

1

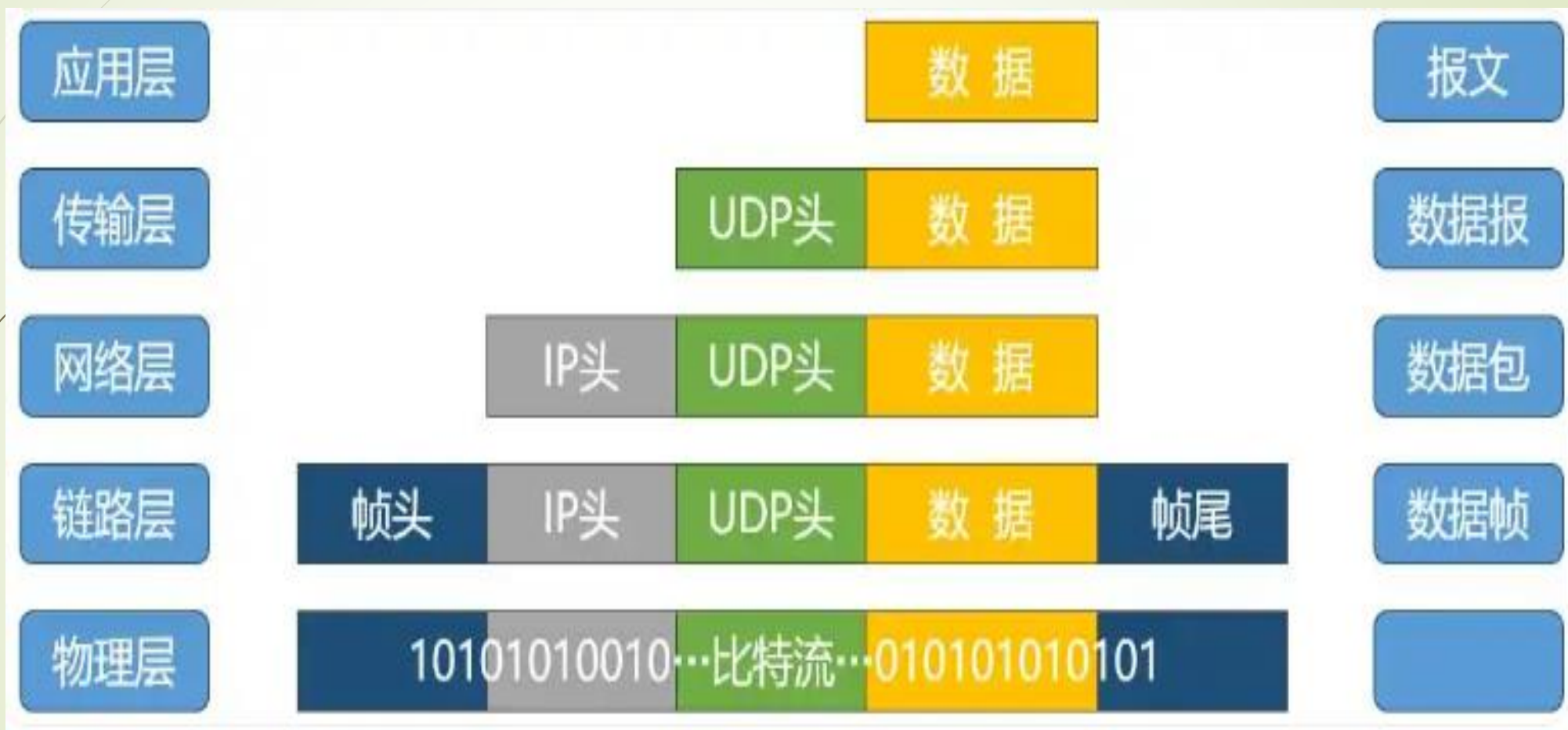
IP数据包分析实验

冯巾松

fengjinsong@tongji.edu.cn

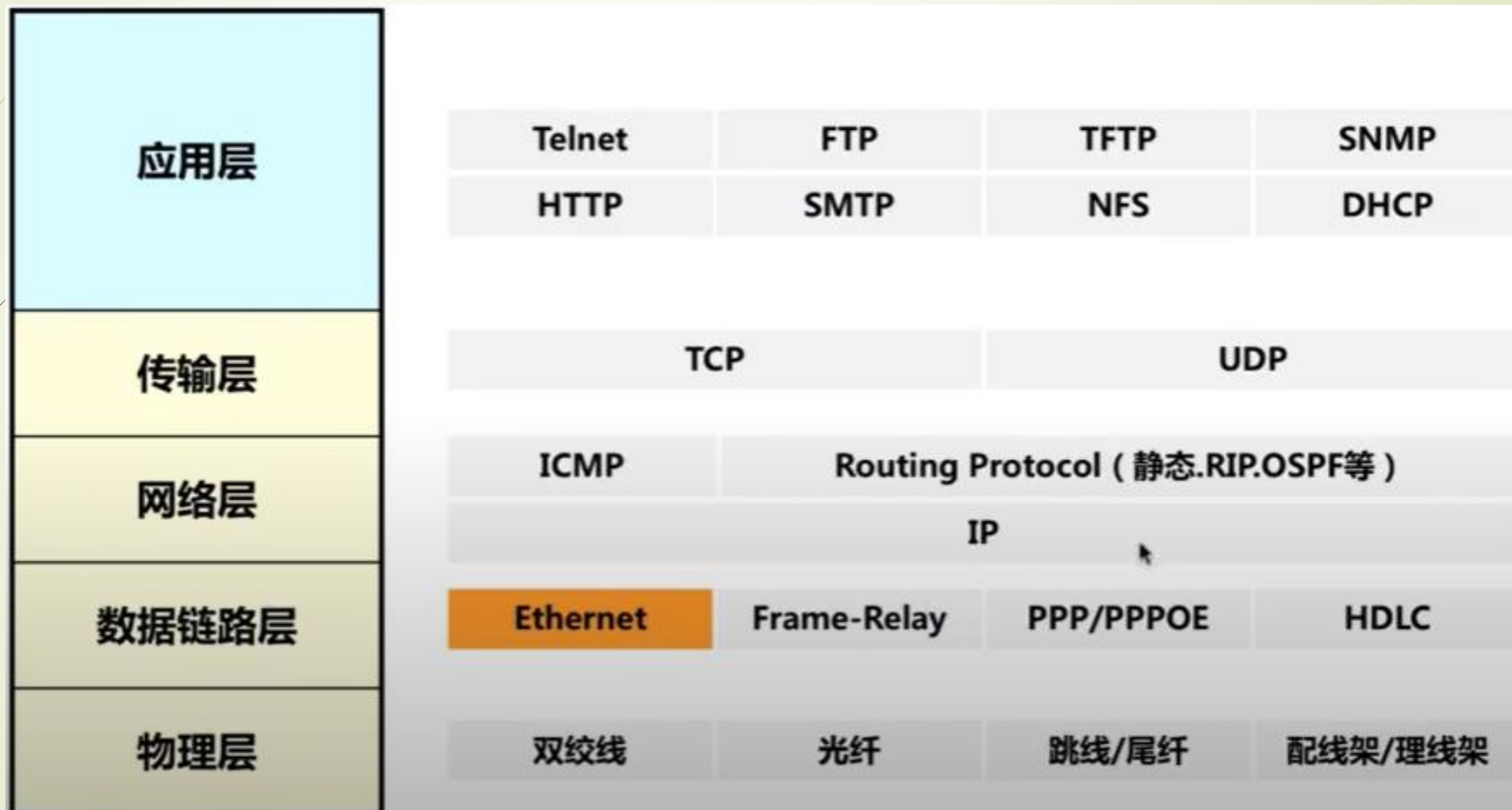
数据逐层封装

2



TCP/IP体系协议分步

3



IP协议

➡ 1. IP数据报文格式总览

IP协议提供不可靠无连接的数据报传输服务，IP层提供的服务是通过IP层对数据报的封装与拆封来实现的。

IP数据报的格式分为报头区和数据区两大部分，其中报头区是为了正确传输高层数据而加的各种控制信息，数据区包括高层协议需要传输的数据。

IP数据报文格式总览

一个 IP 数据报由首部和数据两部分组成。



报文头部

- 头部的前一部分是固定长度，共 20 字节，是所有IP数据报必须具有的。



在头部的固定部分的后面是一些可选字段，其长度是可变的。

数据报头部 - 版本

- 版本 占 4 位，指 IP 协议的版本。目前的 IP 协议版本号为 4 (即 IPv4)



首部长度的

➡ 首部长度的 — 占 4 位，可表示的最大数值是 15 个单位(一个单位为 4 字节)，因此 IP 的首部长度的最大值是 60



区分服务

区分服务 — 占 8 位，用来获得更好的服务。
在旧标准中叫做服务类型



总长度

➡ 总长度 一 占16位，指首部和数据之和的长度，单位为字节，因此数据报的最大长度为65535 字节。总长度必须不超过最大传送单元 MTU



标识

11

➡ 标识(identification) ——占 16 位，它是一个计数器，用来产生 IP 数据报的标识



标志

➤ 标志(flag) 一占 3 位，目前只有前两位有意义。标志字段的最低位是 MF (More ragment)。MF=1 表示后面“还有分片”。MF=0 表示最后一个分片。标志字段中间的一位是 DF (Don't Fragment)。只有当 DF=0 时才允许分片



片偏移

■ 片偏移——占13位，指出：较长的分组在分片后某片在原分组中的相对位置。片偏移以8个字节为偏移单位。



生存时间

■ 生存时间——占8位，记为 TTL (Time To Live)，指示数据报在网络中可通过的路由器数的最大值



协议

➡ 协议 — 占8位，指出此数据报携带的数据使用何种协议，以便目的主机的IP层将数据部分上交给那个处理过程



首部检验和

■ 首部检验和 占16 位，只检验数据报的首部，不检验数据部分。这里不采用 CRC 检验码而采用简单的计算方法。IP 数据报首部检验和的计算采用 16 位二进制反码求和算法



源地址和目的地址

- 源地址和目的地址都各占 4 字节



可变部分

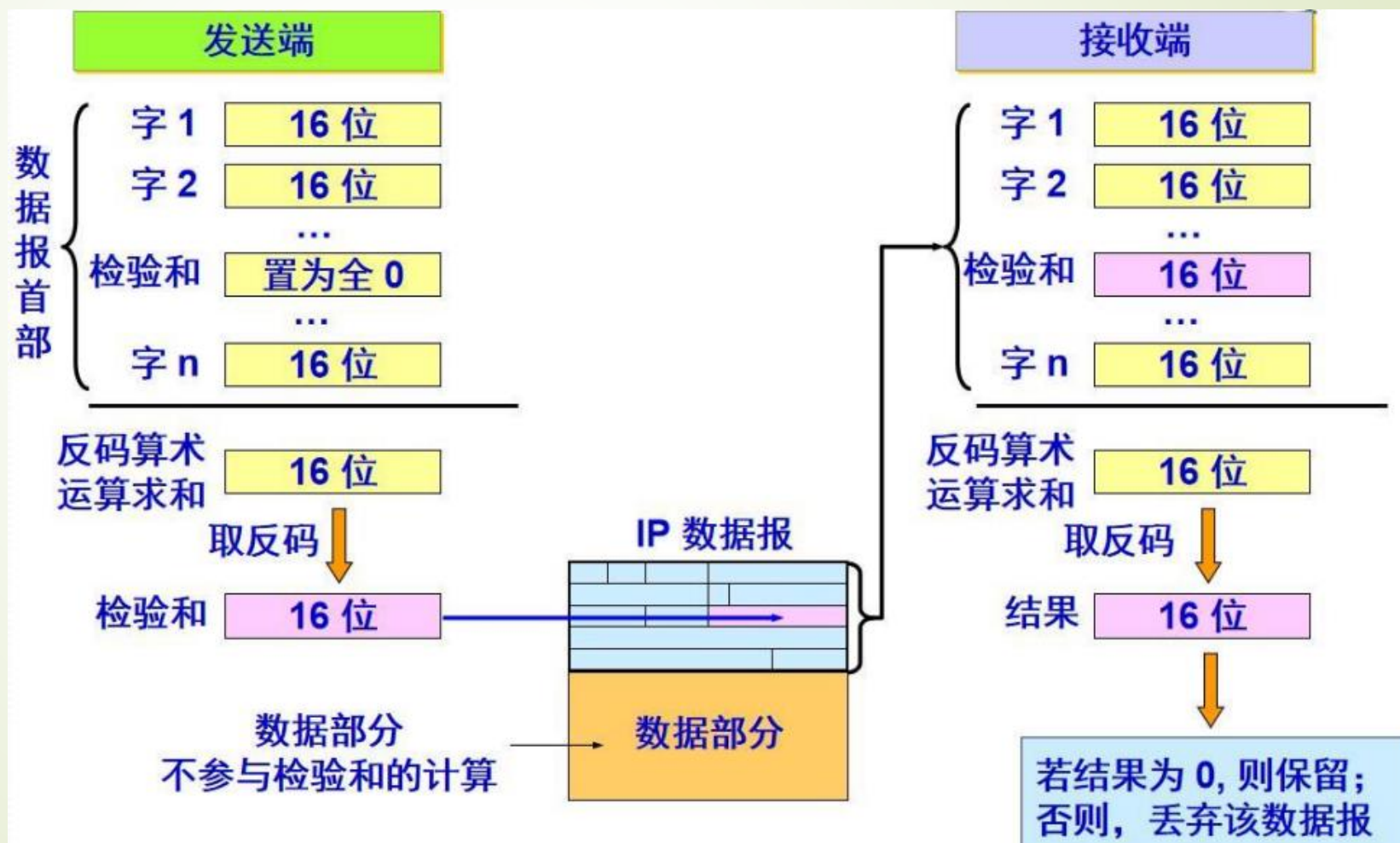
➡ 3. IP 首部的可变部分就是一个选项字段，用来支持排错、测量以及安全等措施，内容很丰富。选项字段的长度可变，从 1 个字节到 40 个字节不等，取决于所选择的项目。



IP协议

19

4. IP 数据报首部校验 IP 数据报首部检验和的计算采用16 位二进制反码求和算法



IP协议

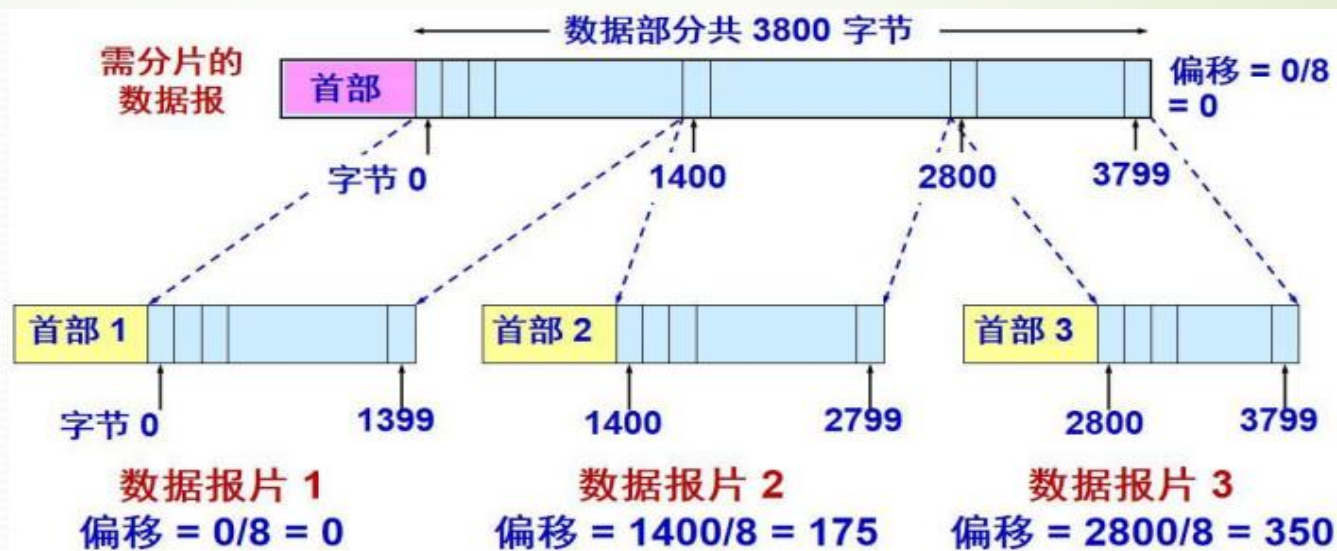
20

- ➡ 5. IP数据报分段给出 一 数据报的总长度为 3820 字节，其数据部分的长度为 3800 字节（使用固定首部），需要分片为长度不超过 1420 字节的数据报片。
- ✓ 1 因固定首部长度为 20 字节，因此每个数据报片的数据部分长度不能超过1400 字节。
- ✓ 2 于是分为 3 个数据报片，其数据部分的长度分别为1400、1400 和1000 字节。
- ✓ 3 原始数据报首部被复制为各数据报片的首部，但必须修改有关字段的值（如标志字段）

IP协议

21

5. IP数据报分段

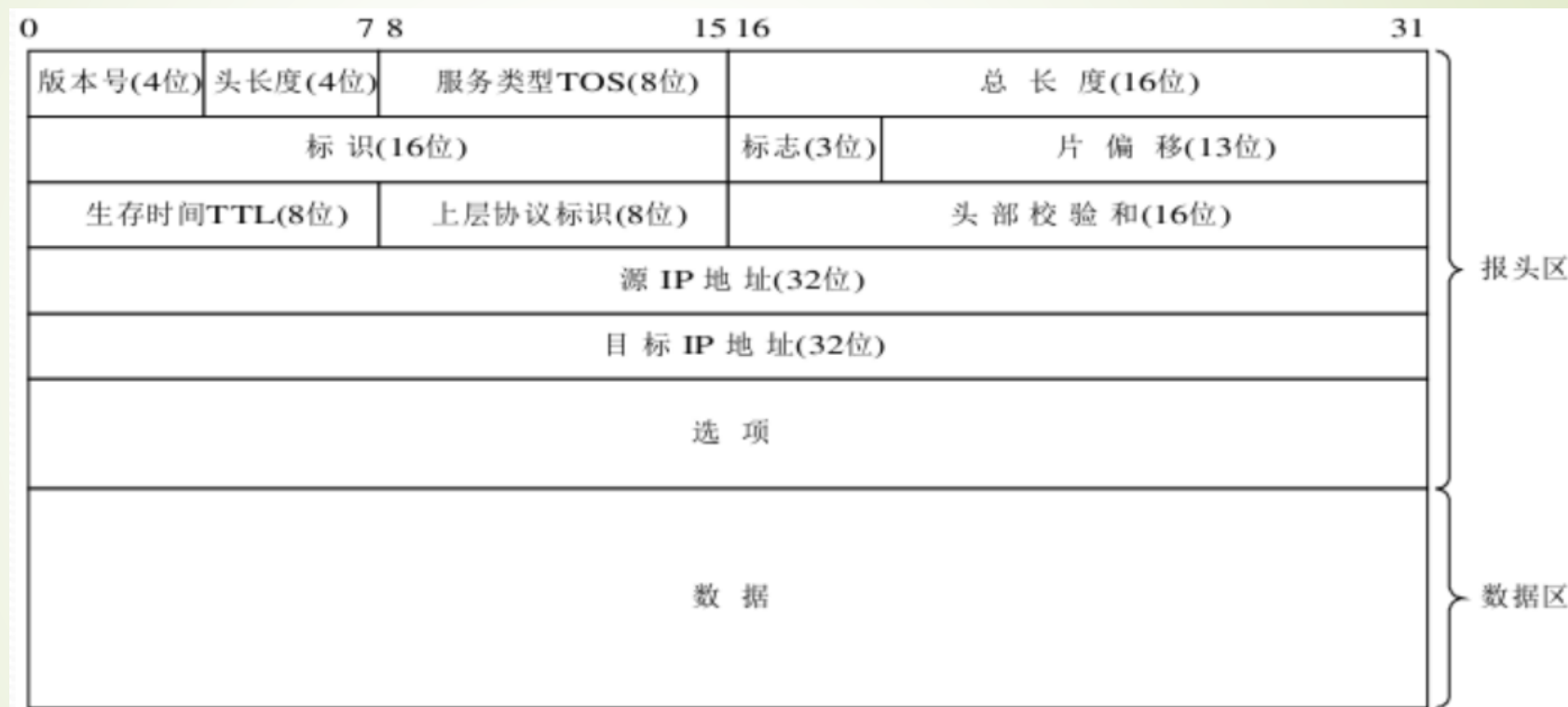


	总长度	标识	MF	DF	片偏移
原始数据报	3820	12345	0	0	0
数据报片1	1420	12345	1	0	0
数据报片2	1420	12345	1	0	175
数据报片3	1020	12345	0	0	350

IP协议

22

6. IP数据报文格式传输



注意，上图表示的数据，最高位在左边，记 0 位；最低位在右边，记为 31 位。在网络中传输数据时，先传输 0~7 位，其次是 8~15 位，然后传输 16~23 位，最后传输 24~31 位

IP协议

23

7. IP数据报文上层协议

十进制编号	协 议	说 明
0	无	保留
1	ICMP	网际控制报文协议
2	IGMP	网际组管理协议
3	GGP	网关—网关协议
4	无	未分配
5	ST	流
6	TCP	传输控制协议
8	EGP	外部网关协议
9	IGP	内部网关协议
11	NVP	网络声音协议
17	UDP	用户数据报协议

IP协议

➡ 8. IP数据报文的TOS 服务类型 (TOS、type of service)：占用8位 二进制位，用于规定本数据报的处理方式。 服务类型字段的8位分成了5个子域：

0	1	2	3	4	5	6	7
优先权			D	T	R	保留	

(1)——优先权 (0-7) 数越大，表示该数据报优先权越高。网络中路由器可以使用优先权进行拥塞控制，如当网络发生拥塞时可以根据数据报的优先权来决定数据报的取舍

➡ 8. IP数据报文的TOS

(2)—短延迟位D(Delay): 该位置1时, 数据报请求以短延迟信道传输, 0表示正常延时。

(3)—高吞吐量位T(Throughput): 该位置1时, 数据报请求以高吞吐量信道传输, 0表示普通。

(4)—高可靠位R(Reliability): 该位置1时, 数据报请求以高可靠性信道传输, 0表示普通。

(5)—保留位。

IP协议

8. IP数据报文的TOS

目前在Internet中使用的TCP/IP协议大多数情况下网络并未对TOS进行处理，但在实际编程时，有专门的函数来设置该字段的各域。一些重要的网际应用协议中都设置了建议使用的TOS值：

应用程序	短延迟位D	高吞吐量位T	高可靠性位	低成本位	十六进制值	特性
Telnet	1	0	0	0	0x10	短延迟
FTP控制	1	0	0	0	0x10	短延迟
FTP数据	0	1	0	0	0x08	高吞吐量
TFTP	1	0	0	0	0x10	短延迟
SMTP命令	1	0	0	0	0x10	短延迟
SMTP数据	0	1	0	0	0x08	高吞吐量
DNS UDP查询	1	0	0	0	0x10	短延迟
DNS TCP查询	0	0	0	0	0x00	普通
DNS 区域传输	0	1	0	0	0x08	高吞吐量
ICMP差错	0	0	0	0	0x00	普通
ICMP查询	0	0	0	0	0x00	普通
SNMP	0	0	1	0	0x04	高可靠性
IGP	0	0	1	0	0x04	高可靠性
NNTP	0	0	0	1	0x02	低成本

➡ 9.最大传输单元:

IP数据报在互联网上传输时，可能要经过多个物理网络才能从源端传输到目的端。不同的网络由于链路层和介质的物理特性不同，因此在传输数据时，对数据帧的最大长度都有一个限制，这个限制值即最大传输单元 MTU (Maximum Transmission Unit)。同一个网络上的两台主机之间通信时，该网络的 MTU 值是确定的，不存在分片问题。分片问题一般只存在于具有不同 MTU 值的互联网中。

➡ 9.最大传输单元:

由于现在互联网主要使用路由器进行网络连接，因此分片工作通常由路由器负责。当两台主机之间的通信要通过多个具有不同 MTU 值的网络时，MTU 的瓶颈是通信路径上最小的 MTU 值，它被称为路径 MTU。由于路由选择不一定是对称的（从 A 到 B 的路由可能与从 B 到 A 的路由不同），因此，路径 MTU 在两个方向上不一定是一致的，下表是几种常用网络的 MTU 值

IP协议

29

➡ 9.最大传输单元:

网 络 名 称	MTU(单位: 字节)
以太网	1500
IEEE802.3/802.2	1492
FDDI	4352
ATM(信元)	48
X.25	576
点到点(低延时)	296
令牌环网(IBM 16 MB/s)	17 914
令牌环网(IEEE802.5 IBM 16 MB/s)	4464

➡ 10.分片：

把一个数据报为了适合网络传输而分成多个数据报的过程称为分片，被分片后的各个IP数据报可能经过不同的路径到达目标主机。一个IP数据报在传输过程中可能被分片，也可能不被分片。如果被分片，分片后的IP数据报和原来没有分片的IP数据报结构是相同的，即也是由IP头部和IP数据区两个部分组成：分片后的IP数据报，数据区是原IP数据报数据区的一个连续部分，头部是原IP数据报头部的复制，但与原来未分片的IP数据报头部有两点主要不同：标志和片偏移：

IP协议

➡ 10.分片位移及说明图：

片偏移：IP数据报被分片后，各片数据区在原来IP数据区中的位置用13位片偏移来表示。上图中分片1的偏移为0；分片2的偏移为600；分片3的偏移为1200实际在IP地址中,由于偏移是以8个字节为单位进行计算的,因而在IP数据报中分片1的偏移是0；分片2的偏移是75；分片3的偏移是150



IP协议

32

11.接收组包：

重组：

当分了片的IP数据报到达最终目标主机时，目标主机对各分片进行组装，恢复成源主机发送时的IP数据报，这个过程叫做IP数据报的重组。在IP数据报头部中，标识用16位二进制数表示，它唯一地标识主机发送的每一份数据报。在一个数据报被分片时，每个分片仅把数据报“标识”字段的值原样复制一份，所以一个数据报的所有分片具有相同的标识。目标端主机重组数据报的原理是

IP协议

11.接收组包：

重组：

- (1)——根据“标识”字段可以确定收到的分片属于原来哪个IP数据报；
- (2)——根据“标志”字段的“片未完MF”子字段可以确定分片是不是最后一个分片；
- (3)——根据“偏移量”字段可以确定分片在原数据报中的位置

- ➡ 12. IP数据报“选项”主要有两大功能：
 - 1) 用来实现对数据报传输过程中的控制，如规定数据报要经过的路由；
 - 2) 进行网络测试，如一个数据报传输过程中经过了哪些路由器。 IP“选项”域共分为四大类，每类分为若干个选项，每个选项有确定的编号：

IP协议

35

12. IP数据报选项

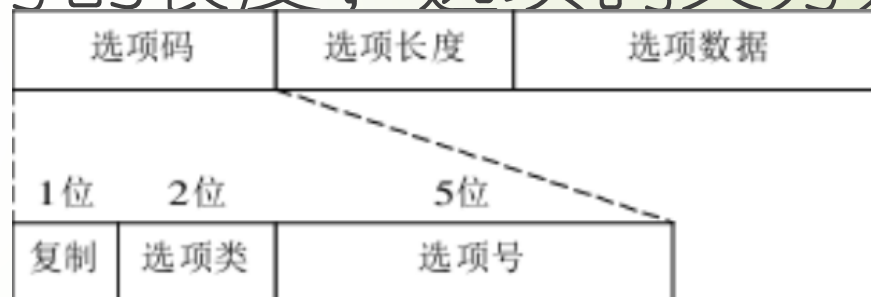
选项类	用 途	选项号	长度	功 能
0 类	数据报或 网络控制	0	—	IP 数据报头中的任选项域结束
		1	—	无操作
		2	11 字节	安全和处理限制(用于军事领域, 详细内容参见 RFC 1108[Kent 1991])
		3	可变	设置宽松源路由选择
		7	可变	记录数据报经过的路由
		9	可变	设置严格源路由选择
1 类	未使用			
2 类	调试与测量		可变	记录 Internet 时戳
3 类	未使用			

IP协议

36

12. IP数据报选项

由三个部分组成：选项码、选项长度和选项数据。选项码和选项长度各占一个字节，中，选项长度用于确定整个选项部分的长度；选项码又分为复制、选项类和选项号：



复制：占一位，用来控制一个带有选项的IP 数据报被分片后对选项的处理方式。该位置1 时将选项复制到所有分片中；置0时将选项仅 复制到第一个分片中。 选项类和选项号用于确定该选项是哪类选项 中的哪个选项，其实就是确定该选项的功能

➡ 12. IP数据报选项

1) 源路由选择：是指IP数据报在互联网中传输时，所经过的路由是由发出IP数据报的源主机指定的，以区别于数据报在互联网中传输时由路由器的IP层自动寻径所得到的路由。通过设置源路由选择选项，可以测试网络中指定路由的连通性，以使数据报绕开出错的网络，也可用于测试特定网络的吞吐量。源路由选择可分为两类：严格源路由选择和宽松源路由选择。

➡ 12. IP数据报选项

(1)——严格源路由选择有发送端规定IP数据报必须经过的路径上的每一个路由器，相邻路由器之间不得有中间路由器，并且所经过的路由器的顺序不可更改。如果一个路由器发送源路由所指定的下一个路由器不在其直接连接的网络上，那么它就返回一个“源路由失败”的ICMP差错报文。严格源路由选择选项格式如下：

1字节	1字节	1字节	4字节	4字节	4字节		4字节
选项码	选项长度	指针	第1站IP地址	第2站IP地址	第3站IP地址	...	第9站IP地址

➡ 12. IP数据报选项

(2)——宽松源路由选择：由发送方指明一个数据报经过的IP地址清单，但是在数据报传输的路径上，在选项中指定的两个IP地址之间可以有其他IP地址的路由器。格式与严格的相同，只是选项码字段值为0x83

➡ 12. IP数据报选项

2) 记录路由：通过设置记录路由选项，IP数据报就可以记录数据报从源主机传输到目标主机时，所经过路径上的各个路由器的IP地址。记录路由选项的数据格式和严格源路由选择格式相同，但选项码字段值为0x87，指针初值为4，指向存放第一个IP地址的位置。每个路由器的IP地址存入选项的数据区中，指针字段的值也随着增加（从4开始到8，12，16，最大到36），它始终指向下一个存放IP地址的位置。当记录了9个IP地址后，指针字段的值为40，表示数据区已满。

IP协议

➤ 12. IP数据报选项

➤ 3) 记录时间戳：就是IP数据报每经过一个路由器都记下它的IP地址和时间。时间戳中的时间以ms为单位，时间戳取值一般为格林威治时间（UT，Universal Time）自午夜开始计时的毫秒数时间戳选项格式如下：

1字节	1字节	1字节	4位	4位	4字节	4字节	4字节	4字节	
选项码	选项长度	指针	溢出	标志	第1站IP地址	第1时间戳	第2站IP地址	第2时间戳	...

时间戳选项的选项码是0x44。选项长度表示选项的总长度（一般为36或40），指针指向下一个可用空间的指针（值为5、9、13等）

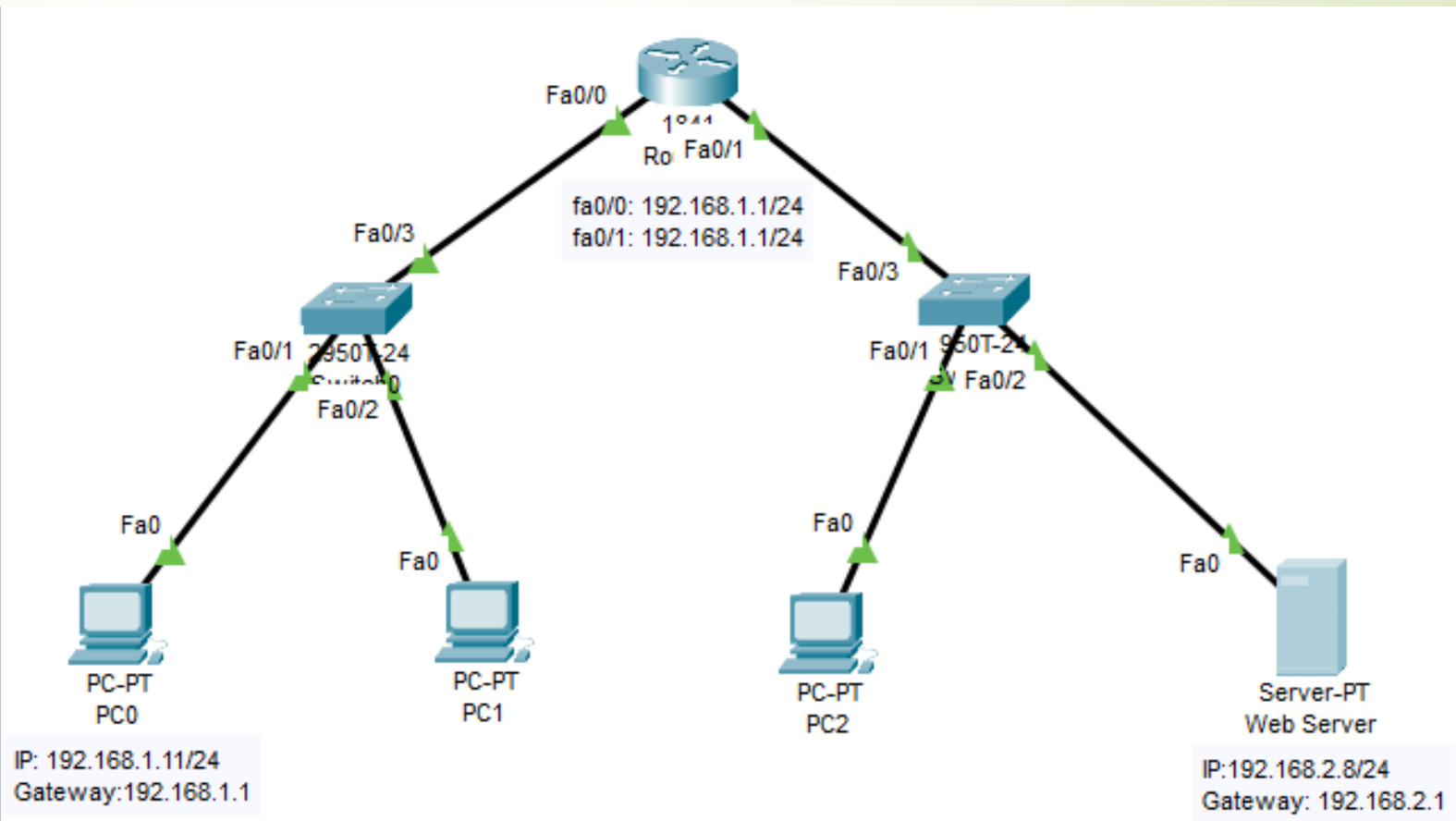
12. IP数据报选项

3) 记录时间戳 “溢出OF”字段表示因时间戳选项数据区空间 不够而未能记录下来的时间戳个数； “标志FL”字段用于控制时间戳选项的格式， 取值如下：

标志字段值	含 义
0	只记录时间戳，不记录 IP 地址，即在图 2-15 所示的格式中去掉 IP 地址项，只记录每台路由器的时间戳。由于没有 IP 地址做参考，所以用途有限
1	记录数据报通过路径时每台路由器的 IP 地址和时间戳。在选项列表中只有存放 4 对 IP 地址和时间戳的空间。其格式与图 2-15 所示的格式一致
3	发送端对选项列表进行初始化，存放了 4 个 IP 地址和 4 个取值为 0 的时间戳值。只有当列表中的下一个 IP 地址与当前路由器地址相匹配时，才记录它的时间戳。这种方式用途较广

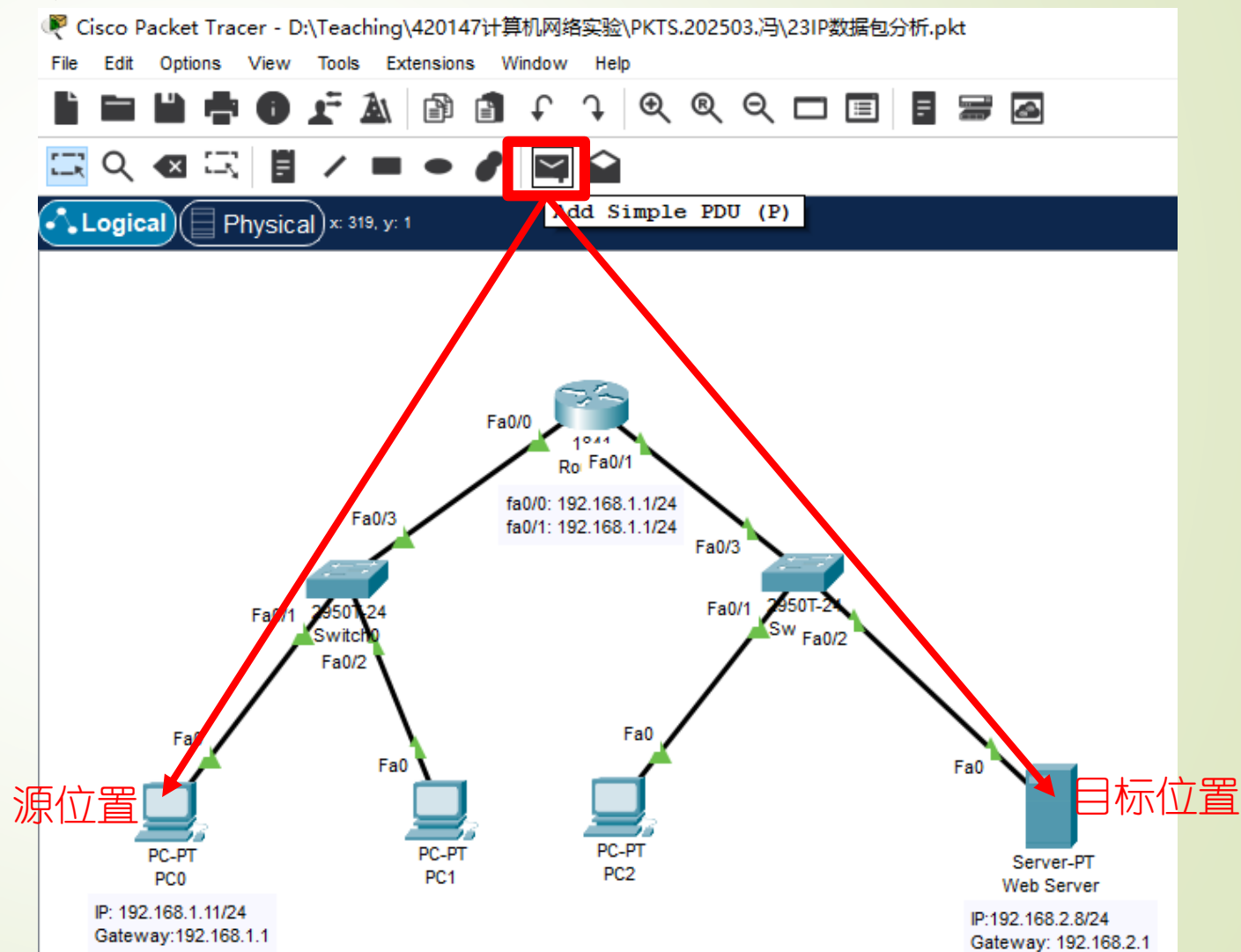
Packet Tracer 分析IP报文实验过程

1, 网络结构图; 2, 设置WEB服务器; 3, 打开PC0浏览器, 输入配置的Web服务器IP地址; 4, 产生IP数据报文



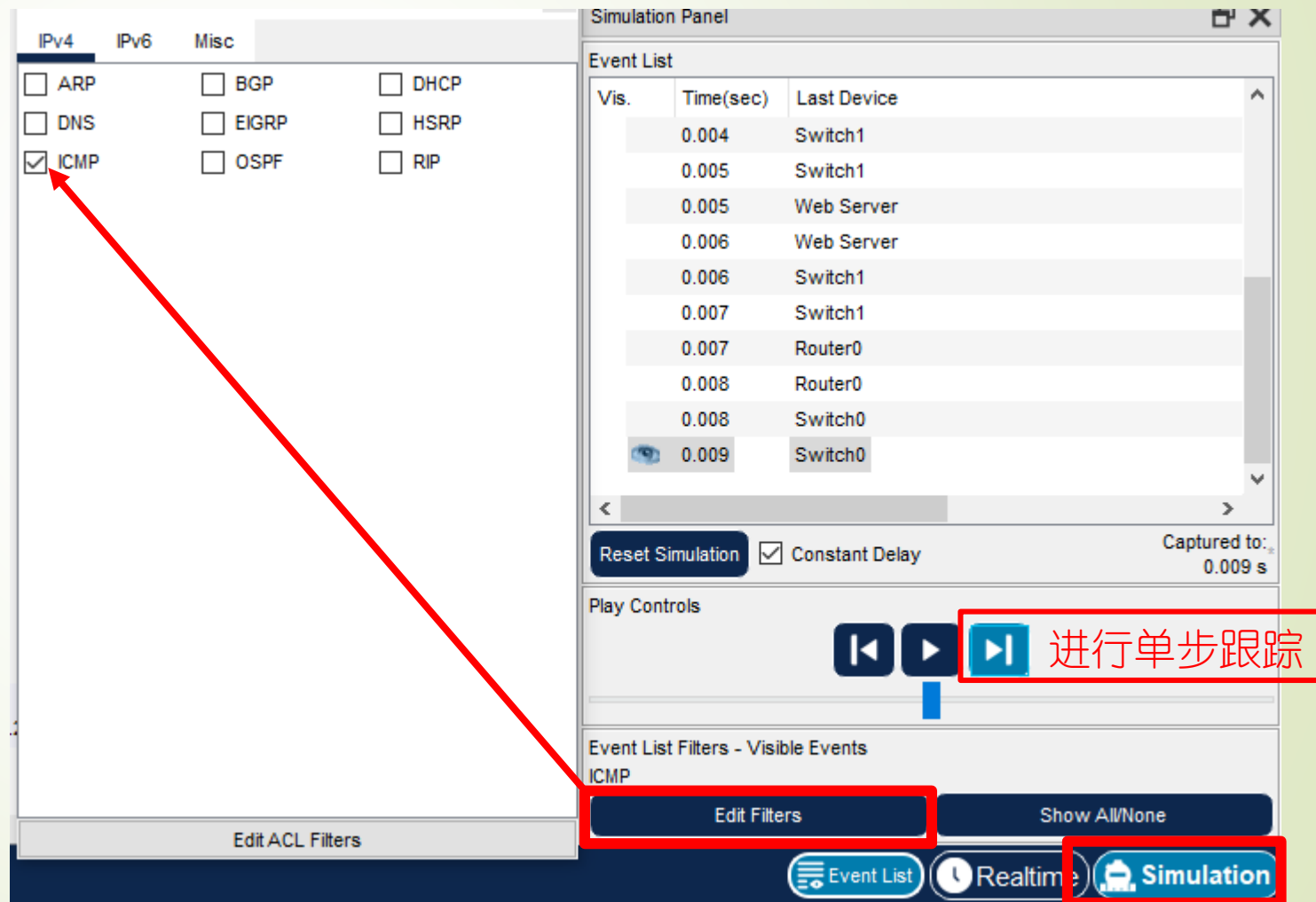
Packet Tracer 分析IP报文实验过程

4, 产生IP数据报文



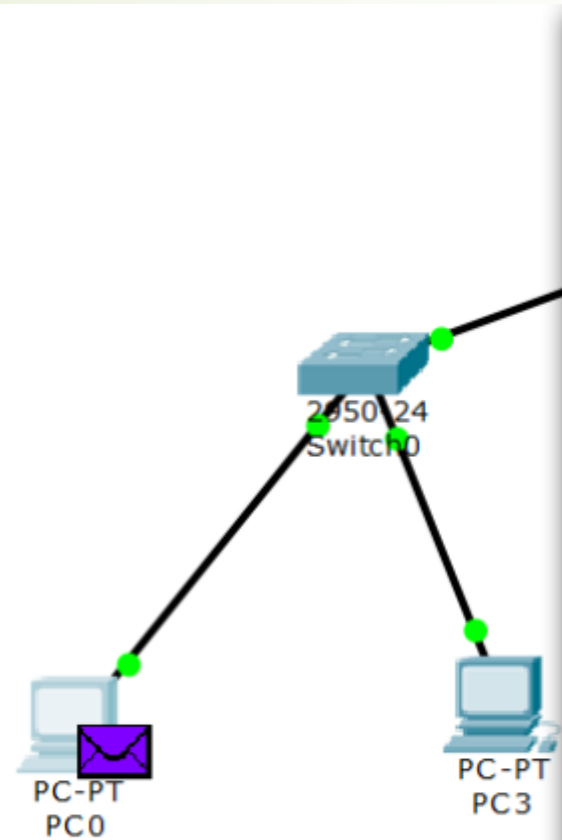
Packet Tracer 分析IP报文实验过程

5, 进入模拟状态, 设置分析协议类型, 进行单步跟踪



Packet Tracer 分析报文

➡ PC0端



PDU Information at Device: PC0

OSI Model

Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0005.5E96.9C01		SRC MAC: 0050.0FAB.0418	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	4	DSCP: 0x0		TL: 120		
ID: 0x16			0x2	0x0		
TTL: 128		PRO: 0x6		CHKSUM		
SRC IP: 192.168.1.11						
DST IP: 192.168.2.8						
OPT: 0x0					0x0	
DATA (VARIABLE LENGTH)						

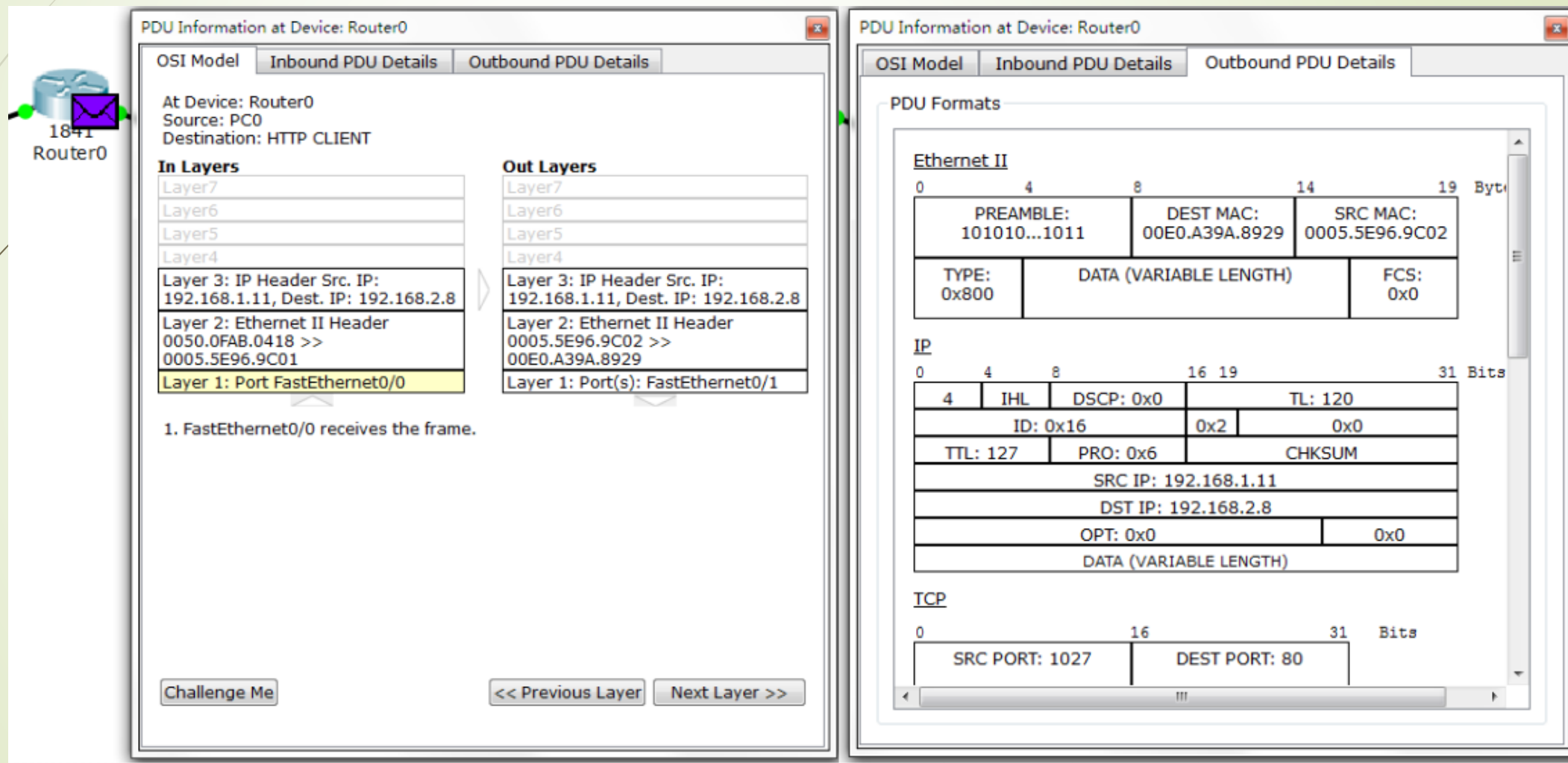
TCP

0	16	31	Bits
SRC PORT: 1027		DEST PORT: 80	

Packet Tracer 分析报文

47

Router0端



PDU Information at Device: Router0

At Device: Router0
Source: PC0
Destination: HTTP CLIENT

In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.2.8
Layer 2: Ethernet II Header 0050.0FAB.0418 >> 0005.5E96.9C01
Layer 1: Port FastEthernet0/0

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.2.8
Layer 2: Ethernet II Header 0005.5E96.9C02 >> 00E0.A39A.8929
Layer 1: Port(s): FastEthernet0/1

1. FastEthernet0/0 receives the frame.

PDU Information at Device: Router0

PDU Formats

Ethernet II

0	4	8	14	19	Byte
PREAMBLE: 101010...1011		DEST MAC: 00E0.A39A.8929		SRC MAC: 0005.5E96.9C02	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL		DSCP: 0x0		TL: 120	
ID: 0x16				0x2	0x0	
TTL: 127		PRO: 0x6		CHKSUM		
SRC IP: 192.168.1.11						
DST IP: 192.168.2.8						
OPT: 0x0					0x0	
DATA (VARIABLE LENGTH)						

TCP

0	16	31	Bits
SRC PORT: 1027		DEST PORT: 80	

Packet Tracer 分析报文

48

Switch0端

PDU Information at Device: Server0

At Device: Server0
Source: PC0
Destination: HTTP CLIENT

OSI Model Inbound PDU Details Outbound PDU Details

In Layers

Layer 7: HTTP
Layer 6
Layer 5
Layer 4: TCP Src Port: 1027, Dst Port: 80
Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.2.8
Layer 2: Ethernet II Header 0005.5E96.9C02 >> 00E0.A39A.8929
Layer 1: Port FastEthernet0

Out Layers

Layer 7: HTTP
Layer 6
Layer 5
Layer 4: TCP Src Port: 80, Dst Port: 1027
Layer 3: IP Header Src. IP: 192.168.2.8, Dest. IP: 192.168.1.11
Layer 2: Ethernet II Header 00E0.A39A.8929 >> 0005.5E96.9C02
Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

Challenge Me << Previous Layer Next Layer >>

PDU Information at Device: Server0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 00E0.A39A.8929		SRC MAC: 0005.5E96.9C02	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits	
4		IHL		DSCP: 0x0		TL: 120	
ID: 0x16				0x2		0x0	
TTL: 127		PRO: 0x6		CHKSUM			
SRC IP: 192.168.1.11							
DST IP: 192.168.2.8							
OPT: 0x0					0x0		
DATA (VARIABLE LENGTH)							

TCP

0	16	31	Bits
SRC PORT: 1027		DEST PORT: 80	
SEQUENCE NUM: 1			
ACK NUM: 1			

Packet Tracer 分析报文

49

Server0端

PDU Information at Device: Server0

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

Ethernet II

0481419 Bytes

PREAMBLE: 101010...1011		DEST MAC: 00E0.A39A.8929		SRC MAC: 0005.5E96.9C02	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0	

IP

048161931 Bits

4	IHL	DSCP: 0x0	TL: 120	
ID: 0x16		0x2	0x0	
TTL: 127	PRO: 0x6	CHKSUM		
SRC IP: 192.168.1.11				
DST IP: 192.168.2.8				
OPT: 0x0			0x0	
DATA (VARIABLE LENGTH)				

TCP

01631 Bits

SRC PORT: 1027		DEST PORT: 80	
SEQUENCE NUM: 1			
ACK NUM: 1			

PDU Information at Device: Server0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0005.5E96.9C02		SRC MAC: 00E0.A39A.8929	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 491			
ID: 0x8		0x2	0x0			
TTL: 128	PRO: 0x6		CHKSUM			
SRC IP: 192.168.2.8						
DST IP: 192.168.1.11						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

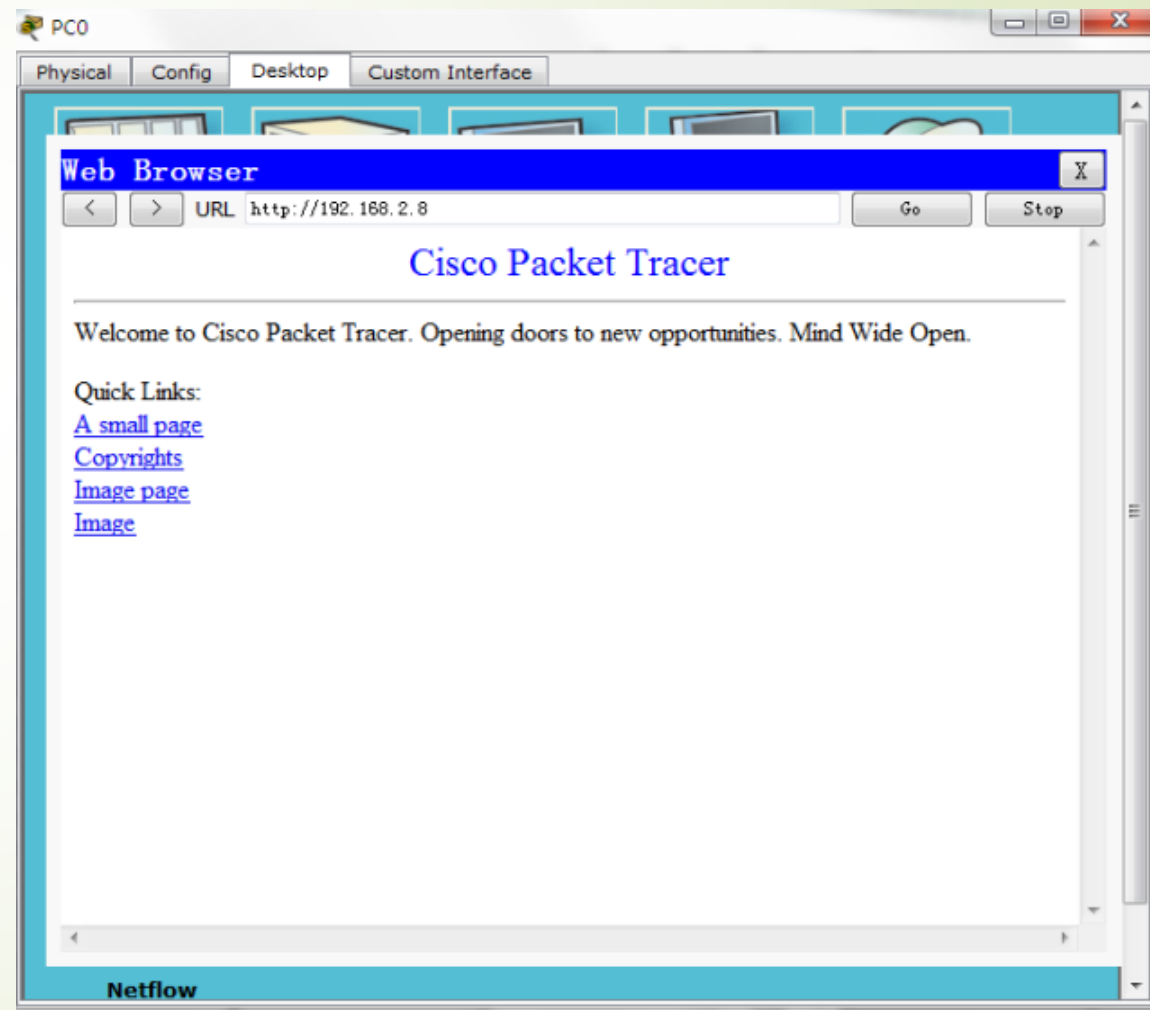
TCP

0	16	31	Bits
SRC PORT: 80		DEST PORT: 1027	
SEQUENCE NUM: 1			
ACK NUM: 101			

Packet Tracer 分析报文

50

➡ PC0 WEB Browser

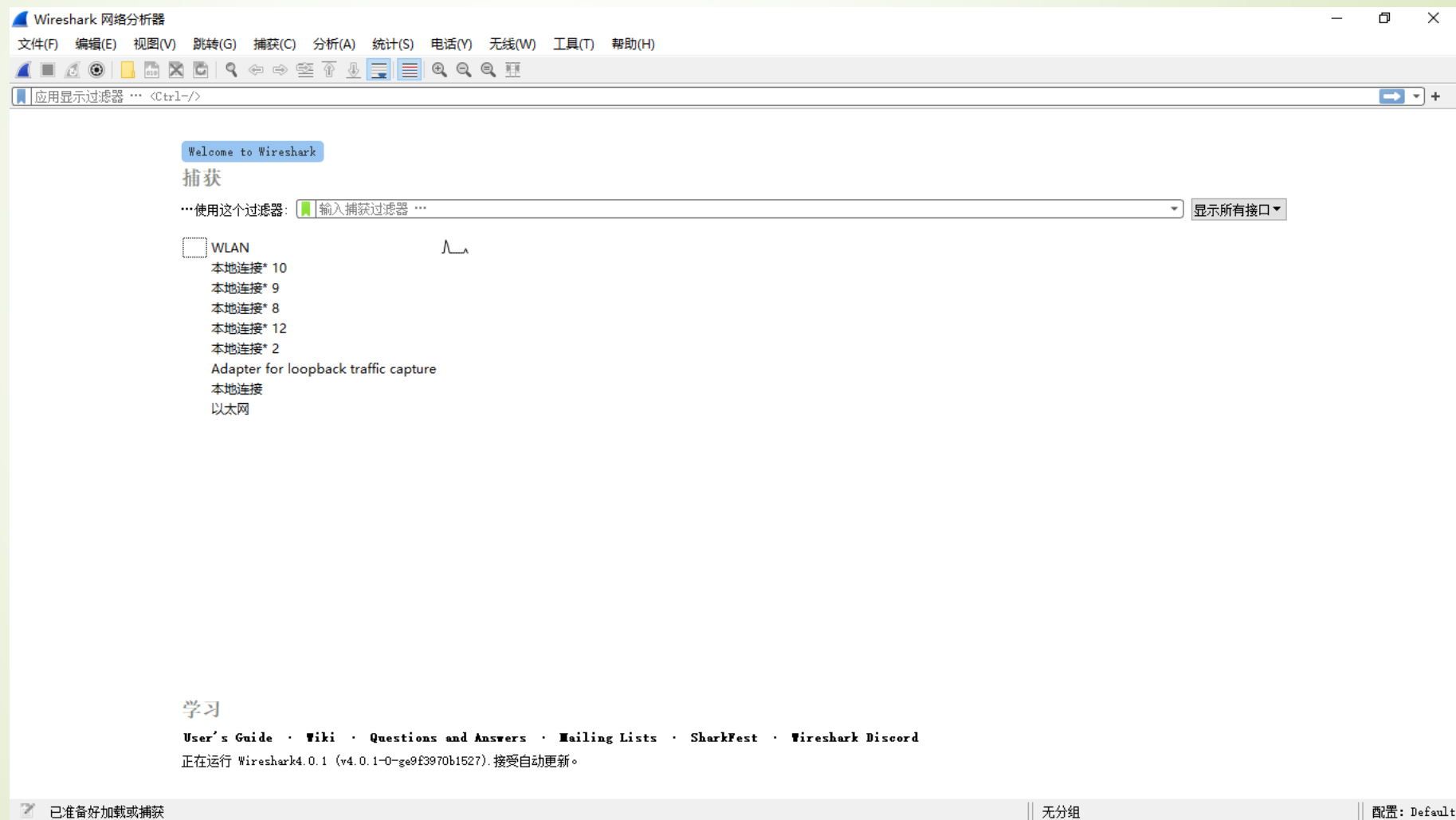


Wireshark进行本地网络IP协议抓包

➡ 点击图标

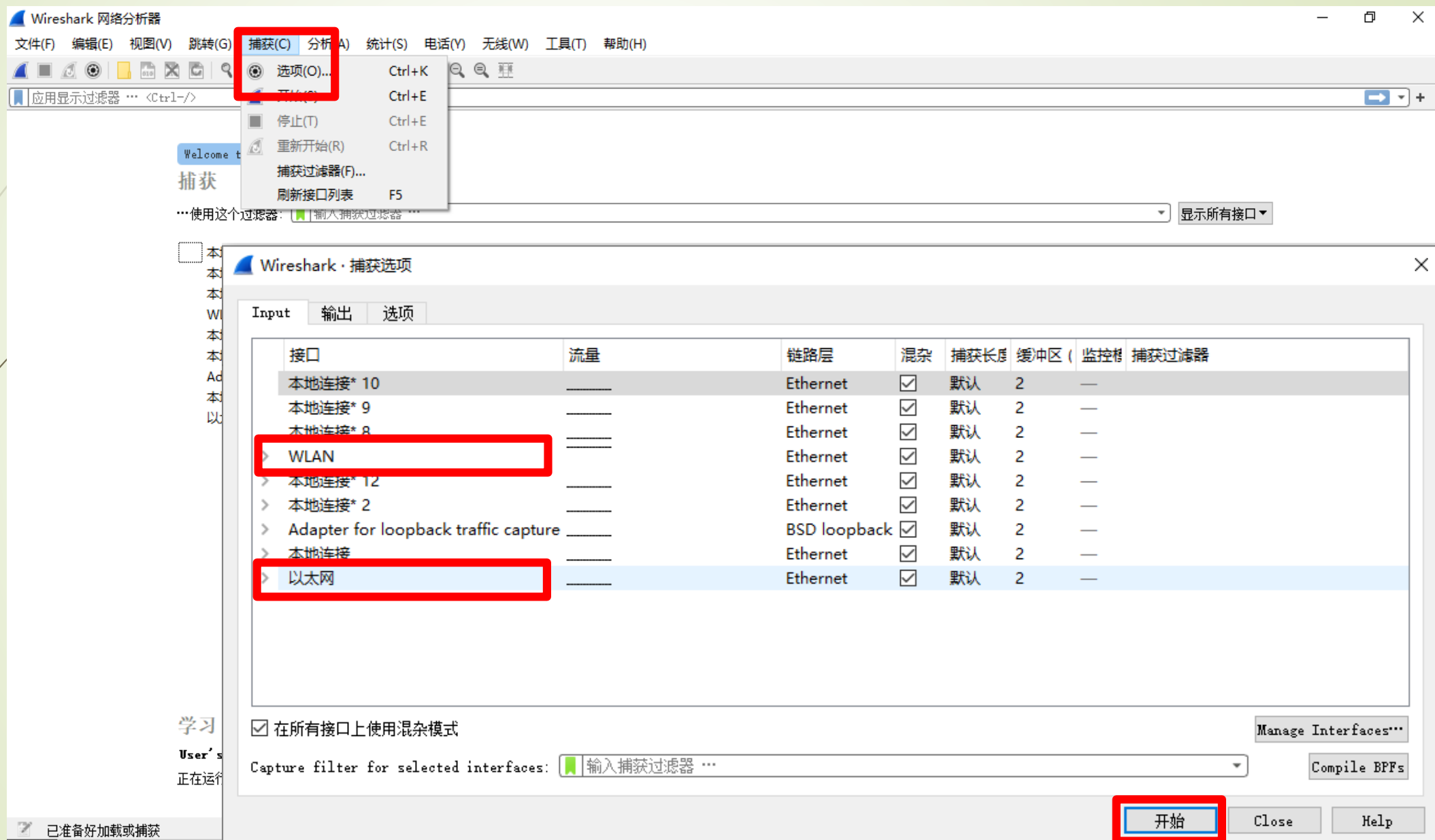


打开Wireshark软件



捕获->选项->以太网/WLAN ->开始

53



Wireshark进行IP协议抓包

54

14. Wireshark IP报文抓取分析（过滤器设置成ip）

Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: **ip** Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
212637	1066.52219	192.168.1.4	183.194.169.61	UDP	Source port: italk Destination port: wiegand
212640	1066.54870	183.192.227.208	192.168.1.4	UDP	Source port: 12166 Destination port: italk
212641	1066.56485	117.143.177.10	192.168.1.4	UDP	Source port: 4398 Destination port: italk
212642	1066.56566	192.168.1.4	117.143.177.10	UDP	Source port: italk Destination port: 4398
212643	1066.56576	192.168.1.4	183.192.9.126	UDP	Source port: italk Destination port: 12438
212644	1066.56583	192.168.1.4	183.193.40.103	UDP	Source port: italk Destination port: csdmbase
212645	1066.56590	192.168.1.4	117.143.117.111	UDP	Source port: italk Destination port: ssowatch
212646	1066.56724	117.143.177.10	192.168.1.4	UDP	Source port: 4398 Destination port: italk
212647	1066.56736	192.168.1.4	117.143.177.10	UDP	Source port: italk Destination port: 4398
212648	1066.56892	183.194.169.61	192.168.1.4	UDP	Source port: wiegand Destination port: italk
212649	1066.57519	192.168.1.4	117.143.177.10	UDP	Source port: italk Destination port: 4398
212650	1066.59523	192.168.1.4	183.195.56.223	UDP	Source port: italk Destination port: aipn-reg
212651	1066.60170	183.193.17.10	192.168.1.4	UDP	Source port: 13037 Destination port: italk
212652	1066.61420	192.168.1.4	183.192.227.208	UDP	Source port: italk Destination port: 12166
212653	1066.63028	192.168.1.4	117.143.177.10	UDP	Source port: italk Destination port: 4398

Frame 212645: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)

- Ethernet II, Src: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2), Dst: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
 - Destination: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
 - Source: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)
 - Type: IP (0x0800)
- Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 117.143.117.111 (117.143.117.111)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - 0000 00.. = Differentiated services codepoint: Default (0x00)
 -0. = ECN-Capable Transport (ECT): 0
 -0 = ECN-CE: 0
 - Total Length: 82
 - Identification: 0x37d5 (14293)
 - Flags: 0x00
 - 0... = Reserved bit: Not set
 - .0. = Don't fragment: Not set
 - ..0. = More fragments: Not set
 - Fragment offset: 0
 - Time to live: 128
 - Protocol: UDP (17)
 - Header checksum: 0x561b [correct]
 - [Good: True]
 - [Bad: False]
 - Source: 192.168.1.4 (192.168.1.4)
 - Destination: 117.143.117.111 (117.143.117.111)
- User Datagram Protocol, Src Port: italk (12345), Dst Port: ssowatch (3644)
 - Source port: italk (12345)
 - Destination port: ssowatch (3644)
 - Length: 62
 - Checksum: 0x8388 [validation disabled]
 - [Good Checksum: False]
 - [Bad Checksum: False]
 - Data (54 bytes)
 - Data: 2c620f6547920a098b76aaf95608cfc798f76ed0084e7adc...
 - [Length: 54]

实验主要分析内容

- ➡ 1.配置Web服务器，并从客户端查看；
- ➡ 2.分析在PT软件中IP报文中各部分字段具体内容
- ➡ 3.用WireShark抓取IP数据包。
- ➡ 4.查看IP报文各字段内容，并解读；