

4-01 网络层向上提供的服务有哪两种？试比较其优缺点。

网络层向上面的运输层提供需要建立连接的**虚电路服务**和无连接的**数据报服务**。优缺点如下：

- (1) 虚电路服务终端简单，需要网络保证其通信的可靠性；数据报服务终端有强大的差错处理能力，可以自己保证通信的可靠性
- (2) 虚电路服务通信前必须先建立连接；而数据报服务通信前无须先建立连接
- (3) 虚电路服务通信的分组均按照同一条线路进行转发，速度慢，容错性低；数据报服务通信的每个分组根据路由各自进行转发，速度快，容错性高
- (4) 虚电路服务可以保证分组按照发送顺序达到目的地址，数据报服务则不能

4-03 作为中间设备，转发器、网桥、路由器和网关有何区别？

- (1) **转发器**在**物理层**使用，主要起放大信号的作用。我们常说的集线器就是一种转发器
- (2) **网桥**在**数据链路层**使用，主要以接收、存储、地址过滤与转发的方式实现局域网互连。我们常说的交换机就是一种简化版网桥
- (3) **路由器**在**网络层**使用，主要的作用就是连接不同的网络，通过路由算法生成路由表，为数据报指明跳转接口
- (4) **网关**在**运输层**及以上使用，将两个使用不同协议的网络段连接在一起

4-07 试说明 IP 地址与硬件地址的区别。为什么要使用这两种不同的地址？

IP 地址是一台计算机或路由器在互联网中的全球唯一标识，在**网络层**使用；**硬件地址**即 MAC 地址，是每台计算机的唯一标识，在生产时就被写入，无法更改，在**数据链路层**使用。

因为全世界硬件地址繁多，且没有统一的约定标准，如果用其作为两台互连主机地址的标识，需要对其做复杂的硬件地址转换。因此想到用统一大小和规范的 IP 地址，然后通过多次路由转发即可到达目的地址。

4-10 试辨认以下 IP 地址的网络类别：

- (1) 128. 36. 199. 3
- (2) 21. 12. 240. 17
- (3) 183. 194. 76. 253
- (4) 192. 12. 69. 248
- (5) 89. 3. 0. 1
- (6) 200. 3. 6. 2

$128_{10}=10000000_2$ ， $21_{10}=00010101_2$ ， $183_{10}=10110111_2$ ， $192_{10}=11000000_2$ ， $89_{10}=01011001_2$ ， $200_{10}=11001000_2$

所以 (2) 和 (5) 是 A 类网，(1) 和 (3) 是 B 类网，(4) 和 (6) 是 C 类网

4-11 IP 数据报中的首部检验和并不检验数据报中的数据。这样做的最大好处是什么？坏处是什么？

因为数据报的数据部分过长，不检验数据部分可以加快分组的转发速度。但正是因为网络层不检查数据报的数据部分，一旦出现差错，需要等到运输层才能发现，增大了上层的重传和检验成本。

4-15 什么是最大传送单元 MTU？它和 IP 数据报首部中的哪个字段有关系？

最大传送单元是数据链路层规定的 MAC 帧的数据部分所能传送的最大数据单元，默认为 1500 字节。它和 IP 数据报首部中的**总长度**字段有关，但其实达不到总长度的最大值那么大，一般超过 1500byte 就会分段传输。

4-18 (1) 有人认为：“ARP 协议向网络层提供了转换地址的服务，因此 ARP 应

当属于数据链路层。”这种说法为什么是错误的？

因为 ARP 是将 IP 地址转换成 MAC 地址，本质上是为网络层服务的。IP 协议需要使用 ARP 协议，因此 ARP 协议应该属于网络层。

(2) 试解释为什么 ARP 高速缓存每存入一个项目就要设置 10-20 分钟的超时计时器。这个时间设置得太大或太小会出现什么问题？

因为 IP 地址和 MAC 地址之间的对应关系随时可能会改变。如果不设置超时计时器或者时间设置的太大，那么 ARP 高速缓存长久得不到更新，就会有許多 IP→MAC 的映射失效，导致地址转换错误，影响通信；如果时间设置的太小，那么 ARP 高速缓存中存储的映射时间太短，还没有更新就被丢弃了，下次还想继续查找时就需要重新写入，达不到记录的效果。

(3) 举出至少两种不需要发送 ARP 请求分组的情况（即不需要请求将某个目的 IP 址解析为相应的硬件地址）。

一台主机的 ARP 高速缓存存储了与该主机处于同一局域网的主机或路由器的 IP 地址到 MAC 地址的映射，当主机在自己的 ARP 高速缓存中检索不到下一跳的目的 MAC 地址时，就会发送 ARP 请求分组。但是如果源主机发送的是广播分组，就不需要发送 ARP 请求；当然，如果源主机的 ARP 高速缓存中存储了该 MAC 地址，也不会发送 ARP 请求。

4-24 试找出可产生以下数目的 A 类子网的子网掩码（采用连续掩码）：

(1) 2；(2) 6；(3) 30；(4) 62；(5) 122；(6) 250

A 类网络的网络号共 8 位，子网号全 1 或全 0 已被定义，因此只有 2 个子网的 A 类网的子网号为 2 位 ($2^2-2=2$)；有 6 个子网的 A 类网的子网号为 3 位 ($2^3-2=6$)；... 以此类推：

子网数	子网掩码
2	11111111 11000000 00000000 00000000
6	11111111 11100000 00000000 00000000
30	11111111 11111000 00000000 00000000
62	11111111 11111100 00000000 00000000
122	11111111 11111110 00000000 00000000
250	11111111 11111111 00000000 00000000

4-25 以下有 4 个子网掩码，哪些是不推荐使用的？为什么？

(1) 176. 0. 0. 0；(2) 96. 0. 0. 0；(3) 127. 192. 0. 0；(4) 255. 128. 0. 0

176. 0. 0. 0 = 10110000 00000000 00000000 00000000

96. 0. 0. 0 = 01100000 00000000 00000000 00000000

127. 192. 0. 0 = 01111111 11000000 00000000 00000000

255. 128. 0. 0 = 11111111 10000000 00000000 00000000

(1) (2) (3) 的子网掩码都不是连续的“1”+连续的“0”，不推荐。只有 (4) 符合子网掩码的标准。

4-31 以下地址中的哪一个和 86. 32/12 匹配？请说明理由。

(1) 86. 33. 224. 123；(2) 86. 79. 65. 216；(3) 86. 58. 119. 74；(4) 86. 68. 206. 154

86. 32/12 的网络号为：01011010 0010 0000 00000000 00000000，

网络掩码为 11111111 11110000 00000000

86. 33. 224. 123 和网络掩码作按位与操作得到网络号 01011010 00100000 00000000 00000000，与 86. 32/12 匹配；

86. 79. 65. 216 和网络掩码作按位与操作得到网络号 01011010 01000000 00000000 00000000，与 86. 32/12 不匹配；

86. 58. 119. 74 和网络掩码作按位与操作得到网络号 01011010 00110000 00000000 00000000，

与 86.32/12 不匹配;

86.68.206.154 和网络掩码作按位与操作得到网络号 01011010 01000000 00000000 00000000, 与 86.32/12 不匹配;

综上, 只有 86.33.224.123 与 86.32/12 匹配。

4-35 已知地址块中的一个地址是 140.120.84.24/20。试求这个地址块中的最小地址和最大地址。地址掩码是什么? 地址块中共有多少个地址? 相当于多少个 C 类地址?

140.120.84.24/20 所在地址块的网络号为 10001100 01111000 0101 0000 00000000,

地址块中最小地址为 10001100 01111000 01010000 00000000/20;

地址块中最大地址为 10001100 01111000 01011111 11111111/20;

地址掩码是 11111111 11111111 11110000 00000000

地址块中含有 $2^{12}=4096$ 个地址

C 类地址的网络号为 24 位, 因此相当于 $2^{12}/2^8=2^4=16$ 个 C 类地址

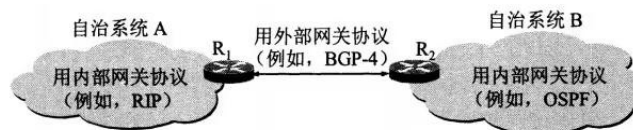
4-38 IGP 和 EGP 这两类协议的主要区别是什么?

互联网可以划分为多个较小的自治系统 AS (如一个 ISP), 一个 AS 使用单一技术管理一组路由器, 这些路由器使用单一、一致的路由选择策略。

内部网关协议 IGP, 也叫域内路由选择, 是在一个 AS 内部的路由选择策略, 与外部无关。如 RIP 和 OSPF;

外部网关协议 EGP, 也叫域间路由选择, 是在两个处在不同 AS 通信时选择的路由策略。当数据报从一个 AS 传到另一个 AS 边界时, 就需要使用 EGP 将其传入该 AS。如 BGP-4;

AS、IGP、EGP 关系如图:



4-39 试简述 RIP, OSPF 和 BGP 路由选择协议的主要特点。

RIP 和 OSPF 是内部网关协议, BGP 是外部网关协议。

RIP, 即路由信息协议, 是一种分布式的基于距离向量的路由选择协议。它要求网络中每一个路由器维护从自己到其他目的网络的路由跳数, 适用于小型互联网。协议的主要特点是: 只有相邻路由器交换信息; 路由器交换当前知道的所有信息; 路由器按固定的时间间隔交换路由信息。

OSPF, 即开放最短路径优先协议, 是一种分布式的链路状态路由选择协议。主要特点是: 使用洪泛法向相邻路由器发送信息; 发送的信息是与该路由器相邻的所有路由器的链路状态; 只有当链路状态改变, 路由器才向所有路由器发送信息。

BGP, 即边界网关协议, 是不同自治系统的路由器间交换路由信息的协议。主要特点是: 交换可达性信息, 即无回路的较好的路由, 并非一定是最佳的。

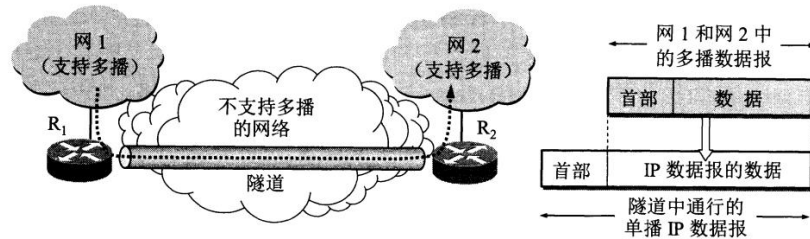
4-43 IGMP 协议的要点是什么? 隧道技术在多播中是怎样使用的?

网际组管理协议 IGMP, 基于 IP 协议。IGMP 协议是让连接在本地局域网上的多播路由器知道本局域网上是否有主机参加或退出了某个多播组。当然, 仅靠 IGMP 协议无法完成多播任务, 多播路由器还需要和互联网中其他多播路由器协同工作, 以便将多播数据以最小代价传送给成员。

隧道技术适用于多播过程中通过不支持多播的网络传输多播数据报。如图所示, 网 1 和网 2 都支持多播, 但路由器 R1 和 R2 之间的网络并不支持多播。如果网 1 中的主机向网 2 中的部分主机进行多播, 就不能直接按多播数据报进行传输。于是需要路由器 R1 对多播数

据报再次进行封装，即再加上普通数据报首部，使之变成单播数据报，然后通过该网络从 R1 发送至 R2。因为这样的操作酷似穿过隧道，因此称为“隧道”技术。

当封装后的单播数据报到达 R2 后，多播路由器 R2 剥取其首部，得到多播数据报，就可以继续向目的地址进行多播转发。



4-48 假设一段地址的首地址为 146.102.29.0, 末地址为 146.102.32.255, 求这个地址段的地址数。

146.102.29.0 = 10010010 01100110 00011101 00000000

146.102.32.255 = 10010010 01100110 00100000 11111111

所以地址范围为 $(32-29+1) * 2^8 = 1024$

4-65 试把以下的零压缩的 IPv6 地址写成原来的形式:

(1) 0::0

0000:0000:0000:0000:0000:0000:0000:0000

(2) 0:AA::0

0000:00AA:0000:0000:0000:0000:0000:0000

(3) 0:1234::3

0000:1234:0000:0000:0000:0000:0000:0003

(4) 123::1:2

0123:0000:0000:0000:0000:0000:0001:0002