**计算机网络第二次作业**

1. **请说明介质访问控制（MAC）子层的作用，并说明在什么网络环境中需要使用MAC子层协议？**

* MAC子层的作用:解决当局域网中共用信道的使用产生竞争时，如何分配信道的使用权问题。用来确定多路访问信道下一个使用者。
* 使用的网络环境：早期的总线以太网、局域网以及其他使用广播信道方式发送数据的网络。

1. **请说明CSMA/CD（带冲突检测的载波侦听多路访问）的含义。**

**Carrier Sense Multiple Access with Coiision Detection**

* CS：载波监听，每一个站在发送数据之前以及发送数据时都要检测一下总线上是否有其他计算机在发送数据。
* MA：多点接入，表示允许多个计算以多点接入的方式连接在同一根总线上，总线型网络。
* CD：碰撞检测，“边发送边监听，适配器边发送数据边检测信道上的信号电压变化情况，以便判断自己在发送数据时其他节点是否也在发送数据。

1. **经典以太网（Classic Ethernet）和交换型以太网（Switched Ethernet）的数据链路层协议有什么不同？**

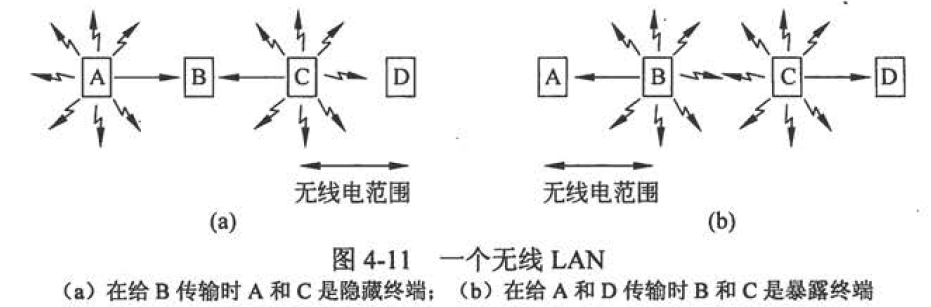
在经典以太网中，由于所有的电脑都都连接在一根总线上存在冲突域，所以需要使用1-坚持CSMA/CD协议来控制对总线的使用。

在交换行以太网中，所有的电脑连接在交换机上，通过交换机传输数据，没有冲突域，所以不需要使用1-坚持CSMA/CD协议

1. **请描述WLAN网络中隐藏终端（Hidden Terminal）问题和暴露终端（Exposed Terminal）问题的含义。**

隐藏终端问题：

假设A向B发送一个数据，由于A未在C的监测范围之内，C没有检测出A正在给B发送数据，因此C也将数据发送给B，由于两个基站同时给B发送数据，从而导致信号冲突，带宽资源浪费。这个问题称为隐藏终端问题。



暴露终端问题：

B正在向A传输数据，同时C想要给D传输数据，C监听介质发现有一个传输在进行，从而得出自己不能向D发送数据，而其实际上C监听到的传输只会破坏B和C的传输，不会破坏C和D的传输。这个问题称为暴露终端问题。

1. **经典以太网和WLAN网络中的介质访问控制子层协议有什么不同？**

经典以太网使用的MAC协议为 CSMA/CD；WLAN网络使用的MAC协议为CSMA/CA.

CSMA/CD与CSMA/CA的不同之处：

1. 载波检测方式不同：由于传输介质不同，因此CSMA/CD通过电缆中的电压变化来检测，当数据发生碰撞时，电缆中的电压会随之发生变化；而CSMA/CA采用能量检测、载波检测、和能量载波混合检测三种方式检测信道空闲。
2. CSMA/CD检测冲突，CSMA/CA避免冲突，二者出现冲突后都会进行有上限重传。

CSMA/CA工作原理：

发送数据前先检测信道是否空闲，空闲则发出RTS，接收端收到RTS后，发送响应信息CTS，发送端接受到CTS后，开始发送数据，同时预约信道，接收端接收到数据帧后，用CRC检验数据是否正确，正确则相应ACK帧，发送方接受到ACK进行下一个数据帧的发送，若没有则重新发送。

1. **请说明网桥（Bridge）、交换机（Switch）转发帧的工作原理，并说明什么是学习型网桥（Learning Bridge）。**
2. 网桥转发帧工作原理：

接收来自集线器的数据帧，从帧头取出帧的目的MAC地址，如果目的MAC地址和源MAC地址为同一个局域网中，则丢弃，如果不同则将帧先储存然后查找站表，找到对应网段的端口号，然后发送出去。

1. 交换机转发帧的工作原理：（交换机有三种转发数据帧的方式）：

* 直通交换方式：是指交换机在收到数据帧后，不进行缓存和校验，而是直接转发到目的端口
* 存储转发方式：交换机首先在缓冲区中存储接收到的整个数据帧，然后进行CRC校验，检查数据帧是否正确，如果正确，再进行转发。如果不正确，则丢弃。
* 碎片隔离转发：交换机在接收数据帧时，会先缓存数据帧的前64个字节，确保数据帧大于64个字节，再进行转发。

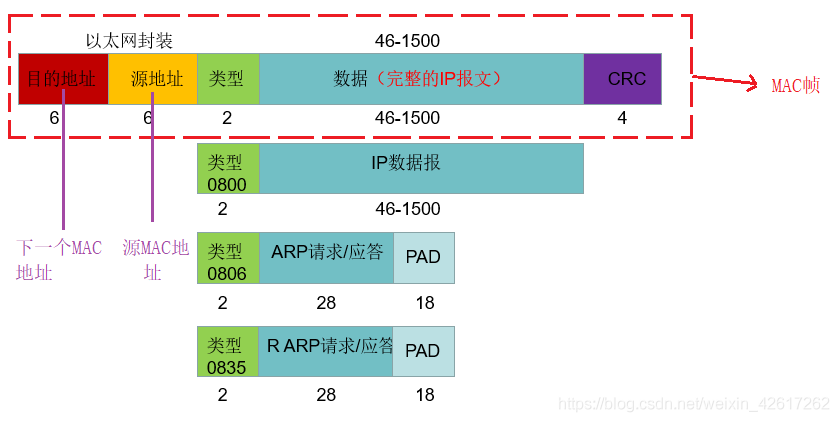
1. 学习型网桥：

对于每个发向未知目的地址的入境帧，网桥会把这个数据包广播到除了源端口以外的所有端口，目的主机收到广播后，就会把自己的MAC地址送回给网桥，网桥就知道了这个设备在这个端口上，并且把这个信息记录到转发表。随着时间的推移网桥会学习到每个目标地址对应的端口，之后每接受到一个数据帧，就通过对应的端口发送，而不是广播发送。

1. **能否在以太网的帧中携带IPv6分组（IPv6 Packet）？请解释说明其中的原因？**

**可以：**

以太网帧可以携带IPv6分组，在以太网帧中IP报文长度限制为：46-1500。只要IPv6分组的长度大于46字节，小于1500字节就可以被以太网的帧携带。



1. **请说明下列协议、标准的作用：HDLC、DHCP、ARP、STP（Spanning Tree Bridges）、IEEE 802.1Q 标准**
2. HDLC协议：

一种面向比特的高效链路层协议。HDLC通信协议IP核为三个部分，即外部接口模块、数据发送部分和数据接收部分。 在这类面向比特的数据链路协议中，帧头和帧尾都是特定的二进制序列， 通过控制字段来实现对链路的监控，可以采用多种编码方式 实现高效的、可靠的透明传输。故其最大特点是不需要数据必须是规定字符集，对任何一种比特流，均可以实现透明的传输。

1. DHCP协议：Dynamic Host Configuration Protocol

动态主机配置协议，应用层协议，使用客户/服务器通过广播的方式进行交互，基于UDP。DHCP提供即插即用联网的机制，主机可以从服务器动态获取IP地址、子网掩码、默认网关、DNS服务器名称与IP地址，允许地址重用，支持移动用户加入网络，支持在地用地址续租。

1. ARP协议：address resolution protocol

地址解析协议，根据IP地址获取目标物理地址的一个协议。主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址，收到返回消息后将该IP地址和物理地址存入本机ARP缓存中保留一定时间，下次请求时直接查询ARP缓存。

1. STP协议：

生成树协议，是用于在局域网中消除数据链路层物理环路的协议，通过在桥之间互相转换BPDU，来保证设备完成生成树的计算过程，防止二层网络的广播风暴的产生。

1. IEEE 802.1Q 标准：

标准化VLAN实现方案，目的是使得一组逻辑上的设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中。

1. **在以太局域网中，一个主机配置有两种地址：MAC地址、IP地址。请说明在以太局域网的设计中，为什么不能仅使用IP地址，还必须使用MAC地址？**

在早期的以太网中，以太网内通过MAC地址通信，但是随着以太网发展变为互联网时，MAC地址本身的缺陷就暴露了出来，**MAC地址虽然唯一但是不能表明用户在整个互联网中的位置**，除非维护一个超级大MAC地址对应表，那寻址效率非常低下，而且会占用极大的存储空间，另外获取MAC地址是通过ARP协议来完成的，如果用MAC地址通信，那么广播风暴是个难题。

因此IP地址被发明了出来并解决了这个问题，因为IP地址是网络提供商给你的，所以你在哪里整个网络都是知道的。IP地址前几位用于锁定目的主机所在网络，后几位用于确定目的主机是网络中具体的哪一台设备。而由于IPv4地址的个数有限，所以有私网地址的概念以及NAT技术。因为不同网络的不同主机可以使用相同的私网IP地址，所以IP地址无法唯一标识一台设备，这个时候就得靠MAC地址。

1. **数据报网络（Datagram Network）和虚电路网络（Virtual-circuit Network）有哪些不同之处？**

主要为两种网络发送数据分组的方式不同：

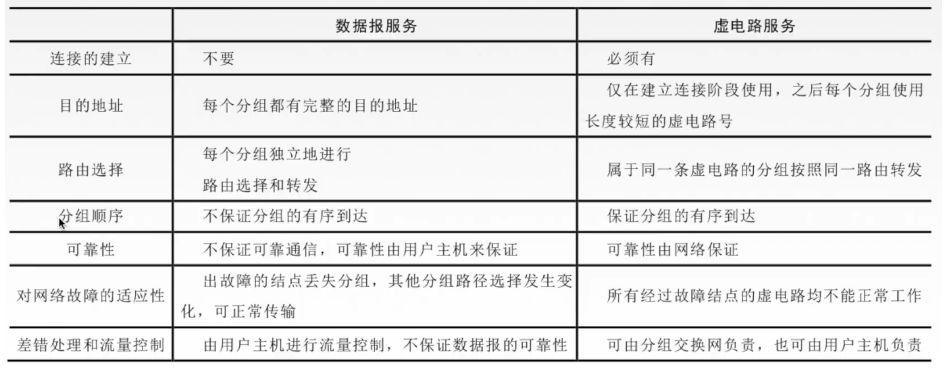
* 数据报网路：

源主机与目的主机通信之前不事先为数据分组的传输确定路径，源主机将数据分组进行**独立发送**到目的主机，在发送过程中各个分组各自行走自己的路线，所传送的分组可能出错、丢失、重复和失序（即不按顺序到达终点），属于不可靠交付。

路由器需要构建转发表，来根据分组的目的地址转发分组。

* 虚拟电路网络：

源主机在通信之前会事先与目的主机**建立一条通道**，数据分组都将沿着这条线路有序可靠的传输，属于可靠交付。



1. **计算机网络中的网络层中的转发（Forwarding）和路由（Routing）有何不同？**
   1. 转发是一个节点在本地执行的一个相对简单的过程，即报文从设备的一个端口进入而从另一个端口出去，其中依靠转发表，转发表里有MAC地址和端口号，转发表由路由表得来。
   2. 路由依靠路由算法获得最简单的路由选择，决定报文发送的下一跳主机的地址，复杂的路由协议可以选择一条从主机1和主机之间经过若干主机的路径，路由选择存在路由表中。
   3. 路由器的基本功能就是路径的选择与数据包的转发。路由就是路径的选择，转发就是将数据包从选定的路径发送出去。
2. **链路状态路由算法和距离矢量路由算法有哪些不同之处？**

* 链路状态路由算法：

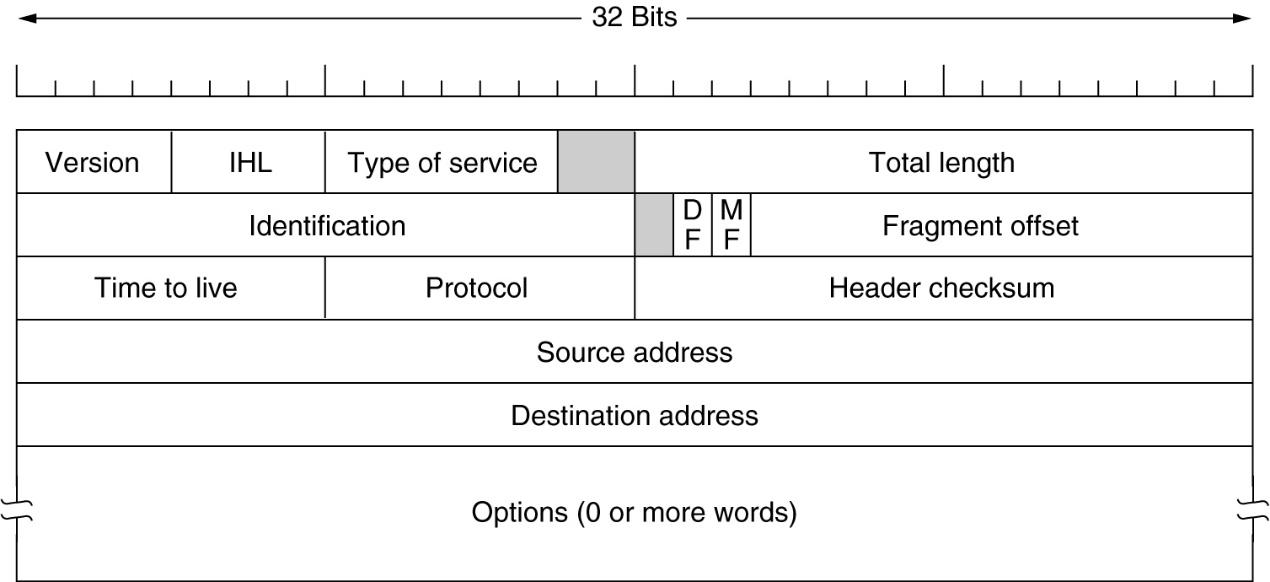
它采用一种“拼图”的设计策略，**即每个路由器将它到其周围邻居的链路状态向全网的其他路由器进行广播**。这样，一个路由器收到从网络中其他路由器发送过来的路由信息后，它对这些链路状态进行拼装，最终生成一个全网的拓扑视图，近而可以通过最短路径算法来计算它到别的路由器的最短路径。运行链路状态路由协议的路由器, 每台路由器在其接口的状态发生变化时，才将变化后的状态发送给其他所有路由器，每台路由器都使用收到的信息重新计算前往每个网络的最佳路径，然后将这些信息存储到自己的路由选择表中。

* 距离矢量路由算法：

每个路由器维护一个距离矢量（通常是以延时是作变量的）表，然后通过相邻路由器之间的距离矢量通告进行距离矢量表的更新。每个距离矢量表项包括两部分：到达目的结点的最佳输出线路，和到达目的结点所需时间或距离，通信子网中的其它每个路由器在表中占据一个表项，并作为该表项的索引。**每隔一段时间，路由器会向所有邻居结点发送它到每个目的结点的距离表，同时它也接收每个邻居结点发来的距离表。这样以此类推，经过一段时间后便可将网络中各路由器所获得的距离矢量信息在各路由器上统一起来，这样各路由器只需要查看这个距离矢量表就可以为不同来源分组找到一条最佳的路由。**

* 距离矢量算法是静态的，链路状态路由算法是动态的。

1. **请说明IP分组中IP头（IP Header）的Version字段、IHL字段、Total Length字段、Identification字段、DF字段、MF字段、TTL（Time To Live）字段、Protocol字段、Source Address字段、Destination Address字段的作用。**



1. Version字段：表示该IP数据报使用的IP协议版本：IPv4/IPv6。
2. IHL字段：指出整个报头的长度，接收端通过此区域可以计算出报头在何处结束以及从何处开始读数据。
3. Total Length字段：包含了整个IP数据报的长度，利用头部长度字段和总长度字段就可以计算出IP数据报中数据内容的起始和结束位置。
4. Identification字段：IP软件在存储器中维持一个计数器，每产生一个数据报，计数器就加1，并将此值付给标识字段。用于使分片后的各数据报片最后能正确地重装成为原来的数据报。
5. DF字段：“不能分片”，只有当DF=0时才允许分片。
6. MF字段：MF=1即表示后面“还有分片”的数据报，MF=0即表示这已是若干数据报片中的最后一个。
7. TTL（Time To Live）字段：它指定了数据报可以在网络中传输的最长时间，实际应用中设为可以经过的最大路由数，每经过一个路由器它的值就减一，当减为零时，数据报废弃，并发送ICMP报文通知源主机，防止数据报进入环路无休止的传输。
8. Protocol字段：IP协议可以承载上层协议，目标端根据协议标识就可以把收到的IP数据报送到TCP或UDP等上层协议。
9. Source Address字段：表示发送端的IP地址，可以作为接收端的目的地址。
10. Destination Address字段：表示接收端的目的IP地址，用于数据路由。
11. **有以下四个IP地址前缀（IP Prefix）:**
12. **192.168.0.0/23**
13. **192.168.2.0/23**
14. **192.168.4.0/22**
15. **192.168.8.0/21**

**请分别写出这四个IP地址前缀的网络掩码（netmask）。**

**若将这四个IP地址前缀进行聚合（aggregation），聚合后得到的IP地址前缀（IP Prefix）是多少？请写出计算过程。**

第一问：

192.168.0.0/23的网络掩码是：255.255.254.0

192.168.2.0/23的网络掩码是：255.255.254.0

192.168.4.0/22的网络掩码是：255.255.252.0

192.168.8.0/21的网络掩码是：255.255.248.0

第二问：

192.168.0.0/23对应的CIDR地址范围：192.168.0.0~192.168.1.255

192.168.2.0/23对应的CIDR地址范围：192.168.2.0~192.168.3.255

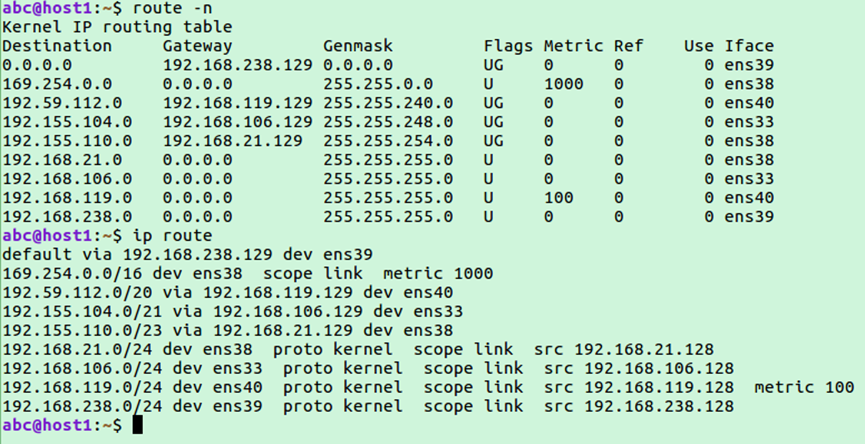
192.168.4.0/22对应的CIDR地址范围：192.168.4.0~192.168.7.255

192.168.8.0/21对应的CIDR地址范围：192.168.8.0~192.168.15.255

将CIDR地址范围聚合后的范围：192.168.0.0~192.168.15.255

因此聚合后的IP地址前缀为192.168.0.0/20

1. **在基于Ubuntu Linux的路由器中，通过route命令和ip route命令打印出来的此路由器的路由表如下。上面这两个命令输出的路由项是等价的。**

****

（注：截图中的“ens 38 proto kernel scope link src 192.168.21.128”中的这个IP地址为此路由器的网络接口（iface）ens38的IP地址）

请说明当此路由器接收到的IP分组中的目的IP地址分别为下列IP地址时，此路由器将分别会怎样处理这些IP分组。如果路由器转发这些分组的话，请写出用于将分组转发出去的网络接口的名字、下一跳设备的IP地址。

1. 192.168.21.153
2. 192.155.105.5
3. 192.155.111.8
4. 192.59.68.69
5. 192.59.114.9

地址范围：

IP前缀3：192.59.112.0/20 对应的IP地址范围：192.59.112.0~192.59.127.255

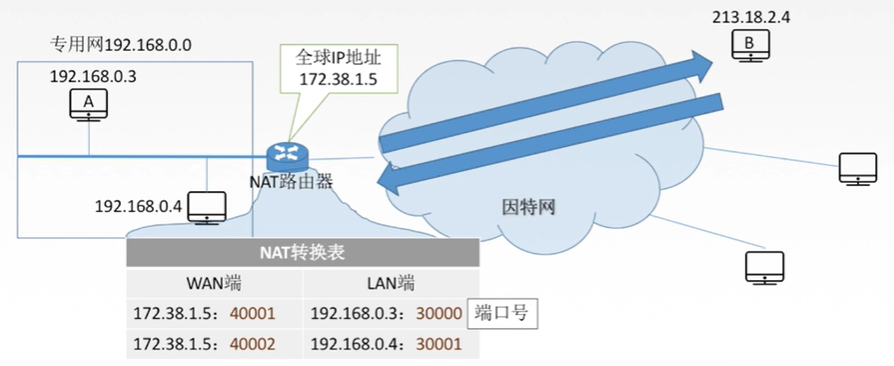
IP前缀4：192.155.104.0/21对应的IP地址范围：192.155.104.0~192.155.111.255

IP前缀5：192.155.110.0/23对应的IP地址范围：192.155.110.0~192.155.111.255

IP前缀6：192.168.21.0/24对应的IP地址范围：192.168.21.0~192.168.21.255

U 表示路由可用， G表示该路由是到一个网关，H该路由到达一个主机。

1. 192.168.21.153属于IP前缀6的IP地址范围，由于目的地址为192.168.21.0/24的路由项的Flags列取值为U，并且网关为0.0.0.0，所以，这条路由表示了本机与IP地址块192.168.21.0/24中的IP地址对应的计算机是直连的，也即不需要通过路由器转发，下一跳设备的IP地址就是目的主机的地址。所以：通过ens38转发，下一跳地址是：192.168.21.153
2. 192.155.105.5属于IP前缀4的IP地址范围，所以：通过ens33转发，下一跳IP地址是：192.168.106.129
3. 192.155.111.8属于IP前缀5的IP地址范围，所以：通过ens38转发，下一跳IP地址是：192.168.21.129
4. 192.59.68.69不属于路由表中任一路由项的目的地址的IP地址范围，在路由表中没有对应的路由项，因此进入默认网关，通过ens39转发，下一跳地址192.168.238.129
5. 192.59.114.9属于IP前缀3的IP地址范围，所以：通过ens40转发，下一跳IP地址是：192.168.119.129
6. **请说明NAT设备的作用。为什么存在NAT穿越（NAT traversal）的问题？**

作用：允许一个整体机构以一个公有IP地址出现在Internet上。是一种把内部私有IP地址翻译成合法的公有IP地址的设备， NAT在一定程度上，能够有效的解决公网地址不足的问题。工作图如下：

NAT穿越问题：

由于各种协议的应用各有不同，有的协议是无法通过NAT的，对于没有中间服务器的纯P2P应用来说，如果主机都位于NAT设备之后，双方是无法建立连接的。因为没有中间服务器的中转，NAT设备后的P2P程序在NAT设备上是不会有映射条目的，对方是不能向你发起一个连接的，因此就需要面对NAT穿透问题。