1. RIP与OSPF区别

（1）【工作核心不同】RIP：数跳数；OSPF：计算链路的度量值

（2）【向谁发】RIP：仅和相邻路由器交换信息；

OSPF：向本自治系统所有路由器发送消息，由于路由器发送的链路状态信息只能单向传送，OSPF不存在“坏消息传播得慢”的问题，更新过程的收敛性得到保证。

（3）【发什么】RIP：路由器交换的信息是当前本路由器所知道的全部信息，即自己现在的路由表

OSPF：发送的信息是与本路由器相邻的所有路由器的链路状态 ，只涉及与相邻路由器的连通状态，与整个互联网的规模无关。

（4）【什么时候发】RIP：按固定的时间间隔交换路由信息（当网络拓扑发生变化时，路由器也及时向相邻路由器通告拓扑变化后的路由信息）

OSPF：在网络刚刚启动计算第一次路由表时，一定发路由信息。只有当链路状态发生变化时，路由器才能向所有路由器用洪泛法发送此消息（链路状态：说明本路由器都和哪些路由器相邻以及该链路的度量）

（5）RIP协议使用运输层的用户数据包UDP来进行传送

OSPF的位置在网络层，直接用IP数据报传送(其IP数据报首部的协议字段值为89)。

由于OSPF构成的数据报很短，不仅减少了路由信息的通信量，而且在传送中不必分片，不会出现一片丢失而重传整个数据报的现象。

（6）对一个给定的目的网络，可以根据IP数据报的服务类型TOS计算出不同的路由

（7）RIP：不能在两个网络之间同时使用多条路由，选择一条具有最少路由器的路由即最短路由

OSPF：如果到同一个目的网络有多条相同代价的路径时，可以将通信量分配给这几条路径，做到路径间的负载平衡

（8）RIP：限制了网络规模，能使用的最大距离为15,16表示不可达

OSPF：链路的度量可以是1~65535中的任何一个无量纲的数，可供管理人员来决定。因此十分灵活。

（9）RIP：1号版本不支持子网划分，2号版本支持子网划分

OSPF在路由分组中包含子网掩码，支持可变长度的子网划分和无分类的编址CIDR

（10）所有在OSPF路由器之间交换的分组（如链路状态更新分组）都具有鉴别功能，因而保证了仅在可信赖的路由器之间交换链路状态信息。

（11）由于各路由器之间频繁地交换链路状态信息，因此所有的路由器最终都能建立一个链路状态数据库，及即全网拓扑结构图。

OSPF的链路数据库能较快地进行更新，使每个路由器能及时更新其路由表，OSPF的更新过程收敛得快是其重要优点。

RIP协议的每个路由器虽然知道到所有的网络距离以及下一跳路由器，但是不知道全网的拓扑结构，只有到了下一跳路由器，才能知道再下一跳应当怎样走

（12）为了使OSPF能够用于规模很大的网络，OSPF 将一个自治系统再划分为若干个更小的范围，叫作区域。

2. RIP防止环路的机制

1. 最大跳数15跳（但这只是回避环路问题，没有解决该问题）
2. 水平分割：不能向路由的来源方向返回路由。比如R3的f0口传给R2的f0口的路由信息，不会被R2的f0口返回给R3，因为这样做毫无意义。但可能会被R2的f1口返回给R3。因此也不能彻底解决环路
3. 路由毒化和毒性反转。路由毒化：将已经断开的路由的距离通告为无穷大（度量=16），例如：R3的f1口的度量设为16并通告R2，R2的路由表中该IP的度量更新为16表示已断开。毒性反转：R2知道已断开后，再发给R3做确认（此时毒性反转会忽略水平分割）。为何要毒性反转？因为不毒性反转告诉R3我知道了，R3会持续给R2发该路由已断开的信息。
4. 抑制计数器：没什么用已经废弃。无效计时器invalid timer：一条路由更新180秒内没收到就将跳数设为16。flush timer：如果一条路由180秒内没更新，还不是马上不能用，而是possibly down，直到240秒内无更新才从路由表中删除
5. 触发更新：一旦网络拓扑发生变化，路由器将立即发送路由更新给邻居，不需要等30秒

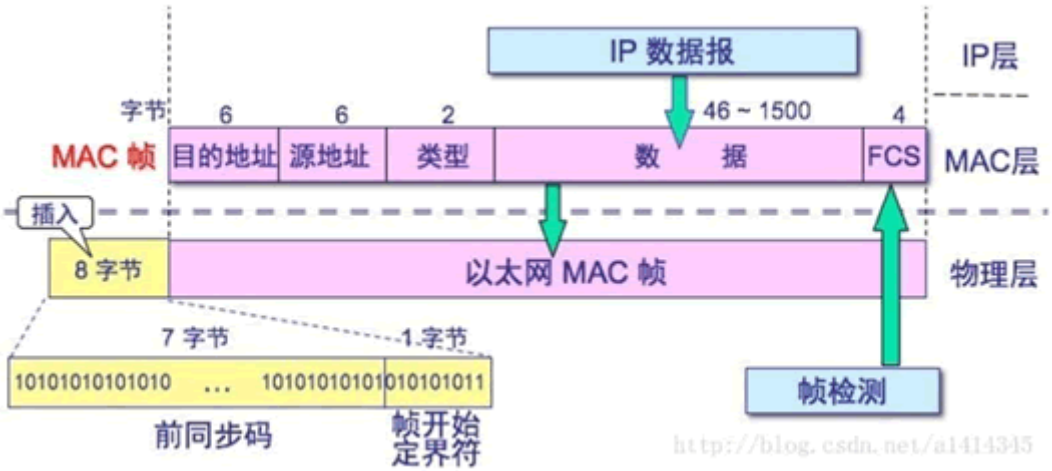
3. 以太网各层数据包打包

1.在链路层，由以太网的物理特性决定了数据帧的长度为（46＋18）-（1500＋18），其中的18是数据帧的头和尾，也就是说数据帧的内容最大为1500（不包括帧头和帧尾），即MTU（Maximum Transmission Unit）为1500；

2.在网络层，因为IP包的首部要占用20字节，所以这的MTU为1500 - 20＝1480；

3.在传输层，对于UDP包的首部要占用8字节，所以这的MTU为1480 - 8＝1472；

所以，在应用层，你的Data最大长度为1472。 （当我们的UDP包中的数据多于MTU(1472)时，发送方的IP层需要分片fragmentation进行传输，而在接收方IP层则需要进行数据报重组，由于UDP是不可靠的传输协议，如果分片丢失导致重组失败，将导致UDP数据包被丢弃）。



那么就一个问题， 用wireshark捕包。 为什么frame那一行是1514bytes?

以太网封装IP数据包的最大长度是1500字节，也就是说以太网最大帧长应该是以太网首部加上1500，再加上7字节的前导同步码和1字节的帧开始定界符，具体就是：7字节前导同步吗＋1字节帧开始定界符＋6字节的目的MAC＋6字节的源MAC＋2字节的帧类型＋1500＋4字节的CRC校验

按照上述，最大帧应该是1526字节，但是实际上我们抓包得到的最大帧是1514字节，为什么不是1526字节呢？原因是当数据帧到达网卡时，在物理层上网卡要先去掉前导同步码和帧开始定界符，然后对帧进行CRC检验，如果帧校验和错，就丢弃此帧。如果校验和正确，就判断帧的目的硬件地址是否符合自己的接收条件（目的地址是自己的物理硬件地址、广播地址、可接收的多播硬件地址等），如果符合，就将帧交“设备驱动程序”做进一步处理。这时我们的抓包软件才能抓到数据，因此，抓包软件抓到的是去掉前导同步码、帧开始分界符、CRC校验之外的数据，其最大值是6＋6＋2＋1500＝1514。

4. 无连接服务和面向连接服务的优缺点

无连接服务：通信简单，不占用信道。但适合于非实时通信，不能可靠交付，报文可能丢失、乱序或者延迟，通常没有反馈和纠错机制。

面向连接服务：提供可靠交付，有纠错反馈机制，报文按序到达，适合实时通信。但是机制复杂，需要建立和释放连接，持续占用信道资源。

5. 既然网络层提供了两种服务方式，为什么还要独立出一层传输层，同时传输层也要提供这两种方式?

传输层的代码完全运行在用户的机器上，而网络层主要运行在承运商控制的路由器上，这也就是网络层应该在的地方，网络层的作用就是为数据包提供路由。这样就照成了用户对于网络层的控制几乎是没有的，用户只能控制自己机器上的程序。那么如果网络层提供的将服务不够用怎么办？ 如果他频繁的丢失分组怎么办？用户在网络层上并没有真正的控制权，所以他们不可能用最好的路由器或者在数据层上用更好的错误处理机制来解决服务太差的问题，唯一的可能是在网络层之上的另一层中提高服务质量。这样就是为什么会出现传输层的原因。

TCP/IP协议在网络层是无连接的（数据包只管往网上发，如何传输和到达以及是否到达由网络设备来管理）。而“端口”，是传输层的内容，是面向连接的。协议里面低于1024的端口都有确切的定义，它们对应着因特网上常见的一些服务。这些常见的服务可以划分为使用TCP端口（面向连接如打电话）和使用UDP端口（无连接如写信）两种。

从本质上来讲，由于传输层的存在，这使得传输服务有可能比网络服务更加可靠。 丢失的分组和损坏的数据可以在传输层上检测出来，并且由传输层来补偿 。

6. 隧道技术以及各层隧道通信应用

隧道技术（Tunneling）是一类网络协议，它是一种数据包封装技术，它将原始IP包（其报头包含原始发送者和最终目的地）封装在另外一个数据包（称为封装的IP包）的数据净荷中进行传输。 ***使用隧道的原因是在不兼容的网络上传输数据，或在不安全网络上提供一个安全路径。*** 隧道协议通常（但并非总是）在一个比负载协议还高的层级，或同一层。

隧道技术（Tunneling）是一种通过使用互联网络的基础设施在网络之间建立一条虚拟链路以传递数据的方式。使用隧道传递的数据可以是不同协议的PDU，隧道将其他协议的PDU重新封装后通过网络发送，新的PDU提供路由信息，以便通过互联网传递被封装的数据。由于PDU经过重新封装，使得数据的发送方和接收方就像在一条专有“隧道”中进行数据传输和通信，隧道技术因此得名。

一般来说，隧道是在高层（或同等层）分组中携带低层数据。例如，在一个IPv4或IPv6分组中携带IPv4数据，在一个UDP、IPv4或IPv6分组中携带以太网数据。隧道转变了在头部中协议严格分层的思路，并允许形成覆盖网络（即这些“链路”实际是其他协议实现的虚拟链路，而不是物理连接的网络）。通过隧道的建立，可实现将数据强制送到特定的地址、隐藏私有的网络地址、在IP网上传递非IP数据包、提供数据安全支持等功能。

PPTP（Point to Point Tunneling Protocol）提供PPTP客户机和PPTP服务器之间的加密通信。PPTP客户机是指运行了该协议的PC机，如启动该协议的Windows95/98；PPTP服务器是指运行该协议的服务器，如启动该协议的WindowsNT服务器。PPTP是PPP协议的一种扩展。它提供了一种在互联网上建立多协议的安全虚拟专用网（VPN）的通信方式。远端用户能够透过任何支持PPTP的ISP访问公司的专用网。通过PPTP，客户可采用拨号方式接入公用IP网。

通用路由封装（GRE：Generic Routing Encapsulation）在RFC1701/RFC1702中定义，它规定了怎样用一种网络层协议去封装另一种网络层协议的方法。GRE的隧道由两端的源IP地址和目的IP地址来定义，它允许用户使用IP封装IP、IPX、AppleTalk，并支持全部的路由协议，如RIP、OSPF、IGRP、EIGRP。通过GRE，用户可以利用公用IP网络连接IPX网络和AppleTalk网络，还可以使用保留地址进行网络互联，或对公网隐藏企业网的IP地址。

隧道技术的应用：

虚拟专用网络：VPN是Internet技术迅速发展的产物，其简单的定义是，在公用数据网上建立属于自己的专用数据网。也就是说不再使用长途专线建立专用数据网，而是充分利用完善的公用数据网建立自己的专用网。它的优点是，既可连到公网所能达到的任何地点，享受其保密性、安全性和可管理性，又降低网络的使用成本。VPN依靠Internet服务提供商（ISP）和其他的网络服务提供商（NSP）在公用网中建立自己的专用“隧道”，不同的信息来源，可分别使用不同的“隧道”进行传输。

IP隧道：为了在TCP/IP网络中传输其他协议的数据包，Linux采用了一种IP隧道技术。在已经使用多年的桥接技术中就是通过在源协议数据包上再套上一个IP协议帽来实现。利用IP隧道传送的协议包也包括IP数据包，Linux的IP包封指的就是这种情况。移动IP（Mobile-IP）和IP多点广播（IP-Multicast）是两个流行的例子。目前，IP隧道技术在VPN中也显示出极大的魅力。

移动IP是在全球Internet上提供移动功能的一种服务，它允许节点在切换链路时仍可保持正在进行的通信。它提供了一种IP路由机制，使移动节点以一个永久的IP地址连接到任何链路上。与特定主机路由技术和数据链路层方案不同，移动IP还要解决安全性和可靠性问题，并与传输媒介无关。移动IP的可扩展性使其可以在整个互联网上应用。随着隧道技术的发展，各种业务已经开始根据本业务的特点制定相应的隧道协议。

IPV4与IPV6互通：网站和用户分别安装IPv6隧道软件，用户应用程序以IPv4协议（私有地址）与网站应用通信，并把IPv4报文封装进IPv6隧道，穿透网络。用于不同协议栈之间的互通。简而言之，假设用户的是IPv4协议栈，公司也是IPv4协议栈，信息则直接可以互通；如果用户的是IPv4协议栈，公司的是IPv6协议栈（不同协议栈不兼容）；用户给公司发送信息时，隧道软件会把信息进行封装，通过隧道穿透网络，将信息传送到公司之后，软件进行解封，获取信息，反之亦然。

不支持多播的网络：绝大多数广域网都不支持物理多播地址。要通过这样的网络发送一个多播分组就需要使用隧道技术。多播分组被封装为单播分组并通过网络发送，而当它出现在另一端再转换为一个多播分组。

7. 计算机网络各层计时器

- IP层计时器

  路由器/主机在收到IP报文的一个分片后会启动一个计时器，当计时器结束前未收到完整报文时，会发送一个ICMP差错报文

- RIP协议中的计时器

  定期计时器：定期发送路由状态（25s~35s）

截止计时器：一定时间未收到则过期（180s）

无用信息收集计时器：确定某路由失效，保留一段时间，到期则删除（120s）

- OSPF协议中的计时器

  Hello interval：每隔10s发送一个Hello报文

  到期计时器（router dead interval）：认为一个路由器断连需等待的时间（40s）

- BGP协议中的计时器

  定期计时器：定期交换保活报文

  保活计时器：一定时间内未收到保活报文则认为该表项失效

- IGMP协议中的计时器

  定期计时器：IGMP查询定期发送查询请求（125s）

  接口计时器：对查询进行延迟反应（P297 很复杂）

  组计时器：P297 很复杂

- TCP协议中的计时器

  重传计时器：设定报文超时时间以用来超时重传

  持续计时器：纠正死锁问题，按期发送探测报文段

  保活计时器：防止两个TCP之间长时间空闲

  TIME-WAIT计时器：连接终止第三次挥手使用，2MSL

- 停止等待协议、后退N协议、选择重传协议中的计时器

  发送方每次发送分组的时候要启动一个计时器，超时重传

8. 计算机网络虚电路