行。 （方法：滑动窗口）

1. 拥塞控制：处理网络拥塞现象，考虑网络能够承受现有的网络负荷，全局性变量，涉及所有的路由器、主机以及与降 低网络传输性能有关的因素。防止过多的数据注入到网络，使网络中的路由器或链路不致过载，确保通信子网可以有效 为主机传递分组。（方法：慢启动、拥塞避免（ssthrelod为窗口大小的一半）、快重传（收到3个以上的重复的ACK即开始重传）、快恢复）
2. 简述以太网设备二层交换机与三层交换机的区别。 （2005年-题1-3分）

答1： 二层交换技术是发展比较成熟，二层交换机属数据链路层设备，可以识别数据包中的MAC 地址信息，根据MAC地址 进行转发，并将这些MAC 地址与对应的端口记录在自己内部的一个地址表中。二层交换机用于小型的局域网络。在 小型局域网中， 广播包影响不大， 二层交换机的快速交换功能、多个接入端口和低谦价格为小型网络用户提供 了很完善的解决方案。

三层交换机的最重要的功能是加快大型局域网络内部的数据的快速转发，加入路由功能也是为这个目的服务的。

如果把大型网络按照部门，地域等等因素划分成一个个小局域网，这将导致大量的网际互访， 单纯的使用二层交 换机不能实现网际互访； 如单纯的使用路由器，由于接口数量有限和路由转发速度慢， 将限制网络的速度和网络 规模， 采用具有路由功能的快速转发的三层交换机就成为首选。

答2：二层交换机：技术发展成熟，属于数据链路层设备，可以识别MAC 地址，根据MAC地址进行数据转发， 同时 将MAC地址与对应端口记录在内部的MAC 地址表中； 多用于小型局域网络，交换速度快，多端口接入，价格低廉。

三层交换机：工作在网络层，具有路由功能，识别IP 地址,可以加快大型局域网络内部数据的快速转发。具有二层交换机和路由器的双重功能。

1. 说明传输层协议TCP 在建立连接时为什么要使用三次握手。 （2005年-题2-3分）



答1：为确保连接的建立和终止都是可靠的，TCP使用三次握手的方式，科学家们已证明三次握手是在包丢失、重复 和延迟的情况下确保非模糊协定的充要条件。

答2：TCP连接的三次握手是确保连接的建立和终止的可靠保证,TCP三次握手方式，科学家们证明是在包丢失、重复和延迟的情况下确保非模糊协定的充要条件。

1. 使用电话线拨号方式传输1M 字节大小的文件， 其中Moden 的数据传输率为2400bps. 若以异步方式传送，采用1 位起始位和1 位停止位，则最少需要多少时间（以秒为单位）才能将该文件传输完毕？

（假设线路传播延迟、误码率、网络层以上开销均忽略不计） （2005年-题4-4分）

注：以异步方式传输1个字节数据，需加1 位起始位和1 位停止位，实际传送10位。

1. 简述TCP/IP 网络体系结构，并说明各层的主要协议和各层的主要功能。 （2004年-题1-3分）

答： TCP/IP 网络体系结构如下图所示，包括应用层、运输层、互连网络层和网络接口层。

网络接口层负责从主机或节点接收IP 分组，并把它们发送到指定的物理网络上，物理网络通常包括OSI 的物理层

和数据链路层。互连网络层定义了标准的分组格式和协议，即IP 协议。互连网络层的功能就是把IP 分组发送到应 该去的地方。选择分组路由和避免阻塞是这里主要的设计问题。

运输层在TCP/IP 模型中位于互连网络层之上，它的功能相当于OSI 的运输层。这里定义了两个端到端的协议。第 一个是传输控制协议TCP。它是一个面向连接的协议，允许从一台机器发出的字节流无差错地发往互联网上的其他 机器。TCP还要处理流量控制，以避免快速发送方向低速接收方发送过多报文而使接收方无法处理。第二个协议是 用户数据报协议UDP（ User Datagram Protocol ）。它是一个不可靠的、无连接协议，用于不需要TCP的排序和流 量控制能力而是自己完成这些功能的应用程序。应用层包含所有的高层协议（相当于OSI 的应用层、表示层和会话 层）。最早引入的是虚拟终端协议（ TELNET）、文件传输协议（ FTP）和简单邮件传输协议（ SMTP）。再后来的 发展又增加了不少协议，例如域名系统服务DNS（ domain name service ）用于把主机名映射到网络地址， HTTP

协议用于在万维网（ WWW）上获取主页等。

1. 简述HTTP 协议的特点和工作过程。 （2004年-题2-3分）

答： HTTP 是传送信息的协议，从层次的角度看， HTTP 是面向事务的应用层协议。虽然HTTP 使用了TCP ，但HTTP 协议是无连接的，也是无状态的，这样可使读取网页信息完成得较迅速。从HTTP 的观点来看，万维网浏览器就是 一个HTTP 客户，而在万维网服务器等待HTTP 请求的进程常称为HTTP 守护程序。HTTP 守护程序在收到HTTP 客户 的请求后，经过一些必要的处理，将所需的文件返回给HTTP 客户。简单的情况就是用户代理与服务器直接建立一 个TCP 连接。客户先发起TCP 连接，在和服务器建立了TCP 连接后就发送HTTP 请求。这个请求包括一个特定的命

令，一个URL ，和一个“类MIME ”报文，它包括一些请求参数和客户自身的信息， 。当服务器收到请求后，就试 图完成所请求的动作，接着就返回HTTP 响应。响应包括状态信息，成功或出错代码，一个类MIME 报文，包括有 关服务器的信息和响应信息。接着就释放TCP 连接。

1. 一个以太网速率从10Mbps 升级到100Mbps，满足CSMA/CD 冲突域条件，为使正常工作,需做哪些调整？为什么？ （2004年-题3-3分）

答：由于10BASE-T 证明比10BASE2 和10BASE5 具有更明显的优越性，因此所有的快速以太网系统都使用集线器 （ Hub），而不采用同轴电缆。100BASE-T MAC 与10Mbps 经典以太网MAC 几乎完全一样， 惟一不同的参数就是帧 际间隙时间， 10Mbps 是9.6 μs（ 最小值），快速以太网（ 100Mbps）是0.96 μs（最小值）。另外为了维持最 小分组尺寸不变，需要减少最大冲突域直径。所有这些调整的主要原因是因为速率提高到了原来的以太网的10 倍。

1. 试述TCP 连接释放的过程。 （2003年-题2-4分）



四次挥手

1. 某网络有50 个IMP 结点，用8 位二进制数来记录交换的延迟时间，每秒交换4次，问分布式路由算法 对每条（全双工）线路要耗费多大带宽？ （2003年-题3-4分）

答：路由表为400bit，每秒交换该路由4次表，分布路由算法每条（全双工）线路要耗费1600b带宽/s。

1. 试述FTP 的工作原理。 （2003年-题4-4分）

答：在FTP客户/服务器模式下工作， 一个FTP服务器可以同时为多个客户提供服务，它总是等待客户系统向它提供

服务请求，工作过程如下：

（1）服务器打开端口（21）等待客户发连接请求，客户端可以用分配的任意一个本地端口号与服务器的21端口联 系，这个过程称为主进程。

（2）客户请求到来时，服务器启动从属进程来处理客户端发来的请求。

（3）主进程返回，继续等待接收端发来的请求，与从进程并行工作。

在客户和服务器传送文件的过程中，有两个进程：控制进程和数据传送进程。

1. 试述公开密钥算法的特点和使用公开密钥密码体制的加密/解密过程。 （2003年-题5-5分）

答：公开密钥算法的特点是， 加密密钥（即公开密钥） 是公开的，而解密密钥（即秘密密钥）是需要保密的。 加密算法和解密算法也都是公开的。虽然秘密密钥是由公开密钥决定的，但却不能根据公开密钥计算出来。 公开密钥算法的优点是解决了公钥传输问题， 且加密内容不易被破解， 缺点是算法运算速度慢。

公开密钥密码体制的加密/解密过程：首先，任何想要接收秘密报文的个人或单位要设计两个算法，即 E 和 D。这两 个算法应满足下述三个条件:（1）如果在一个加密的报文 E(P)上应用 D，即可得到明文;（2）从 E 导出 D 极其困难

1. 使用“已知明文”的攻击方法不能破译出 E。然后，公开加密算法 E（或密钥）。要公开密钥只需把加密算法 放在一个任何人都可以读的文件中即可。
2. 在 OSI 参考模型中，数据链路层和网络层的协议数据单元(PDU)分别是什么?它们之间的封装关系是什么? （2006年-题1-3分）

解析：“分组”(packet)也就是“包”，它是一个不太严格的名词，意思是将若干个比特加上首部的控制信息就封装在 一起，组成一个在网络上传输的数据单元。在数据链路层这样的数据单元叫做“帧”。而在 IP 层（即网络层）这样 的数据单元就叫做“IP 数据报”。IP 数据报在数据链路层被封装成数据帧进行传输。OSI 为了使数据单元的名词准确，

就创造了“协议数据单元”（PDU）这一名词。在数据链路层的 PDU 叫做 DLPDU，即“数据链路协议数据单元”。在网 络层的 PDU 叫做“网络协议数据单元”（NPDU）。

注：PDU 是指将若干比特加上首部的控制信息封装在一起，组成一个在网络上传输的数据单元，

数据链路层的 PDU 是帧，网络层是 IP 数据报（分组）；IP 数据报在数据链路层被封装成数据帧进行传输。11 / 36

1. 简述同步传输与异步传输的区别以及各自的适用环境。 （2006年-题2-3分）

解析：异步传输时，被传送的数据编码成一串脉冲。传送一个 ASCII 字符（每个字符有 7 位）的格式如图 9.1 所示，

首先发送起始位，接着是数据位、奇或偶校验位，最后为停止位。

其中，第 1 位为起始位（低电平“0”），第 2～8 位为 7 位数据（字符），第 9 位为数据位的奇或偶校验位，

第 10～11 位为停止位（高电平“1”）。停止位可以用 1 位、1.5 位或 2 位脉宽来表示。因此，一帧信息由 10 位、 10.5 位或 11 位构成。异步传输就是按照上述约定好的固定格式，一帧一帧地传送。由于每个字符都要用起始位和 停止位作为字符开始和结束的标志，因而传送效率低，主要用于中、低速通信的场合。

同步传输时，用 1 个或 2 个同步字符表示传送过程的开始，接着是 n 个字符的数据块，字符之间不允许有空隙。

发送端发送时，首先对欲发送的原始数据进行编码，如采用曼彻斯特编码或差动曼彻斯特编码，形成编码数据后再 向外发送。由于发送端发出的编码自带时钟，实现了收、发双方的自同步功能。接收端经过解码，便可以得到原始 数据。在同步传输的一帧信息中，多个要传送的字符放在同步字符后面，这样,每个字符的起始、停止位就不需要了， 额外开销大大减少，故数据传输效率高于异步传输，常用于高速通信的场合。但同步传输的硬件比异步传输复杂。

**注：异步传输**：被传送的数据编码成一串脉冲，传送一个 ASCII 字符的格式时，首先发送起始位，接着是数据位、奇偶校验位，停止位。异步传输 就是按照这种约定好的固定格式，一帧一帧的传送， 由于每个字符都要用起始位、停止位，因而传送效率低，主要用于中低通信的场合；

**同步传输**：用 1 个或 2 个同步字符表示传送过程的开始,接着是 n 个字符的数据块，字符之间不允许有空隙,发送端发送时，

首先对欲发送的原始数据进行编码再向外发送。 由于发送端发出的编码自带时钟，实现了收、发双方的自同步功能。

接收端经过解码，便可以得到原始数据。这时每个字符的起始、停止位不需要了，额外开销大大减少，故数据传输效率 高于异步传输，常用于高速通信的场合。但硬件也相对复杂。

1. **简单网络管理协议 SNMP 采用的传输层协议是什么? 为什么采用该传输层协议? （2006年-题3-3分）**

**解析：**SNMP 的通信基础是 TCP/IP 协议,它利用了传输层上的用户数据报协议(UDP). SNMP 定义为依赖于 UDP 数据报 服务的应用层协议,SNMP 实体向管理应用程序提供服务,它的作用是把管理应用程序的服务调用变成对应的 SNMP 协议数据单元,并利用 UDP 数据报文发送出去。之所以选择 UDP 协议而不是 TCP 协议,是因为 UDP 效率较高,这样 实现网络管理不会太多地增加网络负载。但由于 UDP 不可靠,所以 SNMP 报文容易丢失,为此,对 SNMP 实现是将每个 管理信息装配成单独的数据报独立发送,而且报文较短,不超过 484 字节.

解答：SNMP 使用 UDP 传送报文。由于与 TCP 相比，UDP 协议简单，在每个系统中运行时网络负载很轻，故有利于

数据的高速传送，并减少管理交通对网络带宽的消耗。另一方面，尽管 UDP 不保证传输的可靠性，但由于 SNMP

协议通常都结合进轮询机制，即使偶尔有报文传输错误发生，下一次命令不久又会到达，错误能够被纠正。

**注：**SNMP 的通信基础是 TCP/IP 协议，它利用了传输层上的 UDP 协议。SNMP 实体向管理应用程序提供服务，并利用 UDP 数据报文发

送出去，选择 UDP，是因为 UDP 数据传送效率较高，这样实现网络管理不会太多增加网络负载，但由于 UDP 不可靠，所以 SNMP 容

易丢失，为此，对 SNMP 实现是将每个管理信息装配成单独的数据报独立发送，且报文较短，不超过 484 字节。

网络安全

主动攻击：篡改（更改报文流），恶意程序（病毒程序），拒绝服务（发送大量分组，致使服务器瘫痪）——可检测（加密+鉴别）

被动攻击：截获（流量分析，窃听）——检测不出来（加密）

分布式拒绝服务（DDOS）：从很多网站攻击一个网站

计算机网络通信安全的目标：

1、保密性（信息内容保密）

2、端点鉴别（发送方与接收方的鉴别）

3、信息的完整性（信息未被篡改）

4、运行的安全性（规定用户访问权限，访问控制）

密码学：密码编码学+密码分析学

两类密码体制：对称密钥密码体制+公钥密码体制

对称密钥密码体制：加密密钥=解密密钥

公钥密码体制：加密密钥与解密密钥不相同

数字签名：

1、 报文鉴别

2、 可防伪

3、 不可否认

加密与数字签名的区别：加密——接收方的公钥加密，接收方的私钥解密。数字签名——发送方的私钥加密，发送方的公钥解密。

网络层、运输层、应用层的网络安全协议

防火墙：软硬件结合的系统，特殊的路由器，有阻止与允许两个功能，大部分是阻止，解决外联网与内联网的网络安全问题，是一种访问控制策略。分为分组过滤路由器与应用网关代理服务器两种，前者主要应用在网络层与运输层，后者主要应用在应用层，后者是鉴别高层用户。

入侵检测：在已经发生入侵，检测入侵，将入侵的伤害降到最小

两种入侵检测的方法：基于特征的入侵检测+基于异常的入侵检测

名称解析

