华为HCIA数通认证

Huawei HCIA Course

学完本课程后，将能够：

- 理解应用和数据
- 理解网络参考模型与标准协议
- 理解数据通信过程

应用

- 应用，是为满足人们各种需求，比如访问网页，在线游戏，在线视频等。
- 应用会有信息的产生。比如文本、图片、视频等都是信息的不同呈现方式。

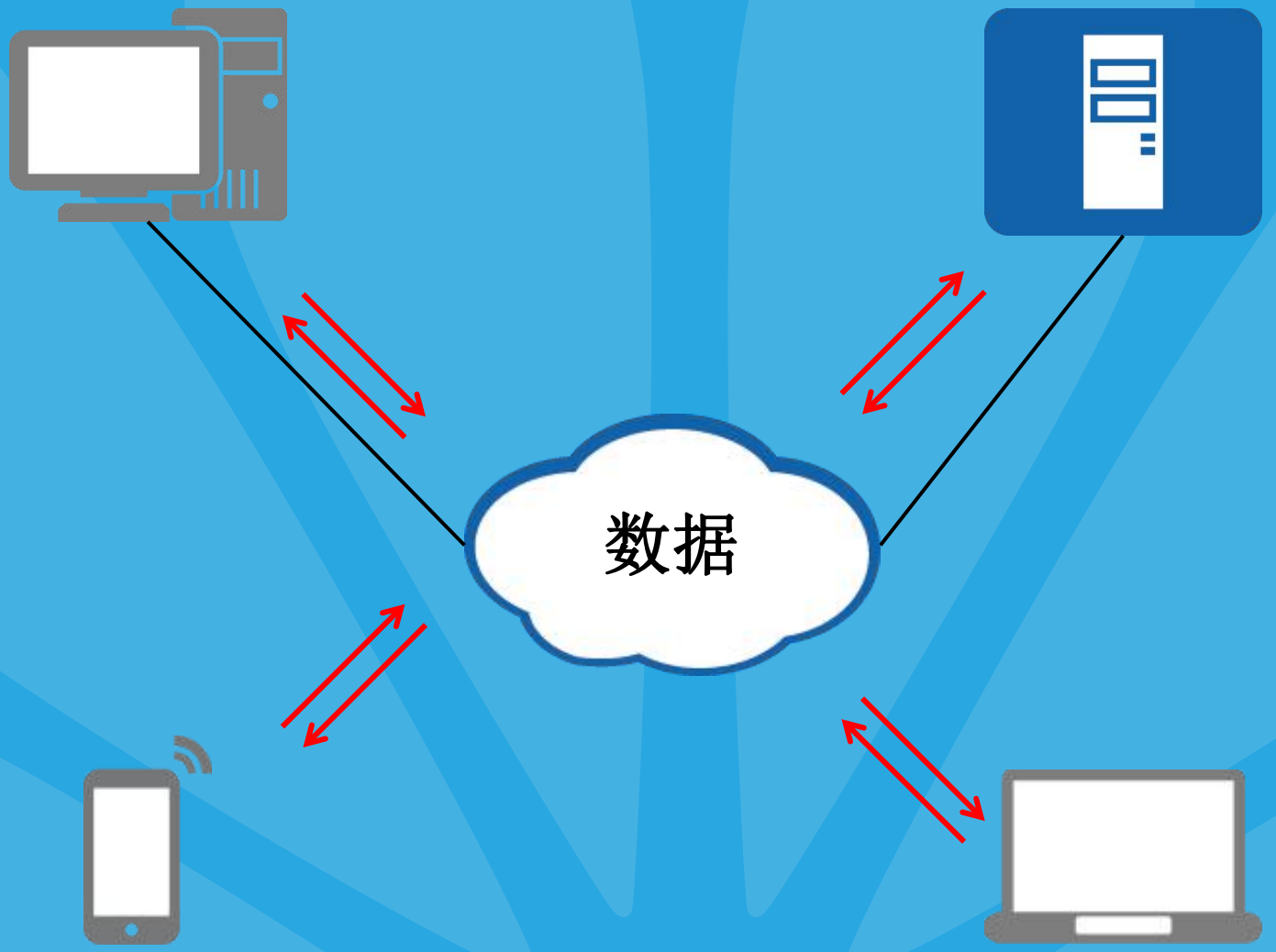
应用的实现 – 数据

- **数据的产生**

  数据是各种信息的载体

- **数据传输**

  数据需要在不同的设备之间传递



OSI参考模型

7.应用层	对应用程序提供接口
6.表示层	进行数据格式的转换，确保一个系统生成的应用层数据能够被另外一个系统的应用层所识别和理解。
5.会话层	通信双方之间建立、管理和终止会话。
4.传输层	建立、维护和取消一次端到端的数据传输过程。控制传输节奏的快慢，调整数据的排序等。
3.网络层	定义逻辑地址；实现数据从源到目的地的转发。
2.数据链路层	将分组数据封装成帧；在数据链路上实现数据的点到点、或点到多点方式的直接通信；差错检测。
1.物理层	在媒介上传输比特流

TCP/IP参考模型

- OSI协议栈比较复杂，且TCP和IP两大协议在业界被广泛使用，所以TCP/IP参考模型成为主流。

TCP/IP常见协议

- TCP/IP协议栈定义了一系列的标准协议。

应用层	Telnet	FTP	TFTP	SNMP
	HTTP	SMTP	DNS	DHCP
传输层	TCP		UDP	
网络层	ICMP		IGMP	
	IP			
数据链路层	PPPoE			
	Ethernet		PPP	
物理层	.....			

发送方数据封装

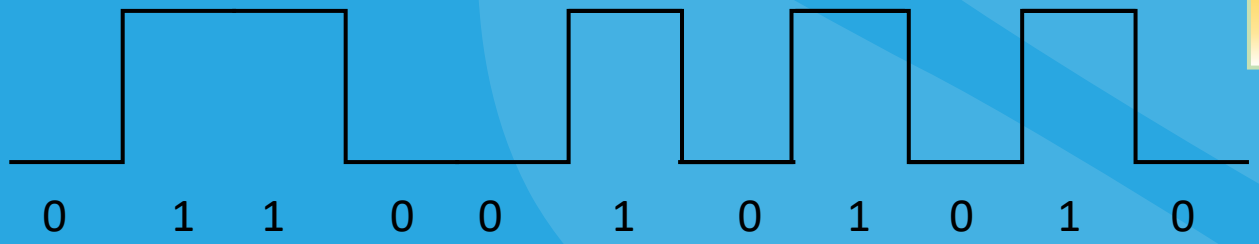
www.huawei.com

DATA

TCP Header | DATA

TCP Header | Payload

TCP Header | Payload | FCS



应用层

传输层

网络层

数据链路层

物理层

数据 DATA

段 Segment

包 Packet

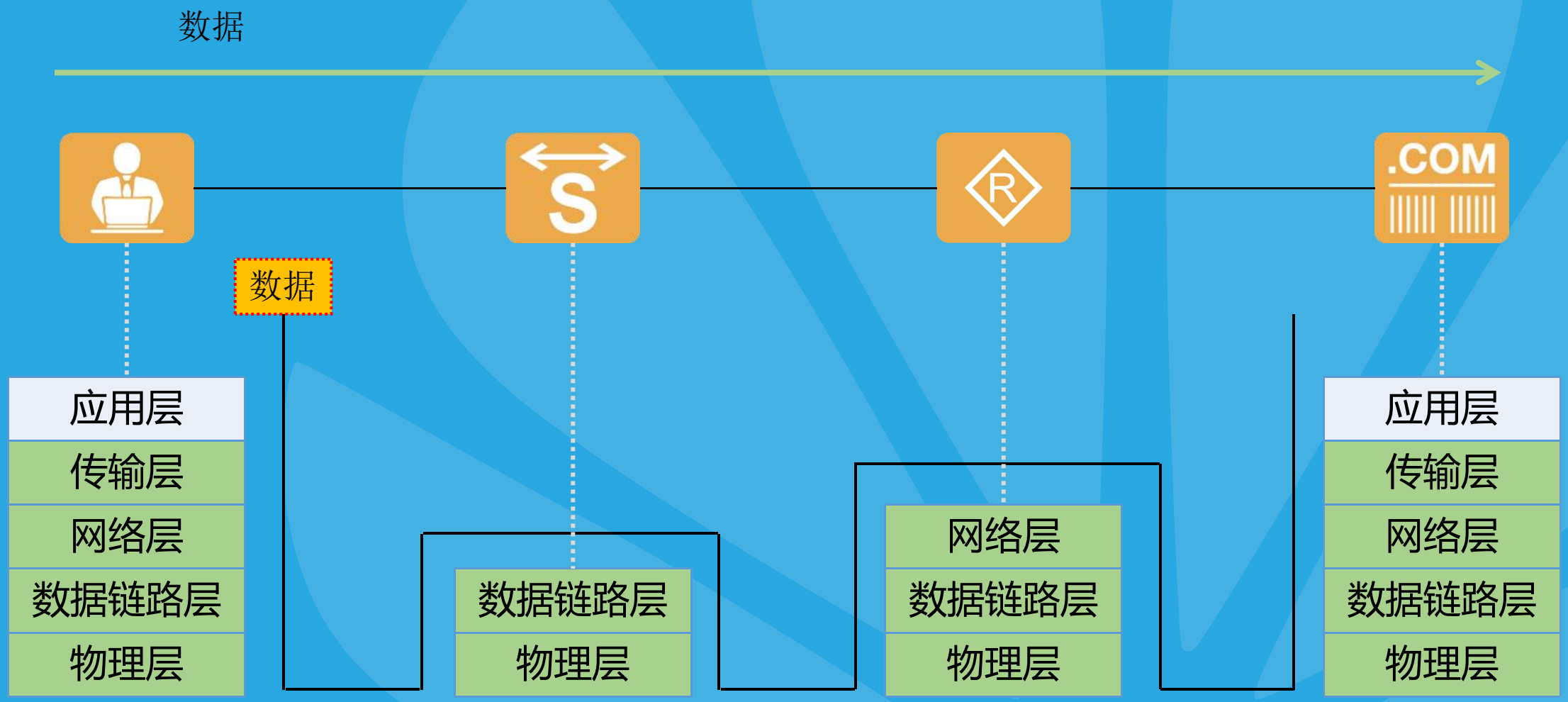
帧 Frame

位 Bit

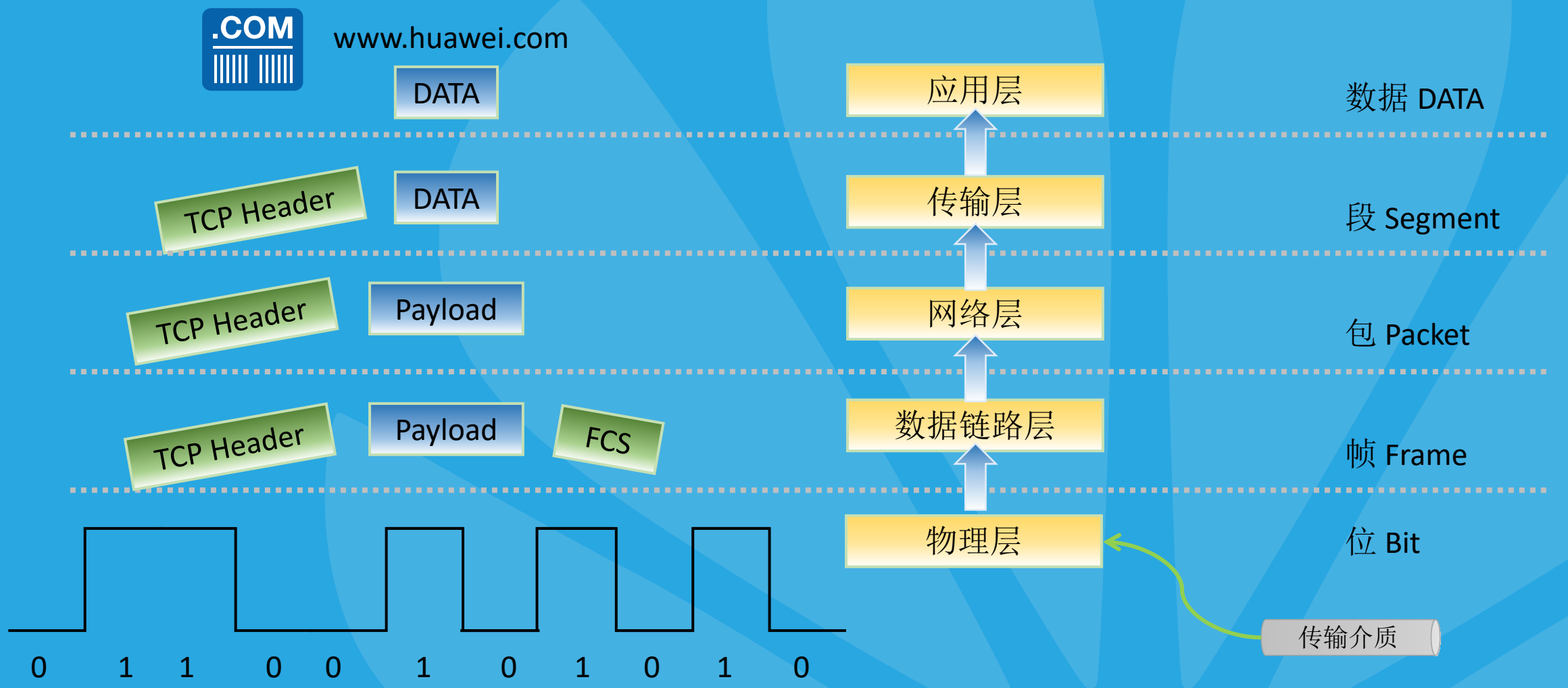
传输介质

网络数据传输

- 封装好的完整数据，将会在网络中被传递。



接收方数据解封装


.COM
www.huawei.com
DATA
TCP Header
DATA
TCP Header
Payload
TCP Header
Payload
FCS
0 1 1 0 0 1 0 1 0 1 0
应用层
传输层
网络层
数据链路层
物理层
数据 DATA
段 Segment
包 Packet
帧 Frame
位 Bit
传输介质

小结

- OSI参考模型和TCP/IP参考模型，都采用分层设计理念。

  各层之间分工、界限明确，有助于各部件的开发、设计和故障排除

  定义模型每一层的功能，实现产业标准化

  通过提供接口的方式，使得各种类型网络硬件和软件相互通信，提高兼容性

- 数据的产生与传递，需要各模块之间相互协作，同时各模块又需要“各司其职”。

物理层

- 物理层会根据物理介质不同，将数字信号转换成光信号、电信号或电磁波信号。
- 物理层的PDU称为比特流（Bitstream）

物理层位于模型最底层：

- 负责比特流在介质上的传输
- 规范了线缆、针脚、电压、接口等物理特性规范。
- 常见传输介质有：双绞线、光纤、电磁波等。

常见传输介质

双绞线传输

光纤传输

串口线缆传输

无线传输

无线路由器

平板

手机

认识二进制

- 进制，即表述数据的方法
- 进制类型：10进制、2进制、16进制
- 10进制：组成数据的基本单元，包含0~9

  主要是让人看
- 2进制：组成数据的基本单元，包含0~1

  主要是让设备看
- 16进制：组成数据的基本单元，包含0~9，a~f

  通常用在“抓包软件”中，用于分析协议数据包内容

常见的进制转换

- 2进制转10进制

  常见应用场景：IP地址的识别和表示

  例如：IP地址表示格式为：11000000 . 10101000 . 00000001 . 00000001 即 192.168.1.1

- 10进制转2进制

  常见应用场景：判断IP地址是否同网段

  例如：判断PC1(192.168.1.1/24) 和 PC2（192.168.1.210/24）是否为同一网段。

2进制转换10进制

- 10进制表示方法

  $127 = 1*10^2 + 2*10^1 + 7*10^0$

- 2进制表示方法

  $10101110 = 1*2^7 + 0*2^6 + 1*2^5 + 0*2^4 + 1*2^3 + 1*2^2 + 1*2^1 + 0*2^0$

- 2进制转10进制的核心

  牢记2n的结果，n=0~7

  1，2，4，8，16，32，64，128

10进制转换2进制

- 10进制转2进制

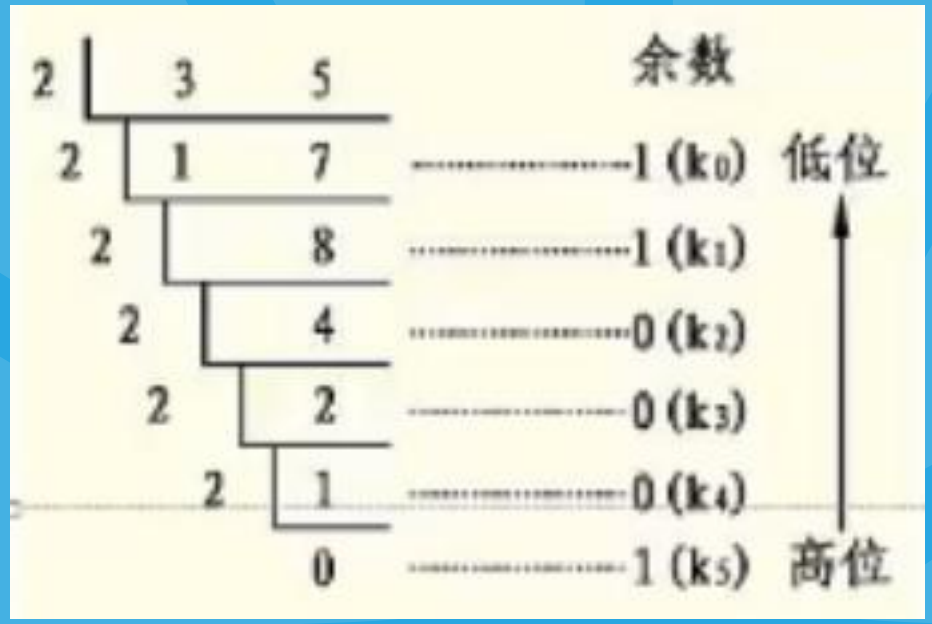
  常见应用场景:IP地址的识别、表示和判断

  例如：IP地址表示格式为：192.168.1.1 255.255.255.0

- 10进制转2进制的核心

  将10进制除以2，将最终的“余数”组合一起，变成8个2进制数，不足8位用零补全。

  10进制35转换2进制为：00100011



小结

- 理解物理层功能
- 了解常见物理层设备
- 掌握常见进制转换

数据链路层

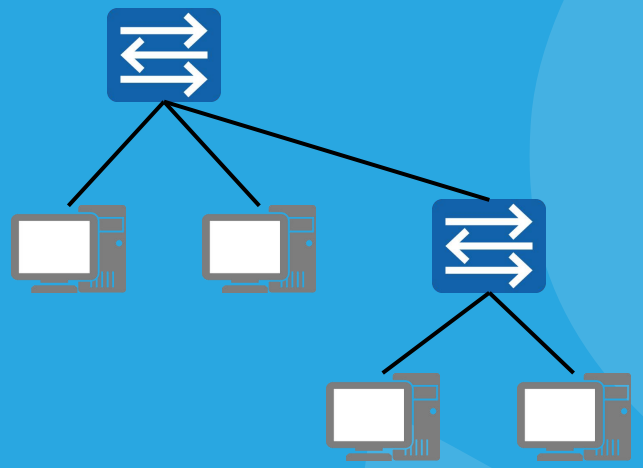
- 数据链路层位于网络层和物理层之间，可以向网络层的IP、IPv6等协议提供服务。数据链路层的PDU被称为Frame（帧）
- 以太网（Ethernet）是最常见的数据链路层协议

数据链路层位于网络层和物理层之间：

- 数据链路层向网络层提供“段内通信”
- 负责组帧、物理编址、差错控制功能
- 常见数据链路层协议有：以太网、PPPoE、PPP等

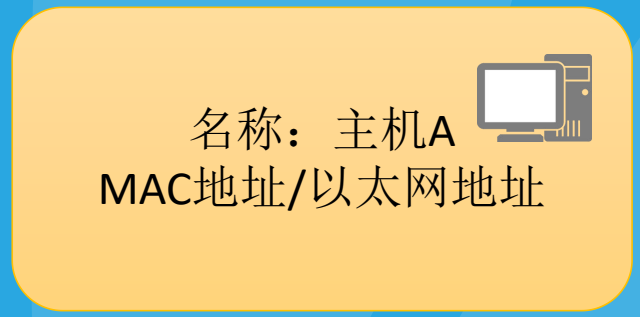
数据链路层

以太网定义



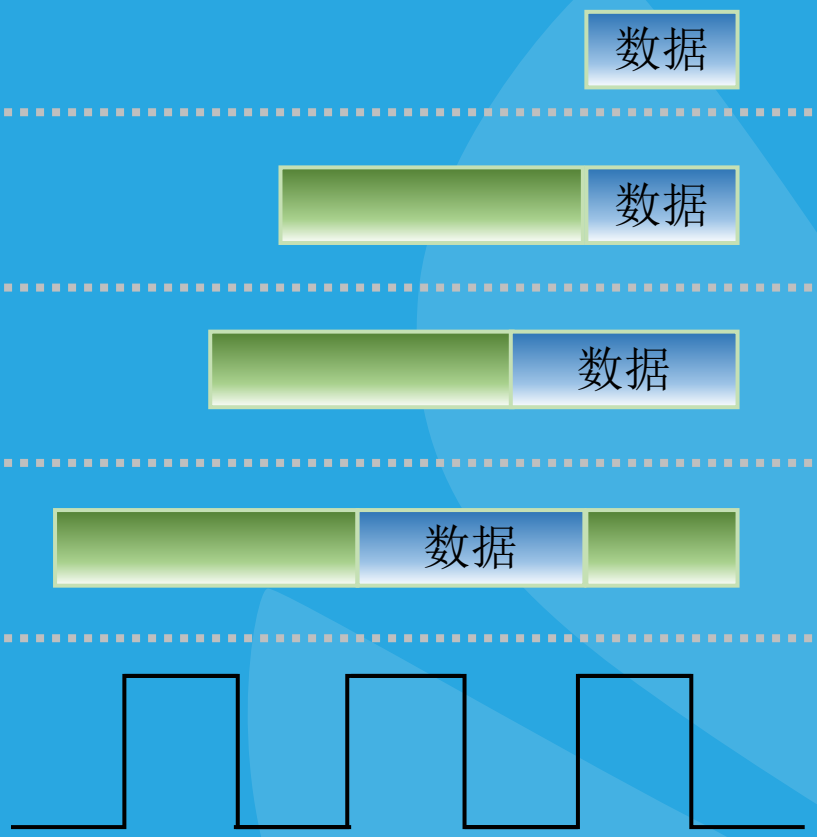
- 以太网是一种广播式数据链路层协议，支持多点接入
- PC的网络接口遵循以太网标准
- 一般情况，一个广播域对应一个IP网段

以太网MAC地址



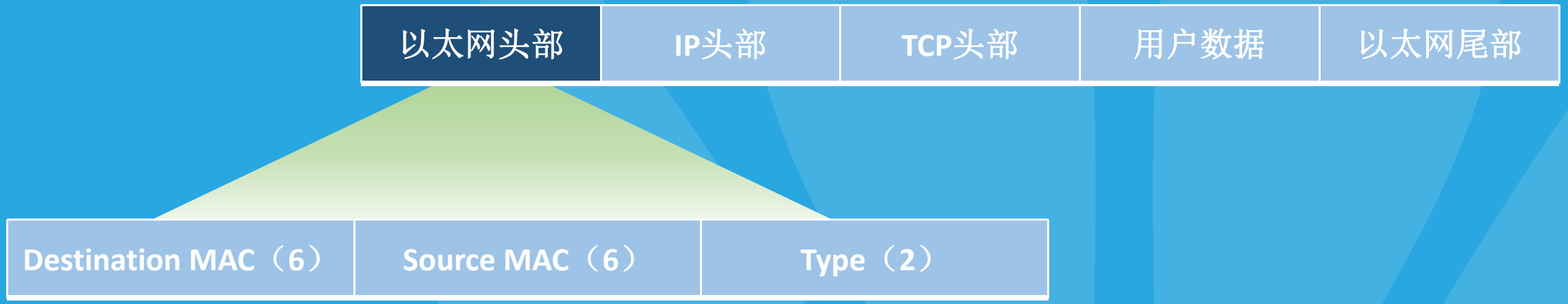
- MAC（media access control）地址在网络中唯一标识一个网卡，每个网卡都需要，且会有唯一的一个MAC地址
- MAC用于在一个IP网段内，寻址找到具体的物理设备
- 工作在数据链路层的设备，例如交换机，会维护一张MAC地址表，用于指导数据帧转发

数据封装



以太网头部	IP头部	TCP头部	用户数据	以太网尾部

以太网报文格式



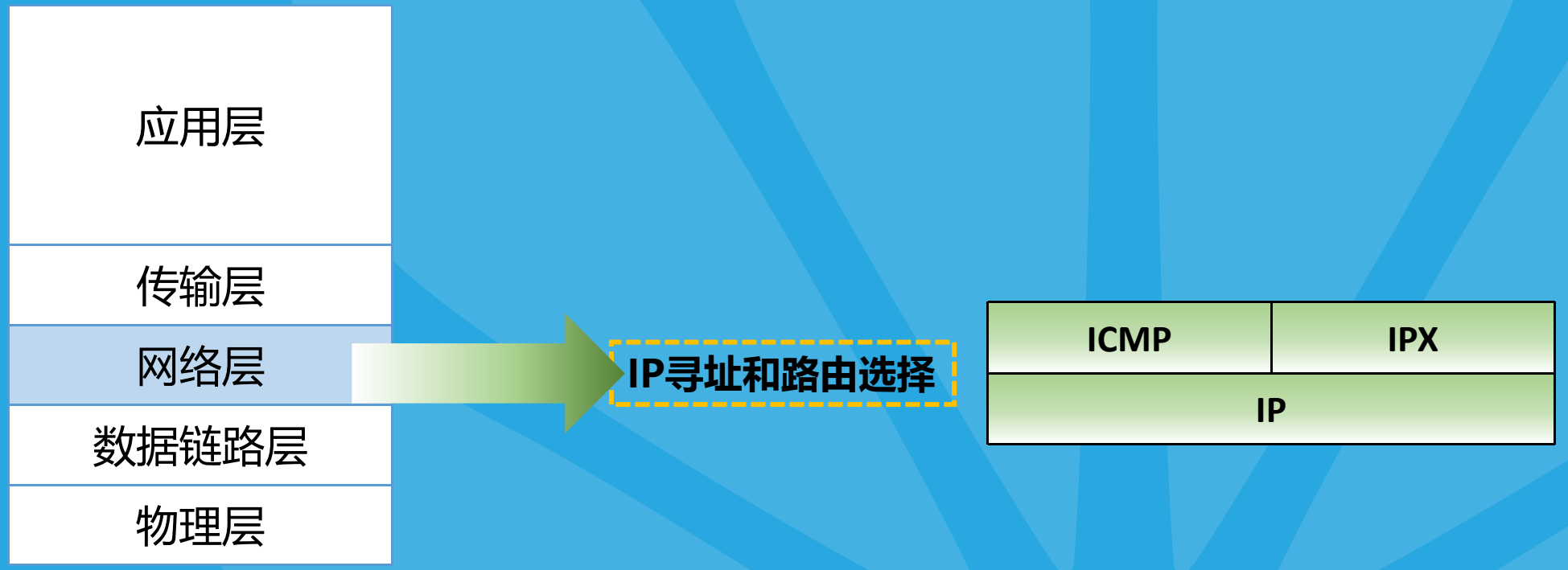
- 任何一个可以上网的节点，都拥有一个MAC地址，该地址全世界范围内唯一
- MAC地址，表示的是一个网络设备，不可以随意修改
- 任何一个可以上网 的节点，也必须拥有一个IP地址，该地址在一个网段内是唯一
- IP地址，也称为一个上网设备的“逻辑地址”，可以随意修改
- 想要设备之间实现互通，必须同时知道目标设备的IP地址和MAC地址

小结

- 理解数据链路层功能，及常见的二层协议
- 理解数据封装的结构及以太网协议的报文格式
- 理解MAC地址结构和作用
- 理解MAC地址和IP地址之间的关系

网络层协议

- 网络层协议也称IP层。但网络层协议并不只是IP协议，还包括ICMP协议、IPX协议等。

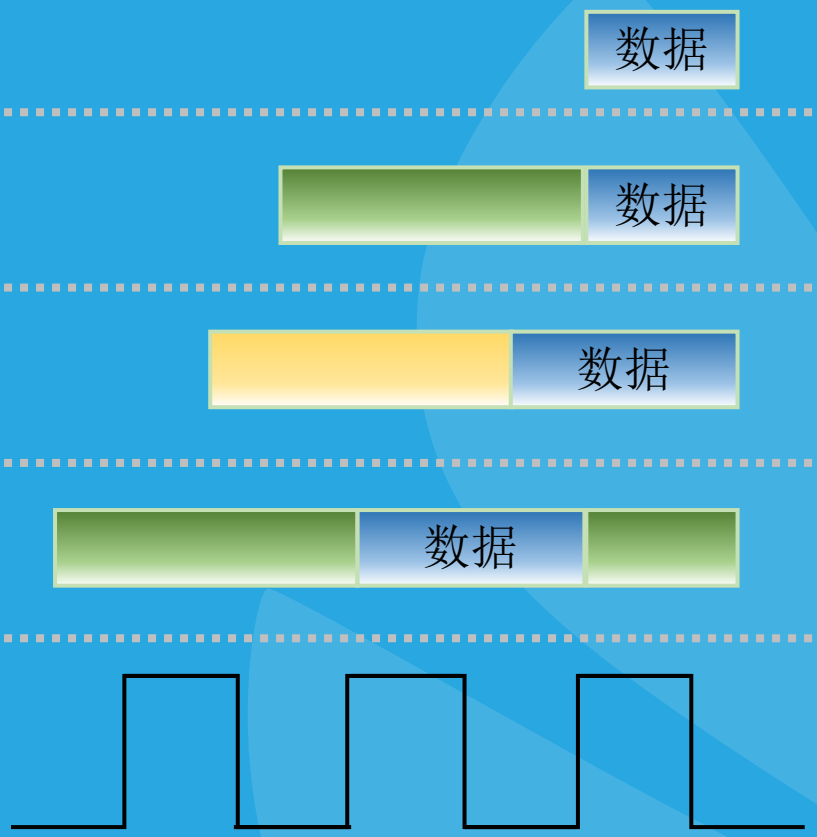


IP协议

- IP是Internet Protocol的缩写，该协议文件的内容非常少，主要是定义并阐述IP报文的格式。
- 经常提及的IP，一般不是特指Internet Protocol这个协议文件本身，而是泛指直接或间接与IP协议相关的任何内容。

作用	版本
◆ 为网络层设备提供逻辑地址 ◆ 负责数据包寻址与转发	◆ IPv4 ◆ IPv6

数据封装



以太网头部	IP头部	TCP头部	用户数据	以太网尾部

IPv4报文格式

以太网头部	IP头部	TCP头部	用户数据	以太网尾部

固定长度
20Byte

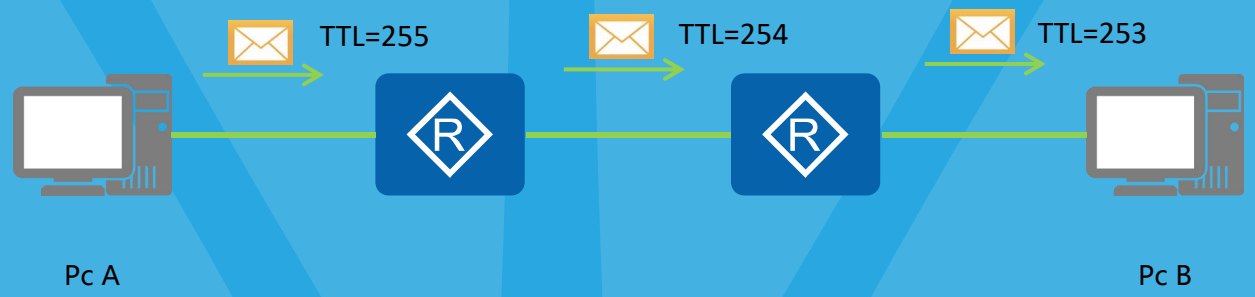
可选长度
0~40Byte

Version	Header Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding

生存时间 Time to Live

- TTL字段设置了数据包可以经过的路由器数目。
- 一旦经过一个路由器，TTL值会减1，当该字段值为0时，数据包被丢弃。

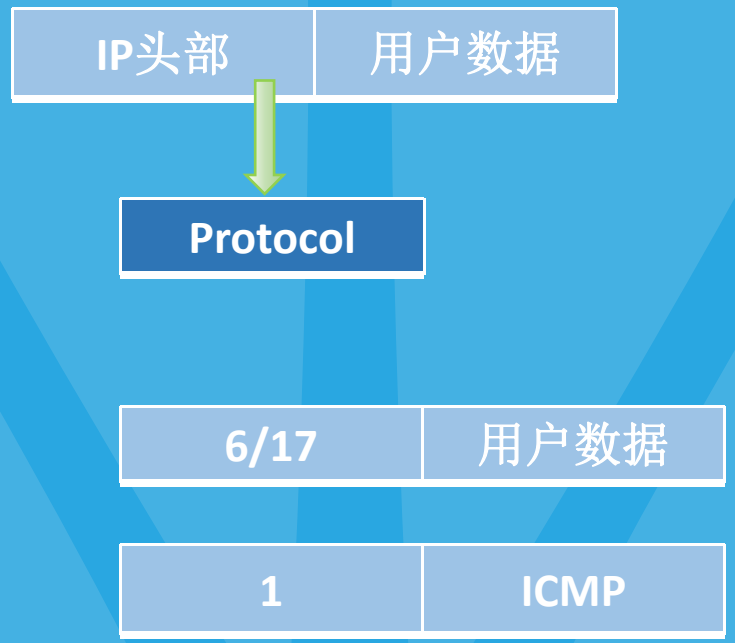
Version	Header Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding



协议号 Protocol

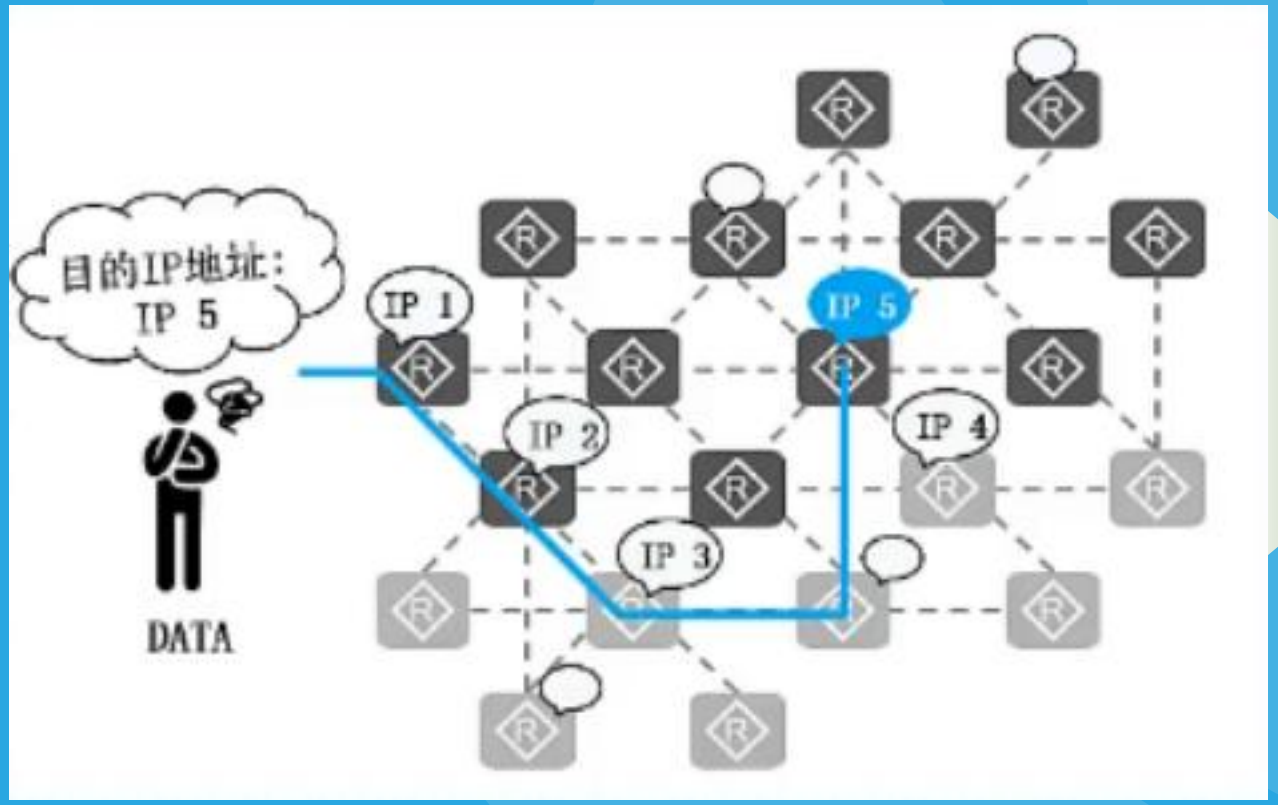
- IP报文头中的协议号字段标识了将会继续处理该报文的协议。
- 即指出此数据包携带的数据使用何种协议，以便目的主机的IP层将数据部分上报给哪个进程处理。

Version	Header Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding



IP地址

- IP地址在网络中标识一个节点或网络设备的接口。
- IP地址用于IP报文在网络中的寻址。



IP地址

IP地址像现实中的地址，用于标识网络中的一个节点，数据就是通过它来找到目的地。

IP地址表示

- IPv4地址有32bit。
- IPv4通常采用“点分十进制”表示
- IPv4地址范围：0.0.0.0~255.255.255.255

点分十进制表示法

十进制	192	168	10	1	4 byte
二进制	11000000	10101000	00001010	00000001	32 bit

十进制转二进制

幂	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	64	32	16	8	4	2	1
位	1	1	0	0	0	0	0	0

= 128 + 64
= 192

IP地址构成

- 网络部分：用来标识一个网络。
- 主机部分：用来区分一个网络内不同的主机。
- 网络掩码：区分一个IP地址中网络部分及主机部分。

网络部分			主机部分
192	168	10	1

192.168.10.1	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1
255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

网络部门

主机部门

192.168.10.1 /255.255.255.0 = 192.168.10.1/24

IP地址寻址

- 网络部分：用来标识一个网络，代表IP地址所属网络。
- 主机部分：用来区分一个网络内不同的主机，能唯一标识网段上的某台设备。

网络部分 → 清风小区

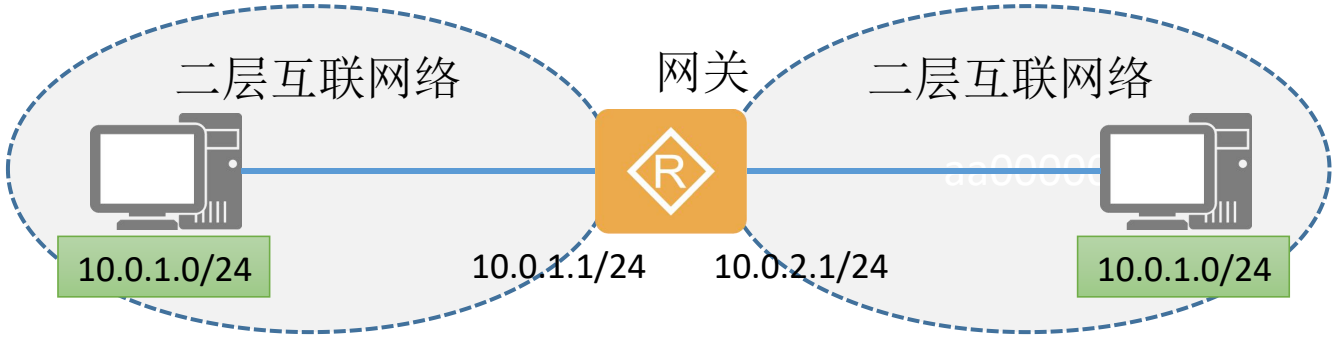
网络部分 → X栋X号 悦悦家

二层网络寻址

清风小区（网络位）

X栋X号 悦悦家（主机位）

三层网络寻址



三层互联网络

IP地址分类

- 为方便管理及组网，IP地址分成五类。
- A/B/C类默认网络掩码

A类：8bit，0.0.0.0~127.255.255.255/8 （255.0.0.0）

B类：16bit，128.0.0.0~191.255.255.255/16 （255.255.0.0）

C类：24bit，192.0.0.0~223.255.255.255/24 （255.255.255.0）

网络部分

主机部分

A	0NNNNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	0.0.0.0~127.255.255.255	分配给主机使用
B	10NNNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	128.0.0.0~191.255.255.255	
C	110NNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	192.0.0.0~223.255.255.255	
D	1110NNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	224.0.0.0~239.255.255.255	用于组播
E	1111NNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	240.0.0.0~255.255.255.255	用于研究

IP地址类型

- 通常把一个网络号所定义的网络范围称为一个网段。
- 网络地址：用于标识一个网络。

  例如：192.168.10.0/24

192	168	10	00000000

- 广播地址：用于向该网络中所有主机发送数据的特殊地址。

  例如：192.168.10.255/24

192	168	10	11111111

- 可用地址：可分配给网络中的节点或网络设备接口的地址。

  例如：192.168.10.1/24

192	168	10	00000001

注意

- 网络地址和广播地址不能直接被节点或网络设备所使用。
- 一个网段可用地址数量为：2^n-2（n为主机部分的比特位数）

IP地址计算

- 例：172.16.10.1/16 这个B类地址的网络地址、广播地址及可用地址数分别是？

	172				16				10				1			
IP地址	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
网络掩码	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
网络地址	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
广播地址	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1

主机位全为0

主机位全为1

IP 地址数　　2^n = （2^{16}=65536）

可用IP地址数　　2^n-2 = （2^{16}-2=65534）

可用IP地址范围　172.16.0.1~172.16.255.254

练习

请计算10.128.10.20/8 这个A类地址的网络地址、广播地址及可用地址数。

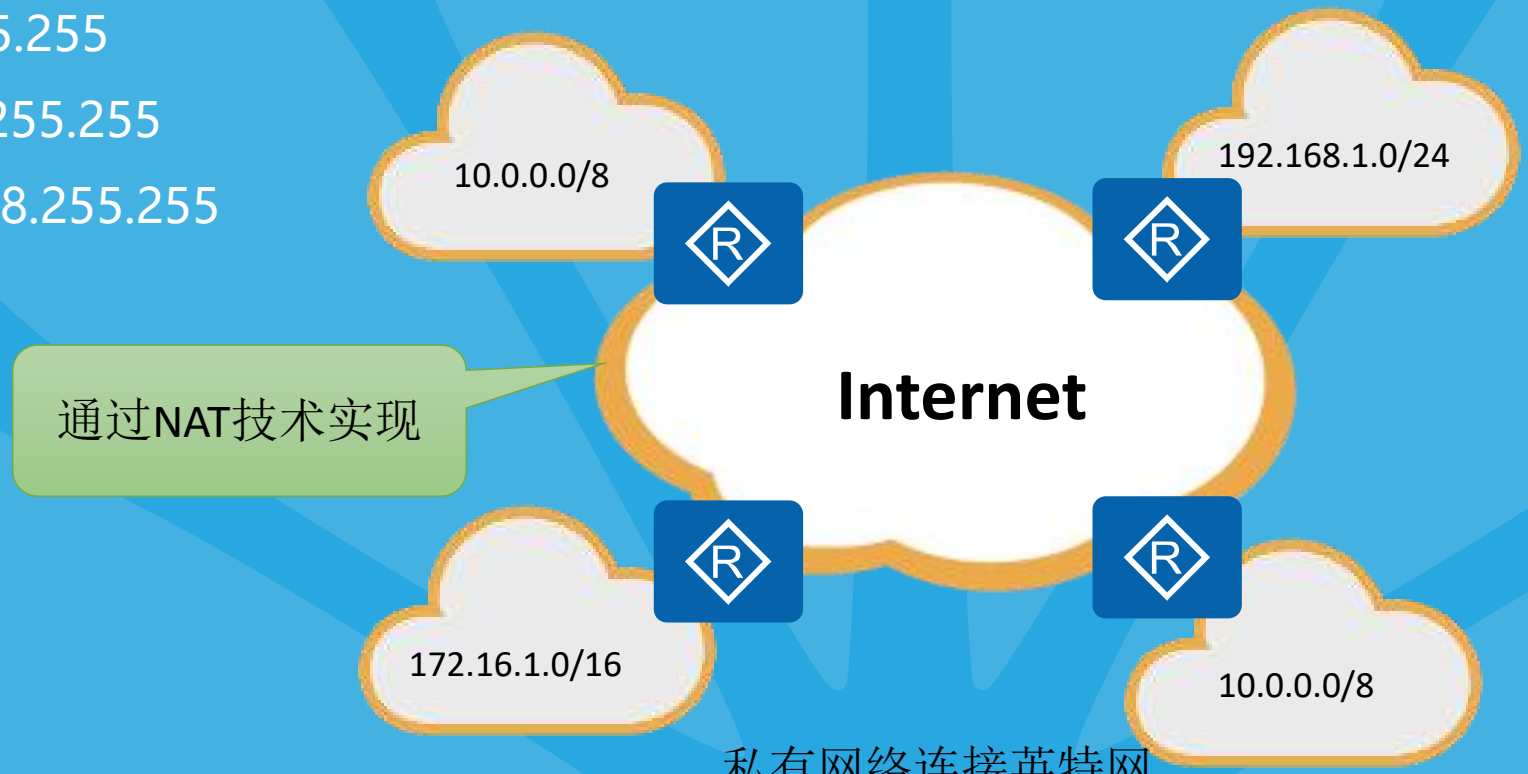
私有IP地址

- 公有IP地址：由IANA统一分配IP地址，以保证任何一个IP地址在英特网上的唯一性。
- 私有IP地址：某些网络不需要连接英特网，例如学校的计算机实训室内的网络，只要保证同一网络中网络设备地址不冲突即可。A、B、C三类地址中各预留一部分地址专门用于上述情况。

A类： 10.0.0.0~10.255.255.255

B类： 172.16.0.0~172.31.255.255

C类： 192.168.0.0~192.168.255.255



私有网络连接英特网

特殊IP地址

- IP地址空间中，有特殊含义和作用的地址。

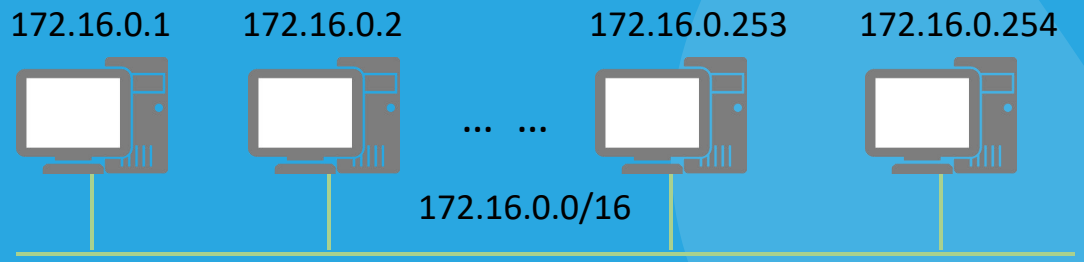
特殊IP地址	地址范围	作用
有限广播地址	255.255.255.255	可作为目的地址，发往该网段所有主机（受限于网关）
任意地址	0.0.0.0	“任何网络”的网络地址； “这个网络上这个主机接口”的IP地址
环回地址	127.0.0.0/8	测试设备自身的软件系统
本地链路地址	169.254.0.0/24	主机自动获取地址失败后，可使用该网络中的某个地址进行临时通信

IPv4 VS IPv6

- IANA管理的IPv4地址于2011年完全用尽。后续接入公网的用户及设备越来越多，IPv4地址枯竭问题日益严重，是IPv6代替IPv4的最大源动力。

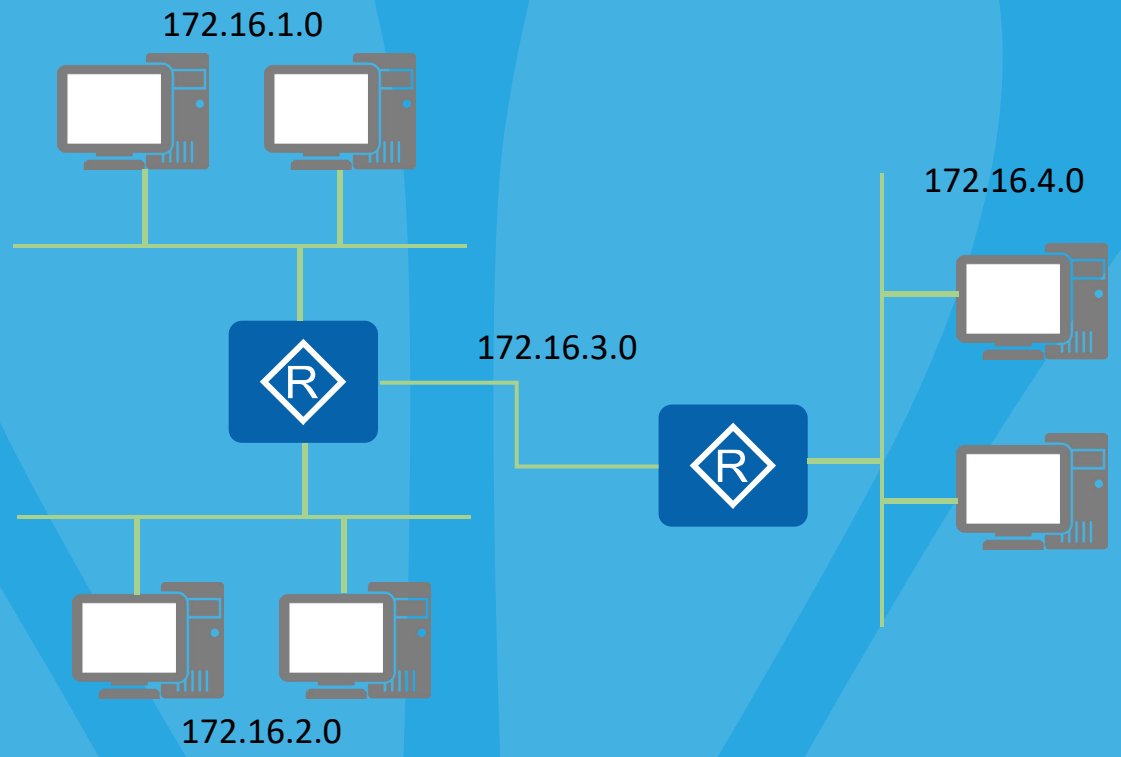
IPv4	IPv6
地址长度：32 bit	地址长度：128 bit
地址分类： 单播地址、广播地址、组播地址	地址分类： 单播地址、组播地址、任播地址
特点：地址枯竭，包头设计不合理， 对ARP的依赖导致广播泛滥	特点：地址无限，简化报文头部， IPv6地址自动部署

为什么要子网划分



2^{16}=65536个地址

- 一个B类地址用于一个广播域，地址浪费
- 广播域太庞大，一旦发生广播，内网不堪重负



- 一个网络号划分成多个子网，每个子网分配给一个独立的广播域
- 广播域规模更小、网络规划更合理
- 合理利用IP地址

如何进行子网划分

192.168.1.1

IP	192	168	1	0	0	0	0	0	0	0	1
掩码	255	255	255	0	0	0	0	0	0	0	0

192.168.1.255

IP	192	168	1	1	1	1	1	1	1	1	1
掩码	255	255	255	0	0	0	0	0	0	0	0

网络部分　　主机部分

网络地址：
192.168.1.0/24
广播地址：
192.168.1.255
IP地址数：2^8=256个
可用地址数：2^8-2=254个

- 例如：192.168.1.0/24网段

如何进行子网划分

- 向主机借位，形成子网

192.168.1.1

IP	192	168	1	0	0	0	0	0	0	0	1
掩码	255	255	255	1	0	0	0	0	0	0	0

192.168.1.255

IP	192	168	1	1	1	1	1	1	1	1	1
掩码	255	255	255	1	0	0	0	0	0	0	0

网络部分　　主机部分

2个子网：
子网1：
192.168.1.0/25
子网2：
192.168.1.128/25
新掩码：
255.255.255.128

IP地址数：2^7=128个
可用地址数：2^7-2=126个

- 可变长子网掩码 VLSM（Variable Length Subnet Mask）

如何进行子网划分

- 主机位全1，计算子网广播地址

192.168.1.0/25

IP	192	168	1	0	0	0	0	0	0	0	0
掩码	255	255	255	1	0	0	0	0	0	0	0
	网络部分				主机部分						

子网1（0~127）

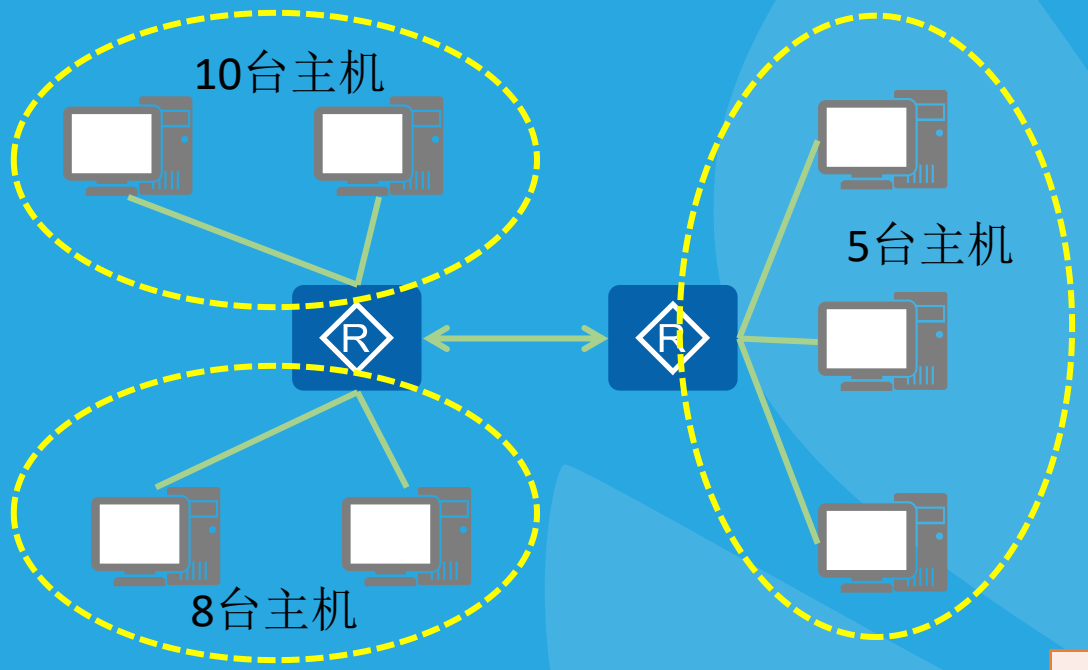
网络地址	192	168	1	0	0	0	0	0	0	0	0
广播地址	192	168	1	0	1	1	1	1	1	1	1

子网2（128~155）

网络地址	192	168	1	1	0	0	0	0	0	0	0
广播地址	192	168	1	1	1	1	1	1	1	1	1

练习：计算子网（1）

问题：C类网 192.168.1.0/24，请使用可变长子网掩码给三个子网分别分配IP地址。



计算：（以10台主机为例）

步骤1：计算所需主机

$2n-2 \geq 10$

$n \geq 4$

步骤2：向主机借位

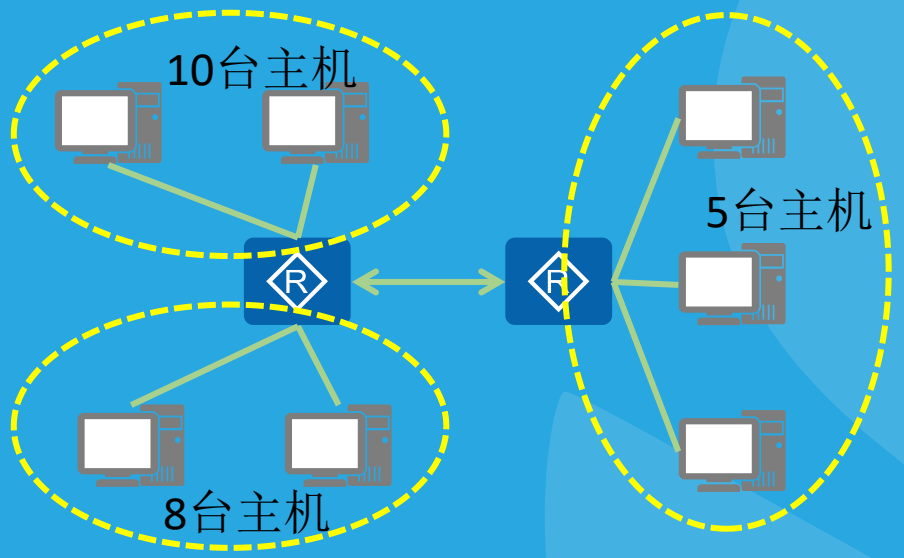
向主机借4位

IP地址	192	168	1	0	0	0	0	0	0	0	0
子网掩码	255	255	255	1	1	1	1	0	0	0	0

子网数：2^4=16个子网

练习：计算子网（2）

问题：C类网 192.168.1.0/24，请使用可变长子网掩码给三个子网分别分配IP地址。



步骤3：计算子网网络地址

IP地址	192	168	1	0	0	0	0	0	0	0	0	
子网掩码	255	255	255	1	1	1	1	0	0	0	0	
子网1	192	168	1	0	0	0	0	0	0	0	0	0
子网2	192	168	1	0	0	0	1	0	0	0	0	16
子网3	192	168	1	0	0	1	0	0	0	0	0	32
子网16	192	168	1	1	1	1	1	0	0	0	0	240

ICMP协议

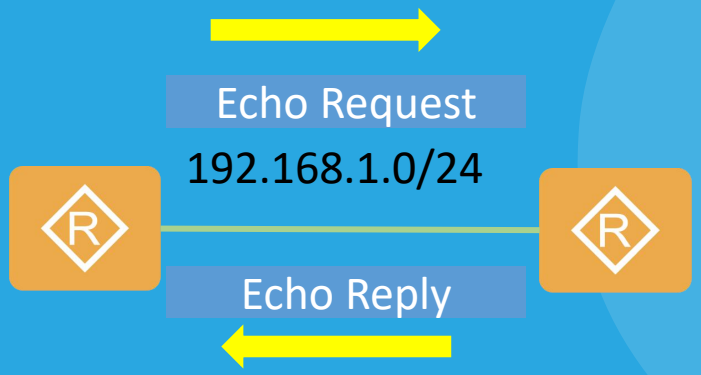
- Internet控制消息协议ICMP（Internet Control Message Protocol）是IP协议的辅助协议
- ICMP协议用来在网络设备间传递各种差错和控制信息，对收集各类网络信息、诊断和排除各种网络故障等方面起到重要作用。

Type	Code	Checksum
ICMP报文内容		

Type	Code	描述
0	0	Echo Reply
3	0	网络不可达
3	1	主机不可达
3	2	协议不可达
3	3	端口不可达
5	0	重定向
8	0	Echo Request

ICMP差错检验

- ICMP Echo消息常用于诊断源和目之间的网络连通性，同时还可提供其他信息，例如报文往返时间等。

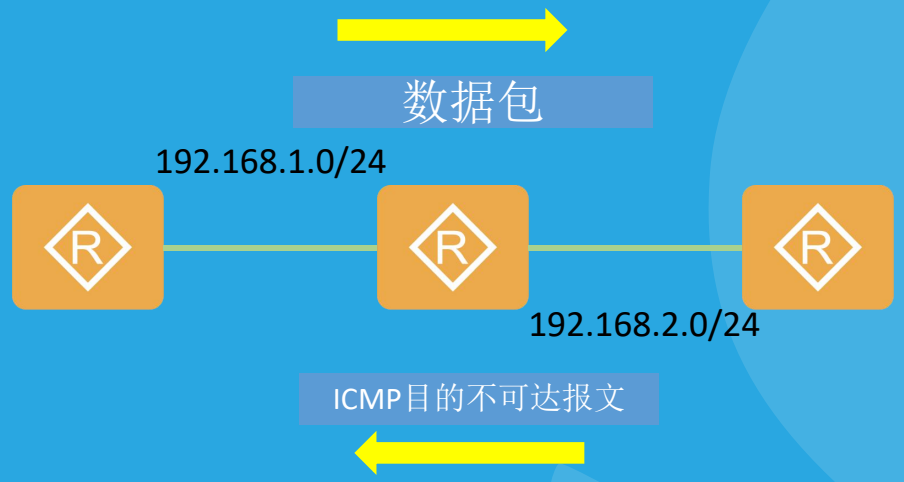



```
C:\Users\ivwnu>ping 192.168.2.1

正在 Ping 192.168.2.1 具有 32 字节的数据:
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.2.1 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.2.1 的回复: 字节=32 时间=69ms TTL=64

192.168.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 69ms, 平均 = 18ms
```

功能： Ping
常用于探测到达目的结点的网络可达性

ICMP差错检验

- ICMP 定义了各种错误信息，用于诊断网络连接性；根据错误信息，源设备可以判断数据传输失败的原因。例如：无法访问目标网络时，会自动发送ICMP目的不可达报文到发送端设备。




```
C:\Users\ivwnu>tracert www.163.com

通过最多 30 个跃点跟踪
到 z163picipv6.v.bsgslb.cn [182.242.61.243] 的路由:

  1     1 ms     1 ms     1 ms  192.168.2.1
  2     7 ms    10 ms     7 ms  100.69.0.1
  3     4 ms     7 ms    13 ms  180.140.104.165
  4     *        *        *     请求超时。
  5    22 ms    23 ms    22 ms  202.97.59.198
  6    25 ms    25 ms    25 ms  106.60.1.22
  7     *        *        *     请求超时。
  8     *        *        *     请求超时。
  9    33 ms    28 ms    41 ms  182.242.61.243

跟踪完成。
```

功能：Tracert
基于报文头中的TTL值逐跳追踪报文转发路径。
是检测网络丢包和延时的有效手段，同时可以帮助发现网络中的路由环路。

IP地址基础配置命令

进入接口视图

```
[Huawei] interface interface-type interface-number
```

- 此命令可以进入指定的接口视图

interface-type interface-number：指定接口类型和编号。接口类型和编号之间可以输入空格也可以不输入。

配置接口的IP地址

```
[Huawei-GigabitEthernet0/0/1]ip address ip-address{mask | mask-length}
```

- 此命令给设备接口配置IP地址

ip-address：指定接口的ip地址，点分十进制形式

mask：指定子网掩码，点分十进制

mask-length：指定子网掩码长度，整数形式，取值范围0~32

小结

- 理解数据链路层功能，及常见的二层协议
- 理解数据封装的结构及以太网协议的报文格式
- 理解MAC地址结构和作用
- 理解MAC地址和IP地址之间的关系

传输层

- 传输层协议接收来自应用层协议的数据，封装上对应的传输层头部，帮助建立“端到端”的连接（Port to Port）。
- 传输层的PDU称为Segment（段）

传输层协议：

TCP:一种面向连接的、可靠的传输层通信协议，由IETF的RFC793定义。

UDP：一种简单的无连接的传输层协议，由IETF的RFC768定义。

TCP和UDP – 报文格式

Source Port (16)			Destination Port (16)
Sequence Number (32)			
Acknowledgement Number (32)			
Header length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)			Urgent (16)
Options			
Date (varies)			

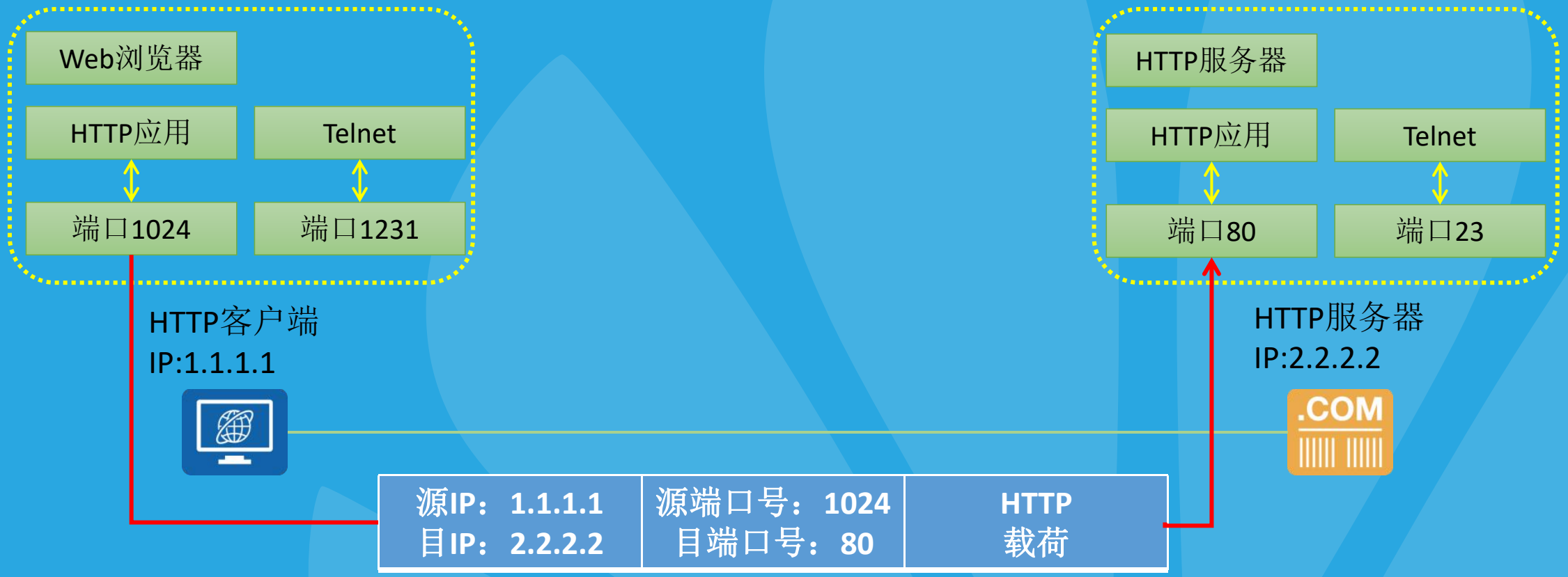
TCP 头部
20 Byte

Source Port (16)	Destination Port (16)
Length (16)	Checksum (16)
Data (if any)	

UDP头部
8 Byte

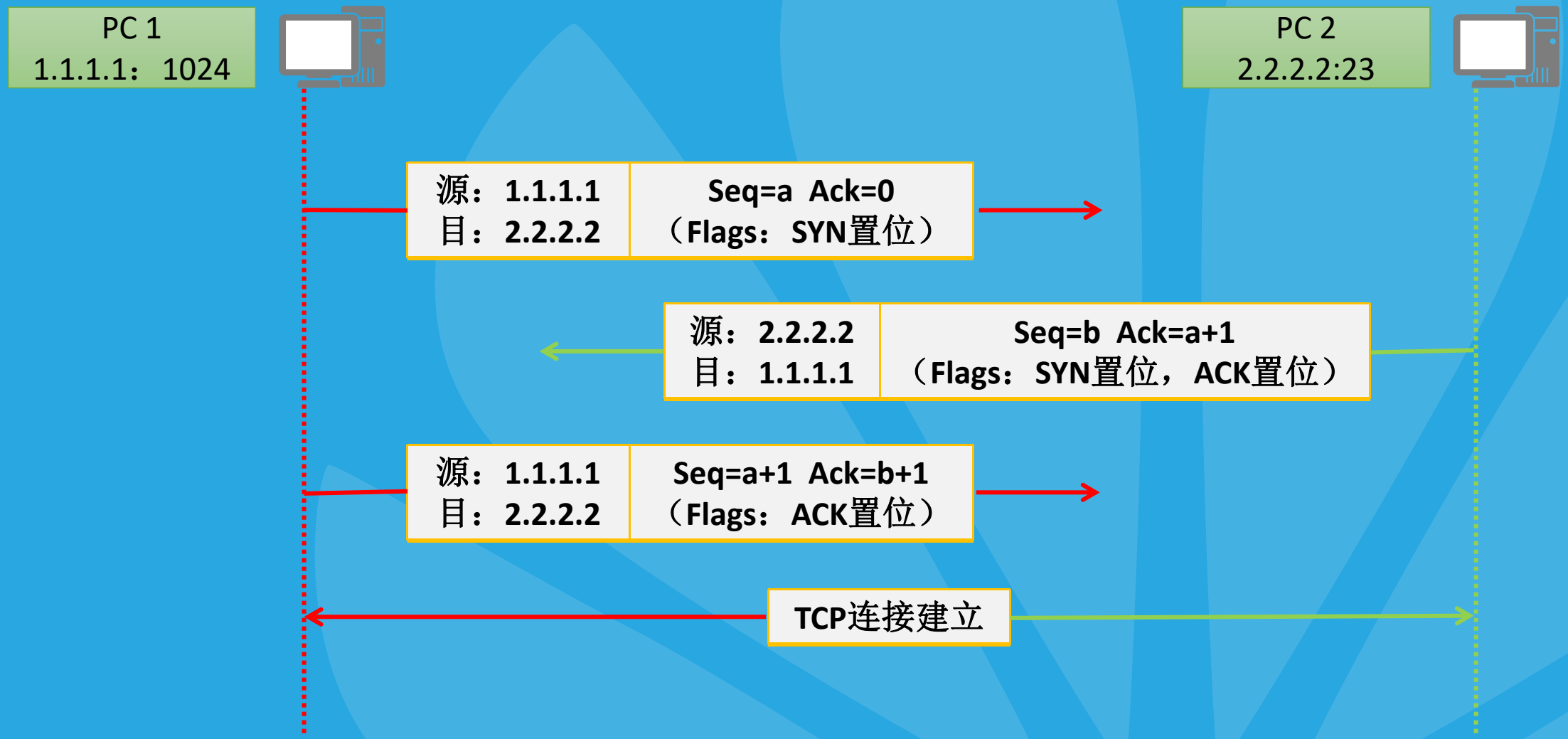
TCP和UDP – 端口号

物理层 | 数据链路层 | 网络层 | 传输层 | 应用层



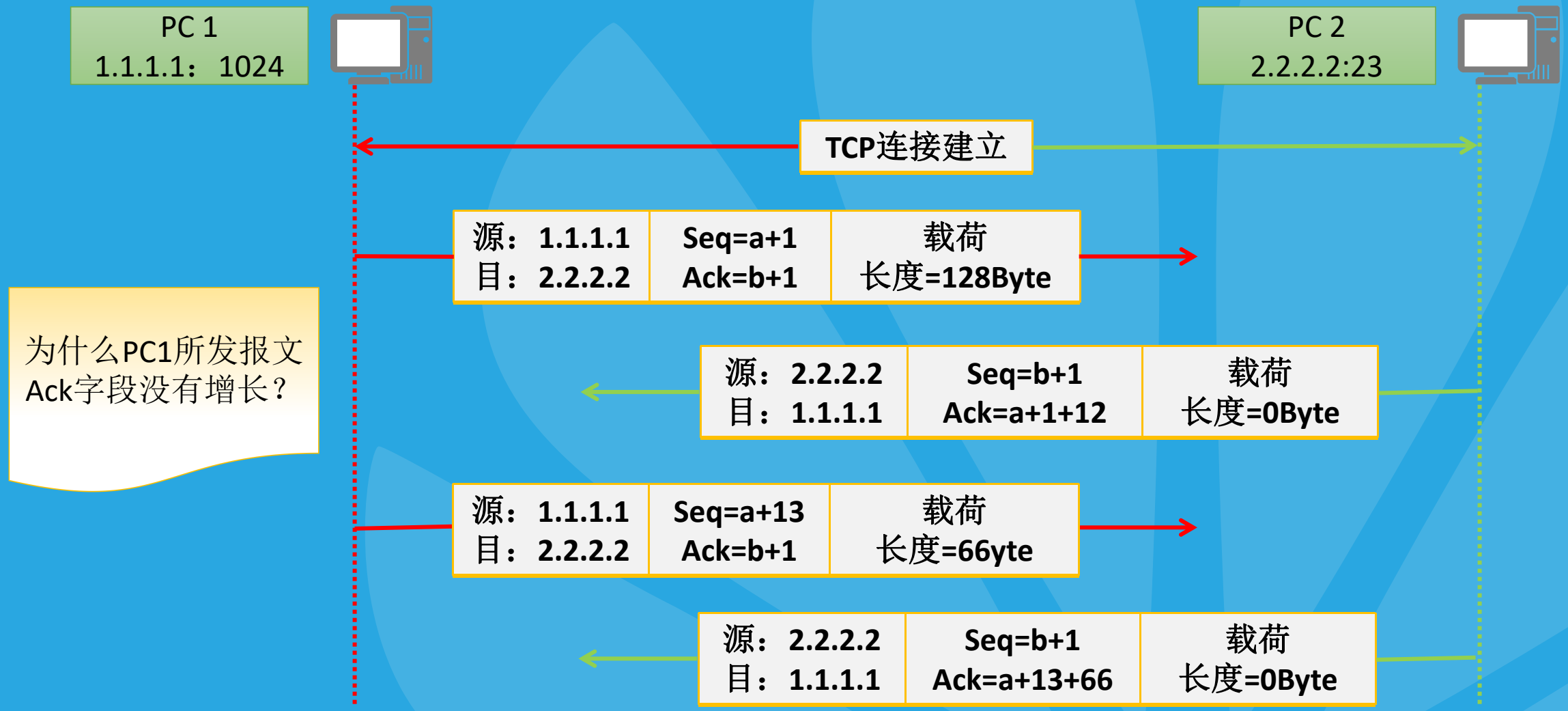
- 客户端使用的源端口一般随机分配，目标端口由服务器的应用指定;
- 源端口号一般为系统中未使用的，且大于1023的;
- 目的端口为服务端开启的应用（服务）所侦听的端口，如HTTP缺省使用80.

TCP的建立 – 三次握手



- 基于TCP的应用，在发数据之前，都需要进行“三次握手”建立连接

TCP的序列号与确认序列号



为什么PC1所发报文Ack字段没有增长？

- TCP使用序列号和确认序列号字段实现数据可靠性和有序传输

TCP的滑动窗口机制

PC 1
1.1.1.1：1024

PC 2
2.2.2.2:23

- TCP通过滑动窗口机制来控制数据的传输速率

Seq=100 win=3 flags=SYN

Seq=200 Ack=101 win=3 flags=SYN，ACK

① 三次握手

Seq=101 Ack=201 win=3 flags=ACK

Seq=101 win=3

Seq=102 win=3

② 发送数据

Seq=103 win=3

③

为什么PC1所发报文Win字段没有增长？

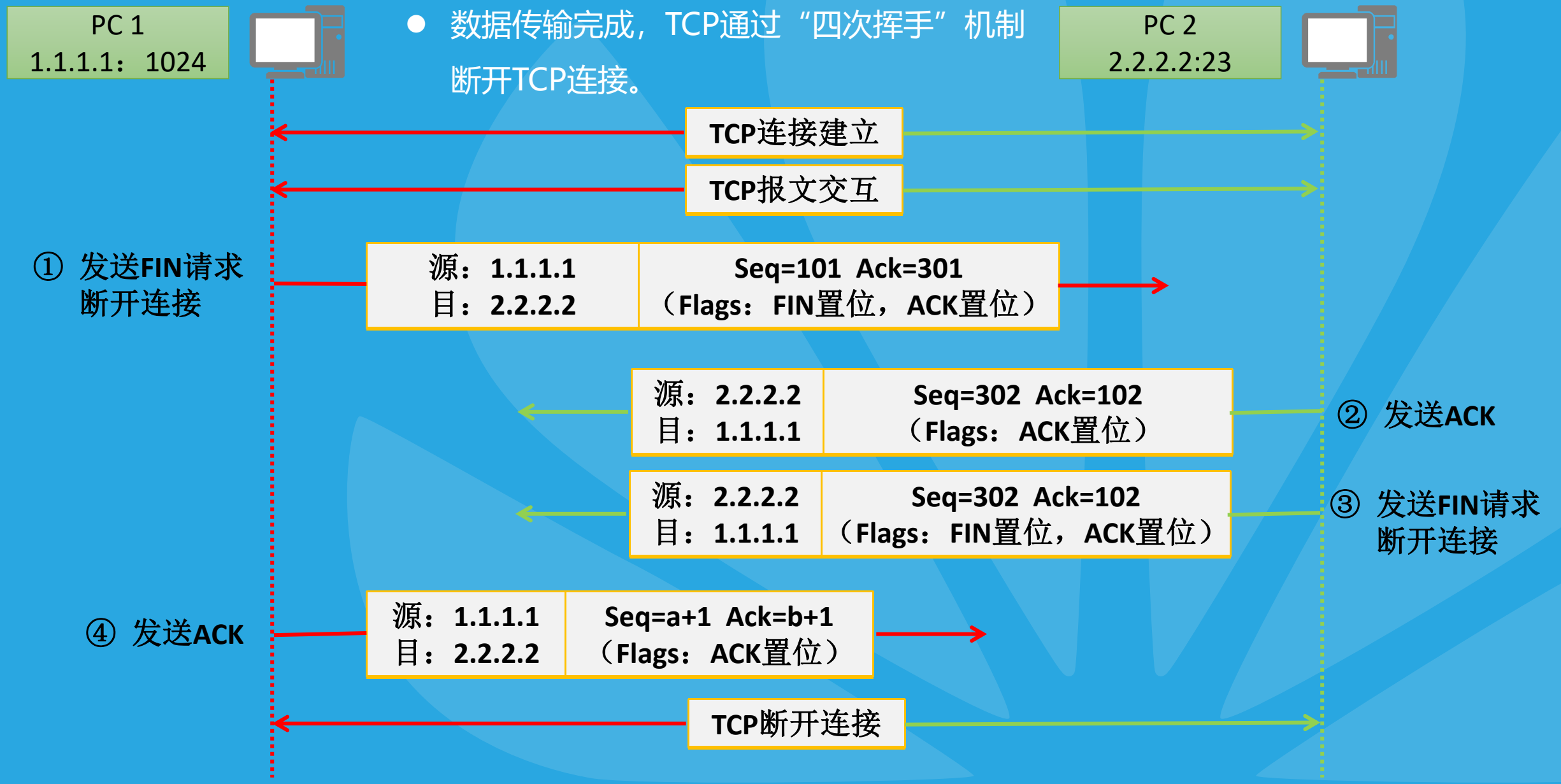
Ack=104 win=3 flags=ACK

④

Seq=104 win=3

⑤

TCP的关闭 – 四次挥手


PC 1
1.1.1.1：1024
PC 2
2.2.2.2:23
数据传输完成，TCP通过“四次挥手”机制断开TCP连接。
TCP连接建立
TCP报文交互
① 发送FIN请求断开连接
源： 1.1.1.1
目： 2.2.2.2
Seq=101 Ack=301
（Flags： FIN置位， ACK置位）
源： 2.2.2.2
目： 1.1.1.1
Seq=302 Ack=102
（Flags： ACK置位）
② 发送ACK
源： 2.2.2.2
目： 1.1.1.1
Seq=302 Ack=102
（Flags： FIN置位， ACK置位）
③ 发送FIN请求断开连接
④ 发送ACK
源： 1.1.1.1
目： 2.2.2.2
Seq=a+1 Ack=b+1
（Flags： ACK置位）
TCP断开连接

谢 谢

走进华为，大有可为

Into the Huawei, have a brilliant future