计网作业五六七章 赵子毅 PB20051107

第五章

R2

不是，链路层的可靠交付无法保证IP报文按序抵达。

R6

选择包括{0,1,2,….,31}。概率为1/32，等待时间：4*512bit/10mbps=204.8ms

R11

因为请求方不知道他请求的对象的mac地址，只能广播找。
回复方已经从请求报文中得知了发送方的mac地址所以只需要点对点回复即可

R12

不会，它们属于不同的子网。

R16

2N-2.将所有交换机串起来就行。除了头尾交换机只需要一个端口外其他交换机需要2个端口，共2n-2。

P2

例如矩阵

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{matrix}$$

出现2bit差错：

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{matrix}$$

根据二维奇偶校验码，只能得知第二、三列出错，不知道第几行出错

P5

R=0100

P6

- 0000
- 1111
- 1001

P8

1. $$E(p) = Np(1-p)^{N-1}$$
$$\frac{\mathrm{d}E(p)}{\mathrm{d}p} = N(1-p)^{N-2}((1-p)-p(N-1))$$
$$\hat{p} = \frac{1}{N}$$
2. $$E(\hat{p}) = \frac{(1-\frac{1}{N})^N}{1-\frac{1}{N}} = \frac{1}{e}$$

P15

1. 不会，该子网中的交换机将会执行转发功能，数据包不会被发送到R1.
(源ip,目标ip,源mac,目标mac):(E的ip,F的ip,E的mac,F的mac)
2. 不会,因为他们不在一个子网中.(源ip,目标ip,源mac,目标mac):(E的ip,B的ip,E的mac,R1连接子网3的端口的mac)
3.
    - 广播该帧,同时学习到A在子网1中
- R1也会受到,但是不会转发
- 不会,因为请求报文中包含了A的mac地址
- 更新确认转发表中B的一项,同时向与a相连的端口转发该报文

P17

$$\frac{512 \times 100bits}{10^7 bps} = 5.12ms$$

对于100mbps,时间为512微秒

P21

	源ip	目标ip	源MAC	目标MAC
1	a的ip	F的ip	a的mac	R1左边端口的mac
2	a的ip	F的ip	R1右边端口mac	R2左边端口mac
3	a的ip	F的ip	R2左边端口mac	F的mac

P26

事件	交换机表状态	转播链路	理由
BtoE	学习到B的地址	向A,C,D,E,F转播	交换机不知道E在哪里,只能广播
EtoB	学习到E的地址	B	交换机已经知道B的地址
AtoB	学习到A的地址	B	交换机已经知道B的地址
BtoA	无事发生	A	交换机已经知道A的地址

P28:

EE的主机IP地址（从左到右）依次为111.111.1.1，111.111.1.2，111.111.1.3,子网掩码111.111.1/24，CS主机IP地址（从左到右）依次为：111.111.2.1，111.111.2.2，111.111.2.3，子网掩码为111.111.2/24。与EE、CS子网相连的路由器IP地址分别为111.111.1.0、111.111.2.0，每个IP地址与VLAN ID相关联，假设111.111.1.0、111.111.2.0分别与VLAN11、VLAN12相关联，子网111.111.1/24、111.111.2/24中的每个帧分别添加一个VLAN ID为11、12的802.1q标记。

当EE主机向CS主机传送一个数据报时：

1. EE主机首先查询路由表，得知CS主机在另一网络，应当将数据报交给路由器转发；于是EE主机通过ARP查询到路由器的MAC地址，将IP数据报封装到MAC帧中发出；
2. 当MAC帧到达交换机时，交换机在该MAC帧上添加包含了EE系的VLAN ID的802.1q标记，并将其发往路由器；
3. 路由器的链路层收到MAC帧后，取出数据报交给网络层；网络根据数据报的目的IP地址，通过ARP查询到CS主机的MAC地址，将IP数据报封装到MAC帧中，并在该MAC帧上添加包含了CS系所在的VLAN ID的802.1q标记然后发出；
4. 当MAC帧到达交换机时，交换机去掉该MAC帧的802.1q标记，将其发往CS主机。
5. MAC帧到达CS主机，CS主机的链路层取出数据报交给网络层。

P31

1. 计算机在DHCP服务器创建一个发255.255.255.255的特殊IP数据报，然后在以太网中广播该帧，之后按照DHCP协议中的步骤，获得一个可以在一段时间内使用的IP地址。
2. 以太网中的DHCP服务器还提供第一跳路由器的IP地址列表、计算机所在子网的子网掩码以及本地DNS服务器的地址（如果存在）。
3. 计算机使用ARP协议来获取第一跳路由器和本地DNS服务器的MAC地址。计算机访问DNS服务器获得网页服务器的IP地址后，若WEB缓存中没有该网页，它将通过第一跳路由器发出HTTP请求。路由器收到计算机发送的以太网帧后，传递到IP层，检查路由表以判断向哪个端口转发。随后该TCP报文通过公共网络到达目标服务器。托管网页的的服务器通过HTTP响应消息将网页发送回计算机。

第七章:

R3

- 路径损耗：信号在传播过程中能量逐渐减少；频率越高衰减程度越高进而导致失真。
- 干扰：受到其他信号源的干扰，例如噪声，周边发送源的信号
- 多径传播：由于地面或物体的反射作用，信号沿着多条不同长度的路径到达接收端

R9

每个无线站点都可以设置一个RTS门限值，只有当传输的**数据帧长度大于该门限值时才使用****RTS/CTS序列传输**。该门限值确保了RTS/CTS机制仅用于较大的帧的传输

R16

- eNodeB的数据平面作用是在UE和P-GW 之间（经过LTE无线电接入网）转发数据报。它的控制平面的作用是代表UE来处理注册和移动性信令流量。
- MME代表位于它所控制单元中的UE，执行连接和移动性管理。它从HHS接收UE订购信息。
- P-GW给UE分配IP地址，并且保证QoS实施。作为隧道端点，当向或从UE转发数据报时，它也执行数据报封装/解封装。
- S-GW是数据平面移动性锚点，即所有UE流量将通过S-GW传递。该S-GW也执行收费/记账功能以及法定的流量拦截。

R23

本地恢复、TCP发送方知晓无线链路、分离连接方法。

P5

- 两个AP有着不同的SSID和MAC地址。当无线终端与SSID关联成功后，新站点和AP之间就有了一条虚拟链路。当站点发送给其中一个AP时，尽管另一个AP也会收到，但它不会处理，因为该帧并不是发给自己的。因此，两个ISP将在同一信道并行工作。然而，两个ISP之间共享相同的无线带宽。如果不同ISP的无线站点在同一时刻发送，将会发生冲突。
- 现在如果两个属于不同ISP（以及不同信道）的无线站点同时传输，它们将不会发生冲突。此外，它们也不会共享带宽，总计带宽翻倍。

P6

如果这一个站点将立即传送下一帧，考虑该站点传送大文件的情况，其他站点将在相当长一段时间内无法使用无线网络。这显然是不合理的。所以设计者是出于公平性来考虑这个问题的。

P7

一个不带数据的帧长度32字节，传输一个控制帧（例如RTS帧、CTS帧和ACK帧）的时间为(256 bits) / (11Mbps) = 23μs。传输数据帧所需的时间为(8256 bits) / (11 Mbps) = 751μs。一共是

$$
\begin{aligned}
&DIFS + RTS + SIFS + CTS + SIFS + FRAME + SIFS + ACK \\
&= DIFS + 3SIFS + (3 * 23 + 751)\mu s \\
&= DIFS + 3SIFS + 820\mu s
\end{aligned}
$$

P8

1. 1/2报文/时隙。必须b发完之后c才能向b发下一份。
2. 互不干扰，2报文/时隙
3. 互相干扰，1报文/时隙
4. 1，2，2
5. 0.25，2/3（第一时隙发报文，第二第三分别回复ack），2/3（第一时隙ctoD，第二DtoC的ACK，atob，第三BtoA的ack）

第八章

R1

- 机密性是攻击者法确定原始明文消息
- 消息完整性是接收方收到的是自从发送方发送后就没有被修改，即发送的报文和接受的报文是一致的

R3

在对称密钥系统中,发送方和接收方必须知道相同的密钥。在公开密钥系统中，加密和解密密钥是不同的。所有人都知道加密密钥，但是只有接收方知道解密密钥。

R13

公钥签名只需要加密短消息摘要，而不需要加密整个消息，极大程度地减小了计算开销

R14

错，使用其私钥加密，对方使用公钥解密。

R16

防御回放攻击。

P8

1. n = p * q = 55, z = (p - 1)(q - 1) = 40
2. e < n,且与 z 没有公因数
3. d = 27
4. $m = 8, m^e = 512，密文 c = m^e \mod n = 17$

P17

1. Bob级联分解该包
2. 首先使用Bob的私钥解密被Bob公钥加密的随机堆成会话密钥，得到该会话密钥
3. 使用该密钥解密使用该密钥加密的会话报文
4. 解密该报文后得到了一个带数字签名的会话报文，Bob将其级联分解
5. Bob使用alice的公钥解密上一步得到的数字签名，同时将散列函数作用于该报文，比较两者内容以确认发送者身份和报文完整性。