Wireless Networking Technology

Fall 2013

Chapter 2 无线网络逻辑结构

Weifeng Sun

Wfsun.dlut@gmail.com

School of Software

Dalian University of Technology

无线网络技术和覆盖范围

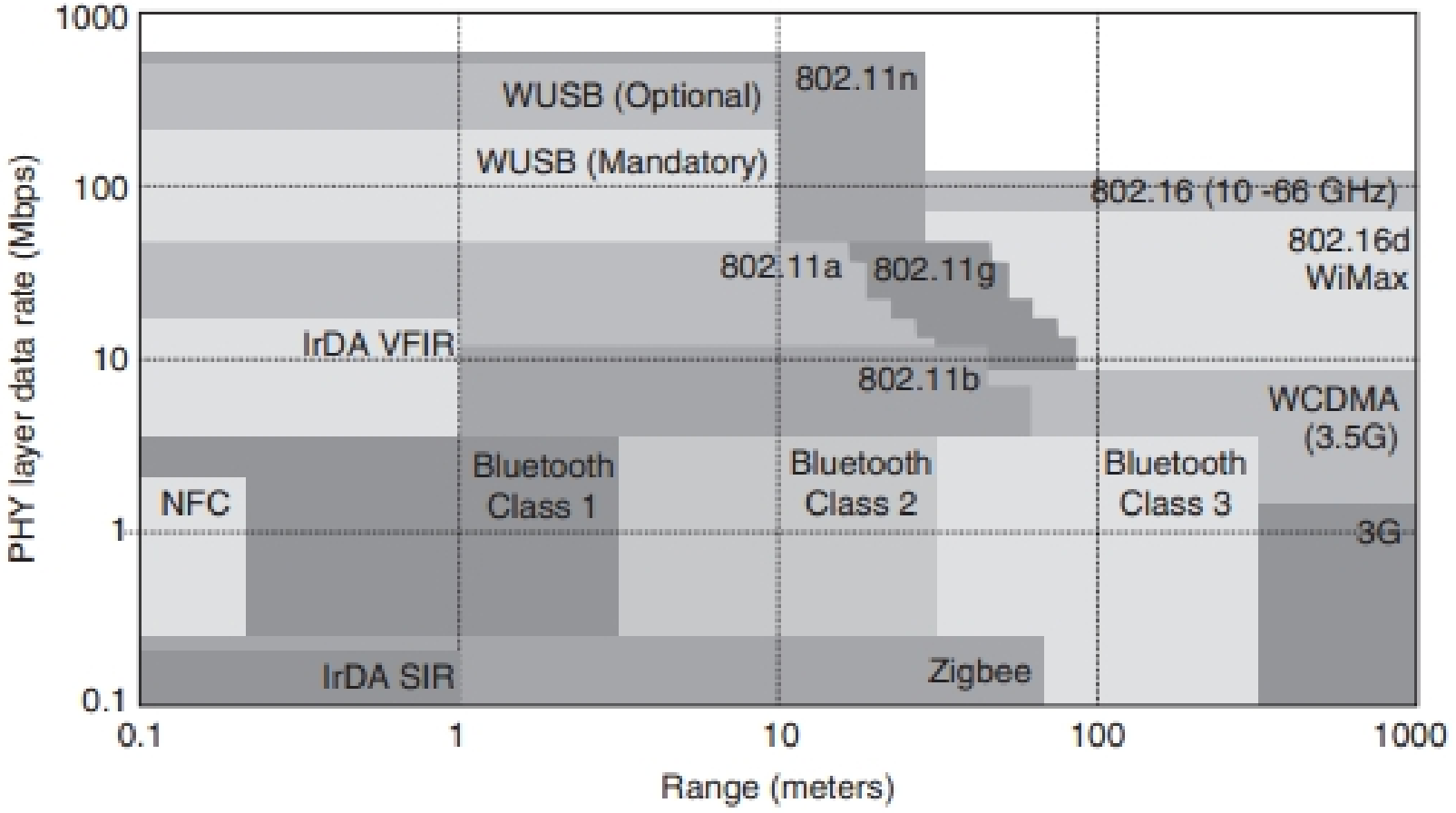


Figure 1-1: Wireless Networking Landscape (rate vs. range)

Layer	*Description*	*Standards and Protocols*
7 — Application layer	Standards to define the provision of services to applications — such as checking resource availability, authenticating users, etc.	HTTP, FTP, SNMP, POP3, SMTP
6 — Presentation layer	Standards to control the translation of incoming and outgoing data from one presentation format to another.	SSL
5 — Session layer	Standards to manage the communication between the presentation layers of the sending and receiving computers. This communication is achieved by establishing, managing and terminating "sessions".	ASAP, SMB
4 — Transport layer	Standards to ensure reliable completion of data transfers, covering error recovery, data flow control, etc. Makes sure all data packets have arrived.	TCP, UDP
3 — Network layer	Standards to define the management of network connections — routing, relaying and terminating connections between nodes in the network.	IPv4, IPv6, ARP
2 — Data link layer	Standards to specify the way in	ARP

Table 2-2: Local and Remote IP Addresses

Sending Device		
IP Address:	200.100.50.10	11001000.01100100.00110010.00001010
Subnet Mask:	255.255.255.240	11111111.11111111.11111111.11110000
Network ID:	200.100.50.000	11001000.01100100.00110010.00000000

Table 2-3: Private IP Address Ranges

Class	*Private address range start*	*Private address range end*
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

- IPv6
- ARP
- Routing
- NAT

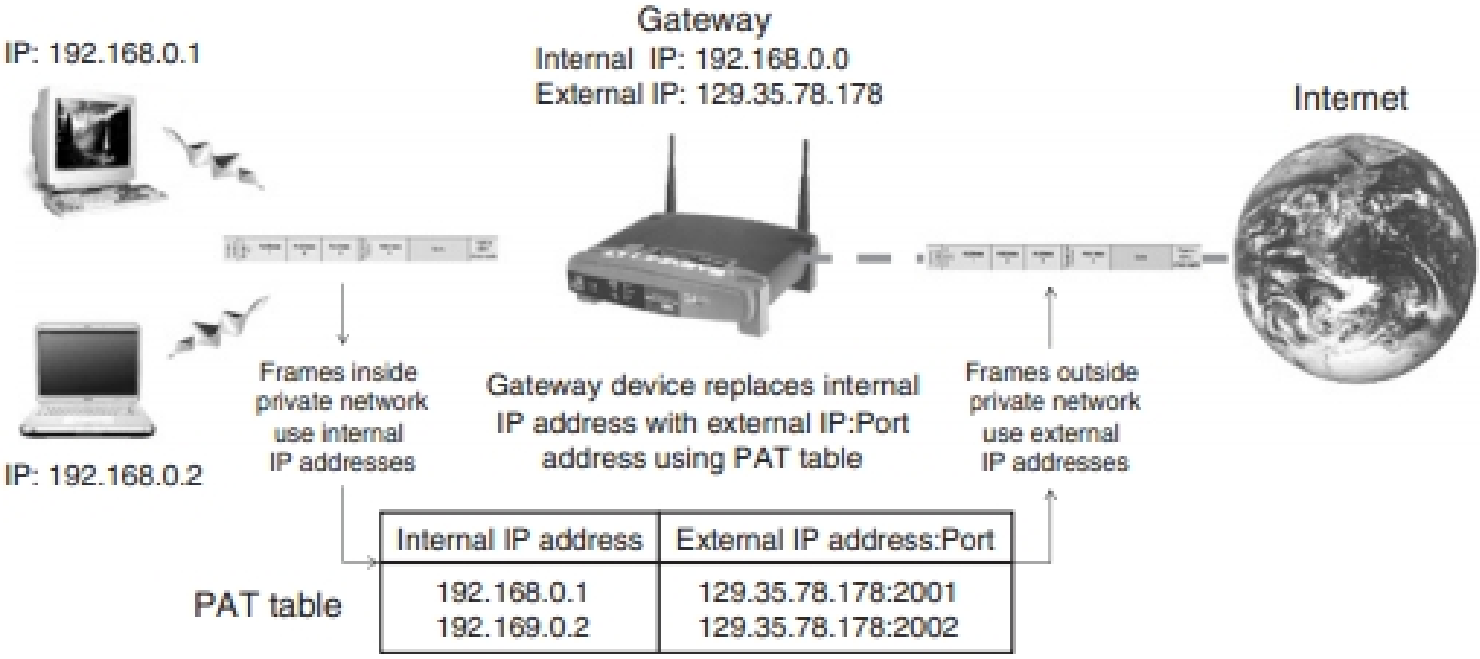
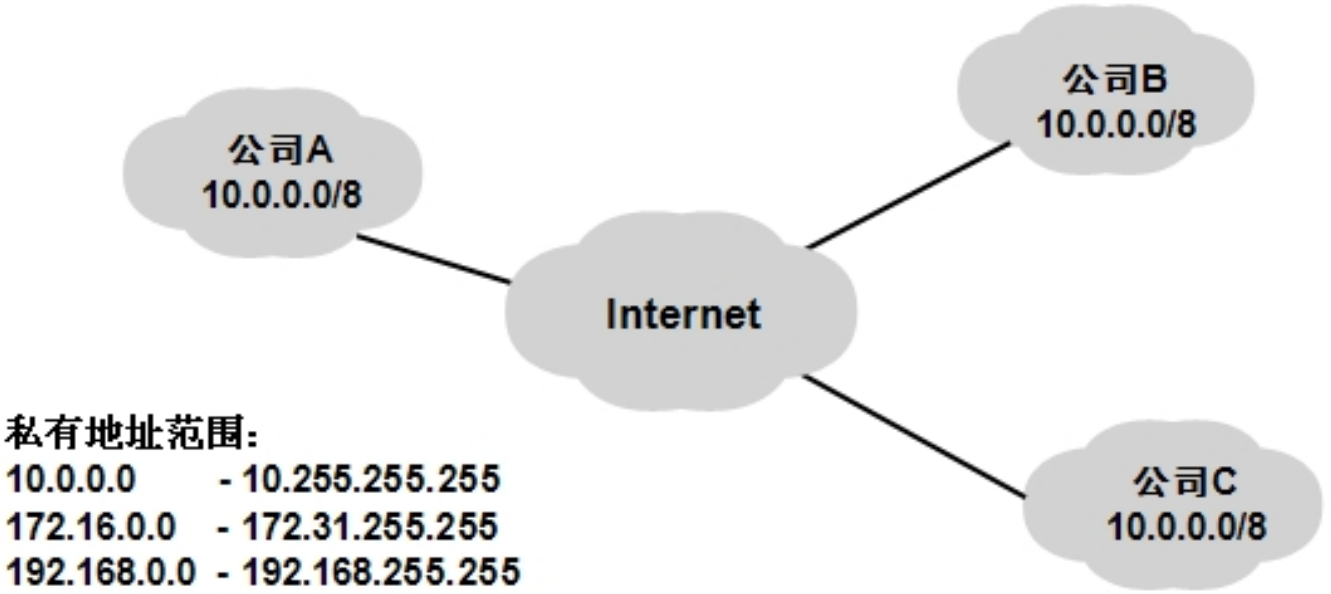


Figure 2-2: Port Address Translation in Practice

Table 2-5: Example of a Simple PAT Table

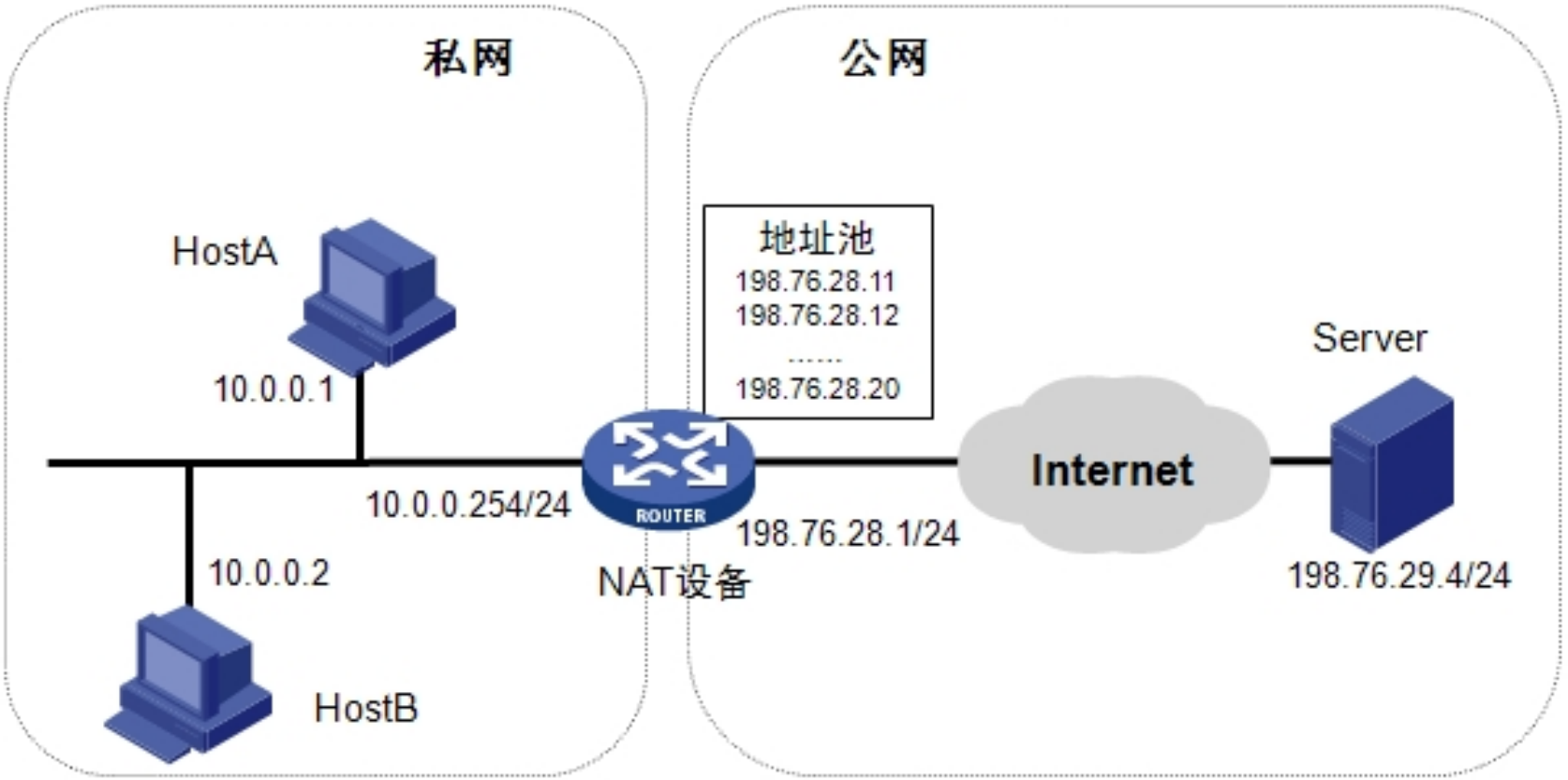
Private IP address	*Public IP address:Port*
192.168.0.1	129.35.78.178:2001
192.168.0.2	129.35.78.178:2002
192.168.0.3	129.35.78.178:2003
192.168.0.4	129.35.78.178:2004

共有地址和私有地址

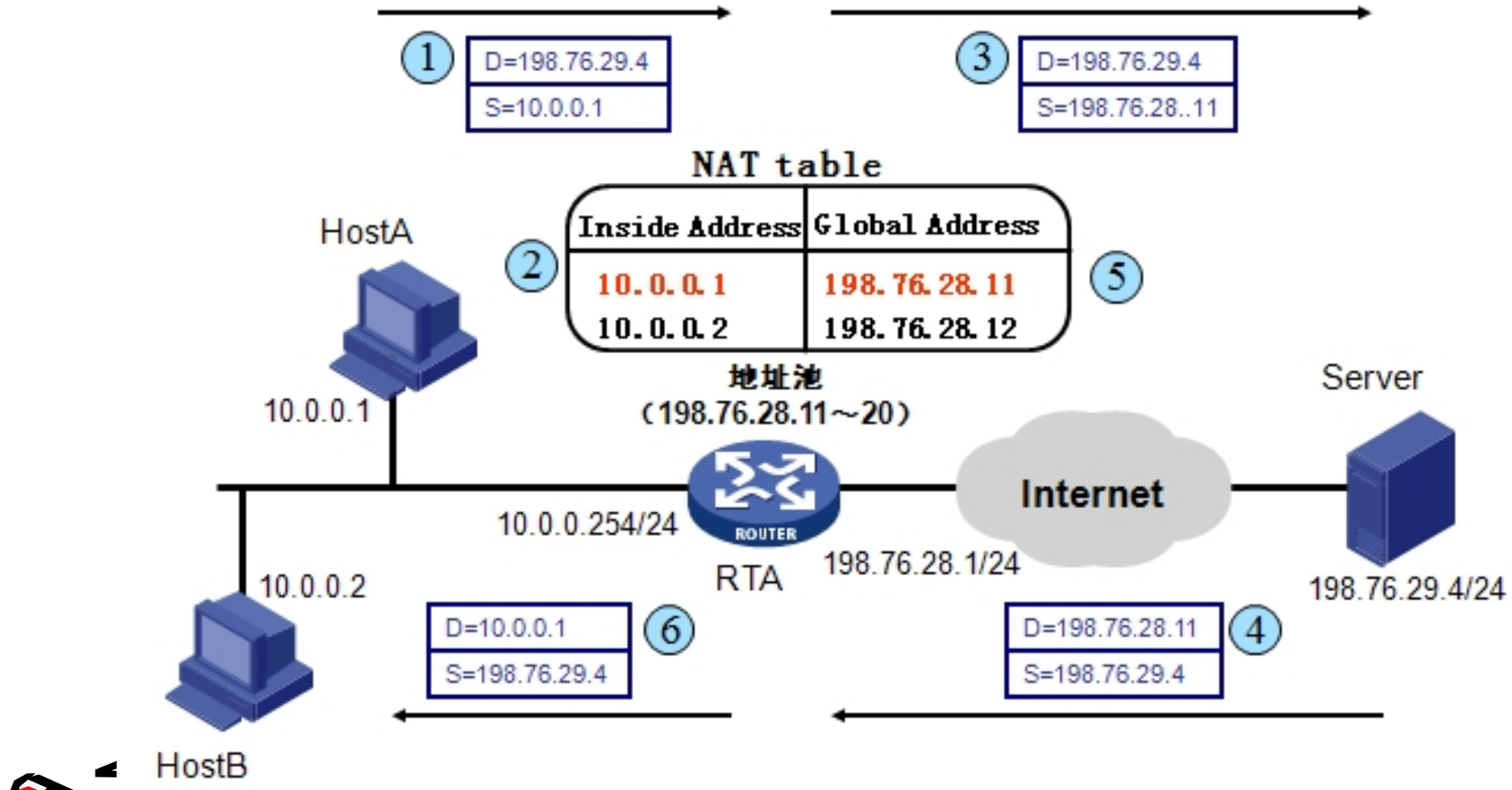


私有地址范围:
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

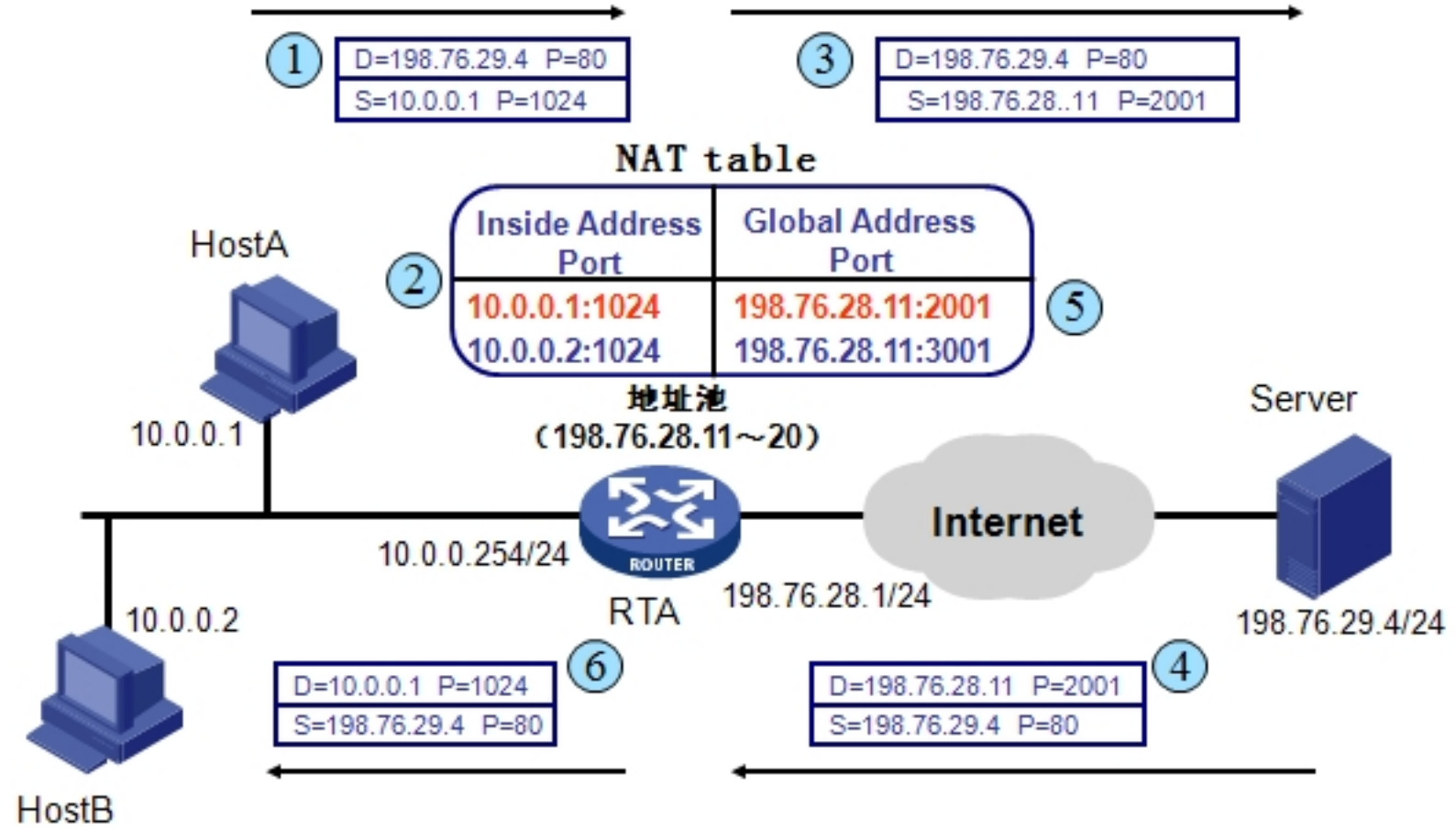
- 任何组织都可以任意使用私有地址空间
- 私有地址在Internet上无法路由
- 如果采用私有地址的网络需要访问Internet，必须在出口处部署NAT设备


私网
公网
HostA
10.0.0.1
地址池
198.76.28.11
198.76.28.12
.....
198.76.28.20
Server
Internet
10.0.0.254/24
ROUTER
198.76.28.1/24
10.0.0.2
NAT设备
198.76.29.4/24
HostB

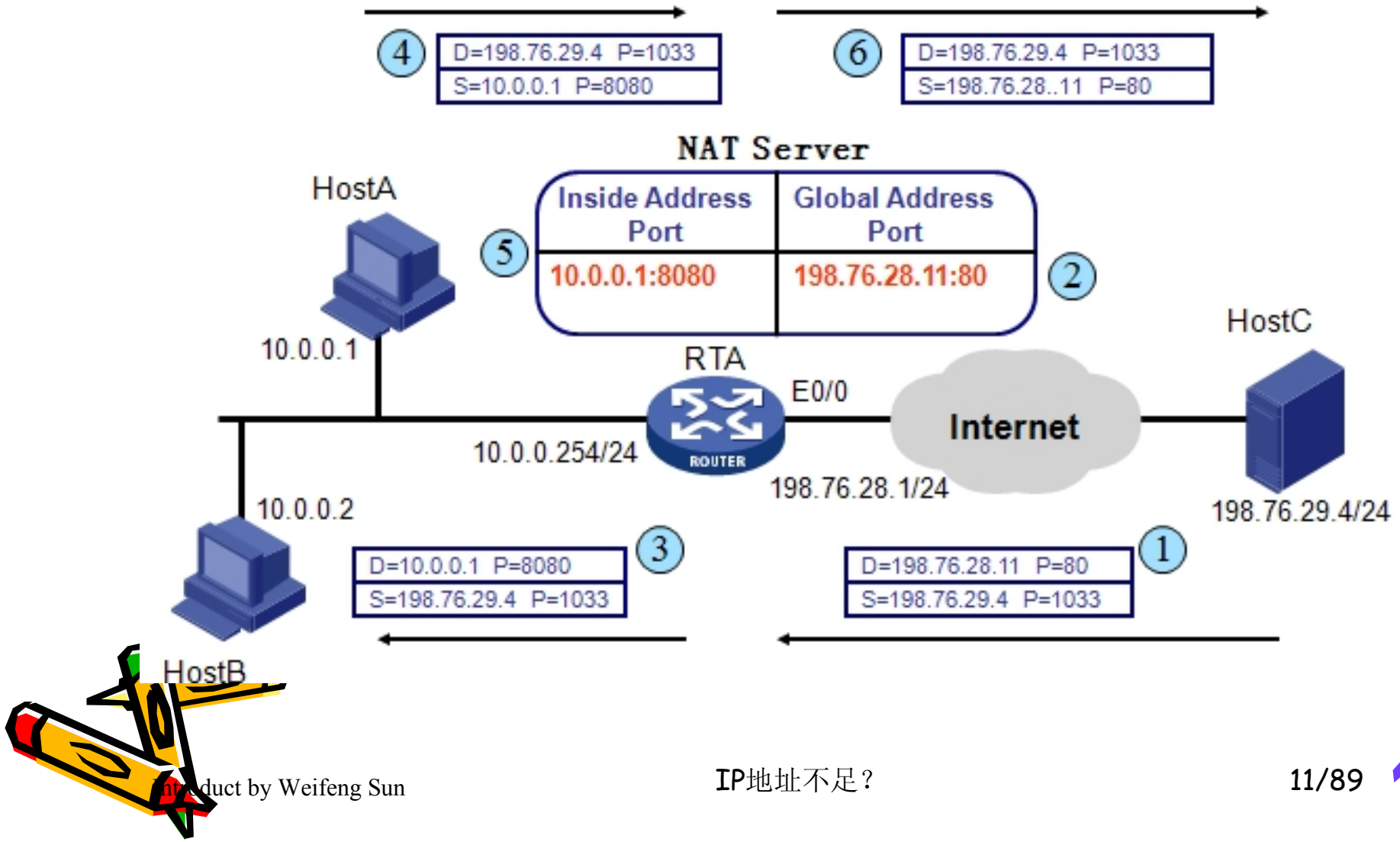
Basic NAT


1
D=198.76.29.4
S=10.0.0.1
3
D=198.76.29.4
S=198.76.28..11
NAT table
Inside Address
Global Address
10.0.0.1
198.76.28.11
10.0.0.2
198.76.28.12
2
5
HostA
10.0.0.1
地址池
(198.76.28.11～20)
Server
10.0.0.254/24
ROUTER
RTA
Internet
198.76.28.1/24
198.76.29.4/24
10.0.0.2
D=10.0.0.1
S=198.76.29.4
6
D=198.76.28.11
S=198.76.29.4
4
HostB

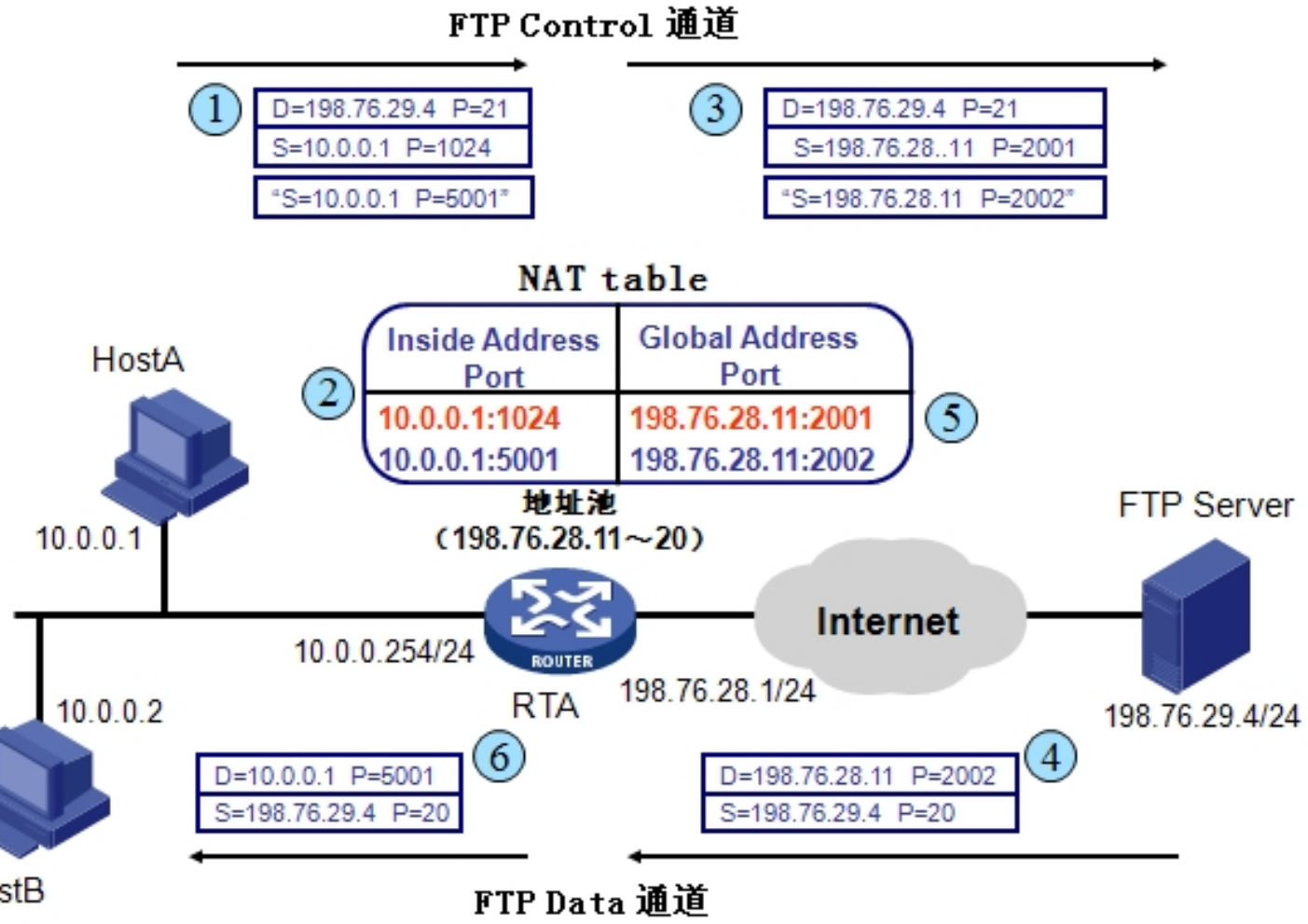
NAPT


1
D=198.76.29.4 P=80
S=10.0.0.1 P=1024
3
D=198.76.29.4 P=80
S=198.76.28..11 P=2001
NAT table
Inside Address Port
Global Address Port
10.0.0.1:1024
198.76.28.11:2001
10.0.0.2:1024
198.76.28.11:3001
2
5
HostA
10.0.0.1
地址池
(198.76.28.11~20)
Server
Internet
10.0.0.254/24
ROUTER
RTA
198.76.28.1/24
198.76.29.4/24
10.0.0.2
6
D=10.0.0.1 P=1024
S=198.76.29.4 P=80
4
D=198.76.28.11 P=2001
S=198.76.29.4 P=80
HostB

NAT Server


4
D=198.76.29.4 P=1033
S=10.0.0.1 P=8080
6
D=198.76.29.4 P=1033
S=198.76.28..11 P=80
NAT Server
Inside Address Port
Global Address Port
10.0.0.1:8080
198.76.28.11:80
5
2
HostA
10.0.0.1
RTA
E0/0
10.0.0.254/24
ROUTER
Internet
198.76.28.1/24
HostC
198.76.29.4/24
10.0.0.2
HostB
3
D=10.0.0.1 P=8080
S=198.76.29.4 P=1033
1
D=198.76.28.11 P=80
S=198.76.29.4 P=1033

NAT ALG


FTP Control 通道
1
D=198.76.29.4 P=21
S=10.0.0.1 P=1024
"S=10.0.0.1 P=5001"
3
D=198.76.29.4 P=21
S=198.76.28..11 P=2001
"S=198.76.28.11 P=2002"
NAT table
2
Inside Address Port
Global Address Port
10.0.0.1:1024
198.76.28.11:2001
10.0.0.1:5001
198.76.28.11:2002
5
地址池
(198.76.28.11~20)
HostA
10.0.0.1
10.0.0.254/24
ROUTER
RTA
Internet
198.76.28.1/24
FTP Server
198.76.29.4/24
10.0.0.2
HostB
6
D=10.0.0.1 P=5001
S=198.76.29.4 P=20
4
D=198.76.28.11 P=2002
S=198.76.29.4 P=20
FTP Data 通道

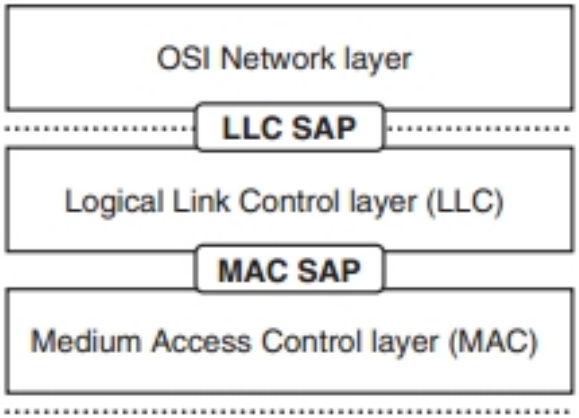


Figure 2-4: Logical Location of LLC and MAC Service Access Points

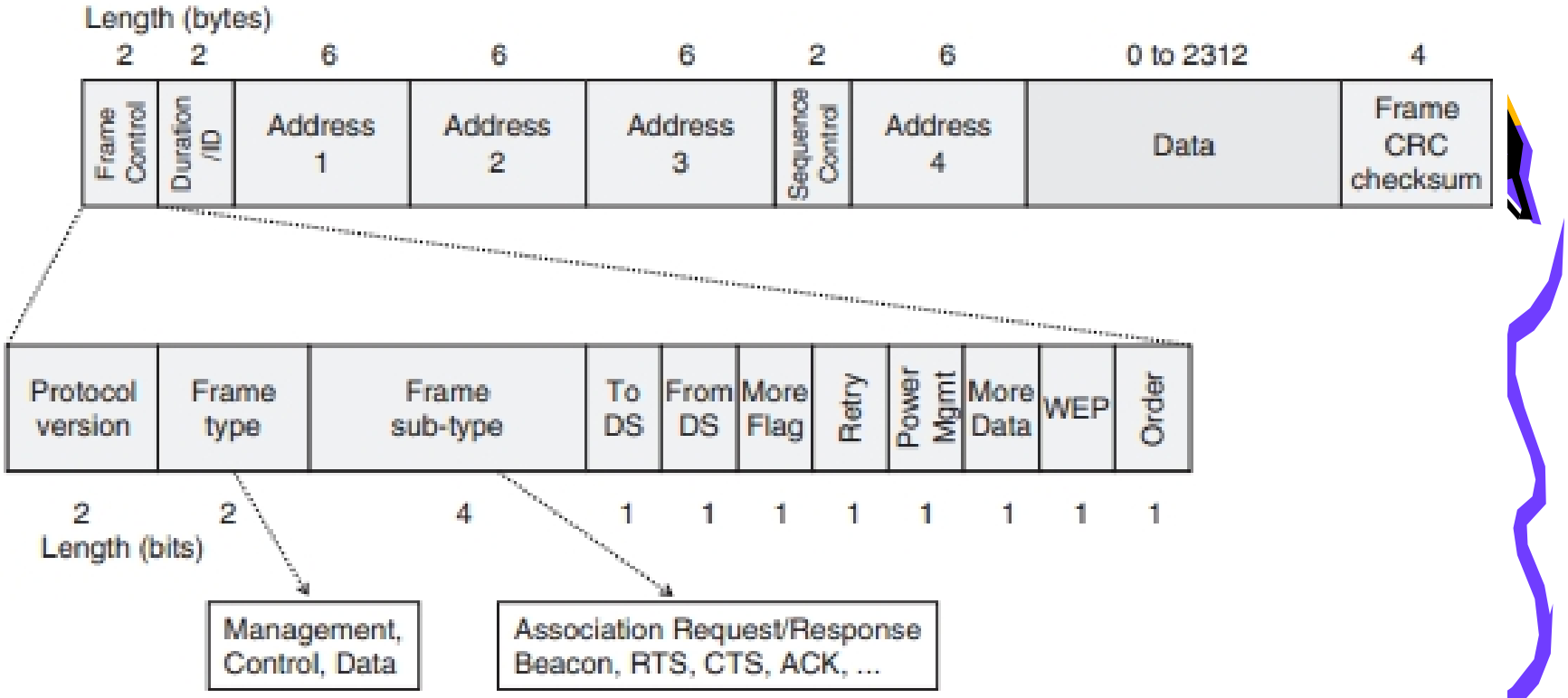


Figure 2-5: MAC Frame Structure

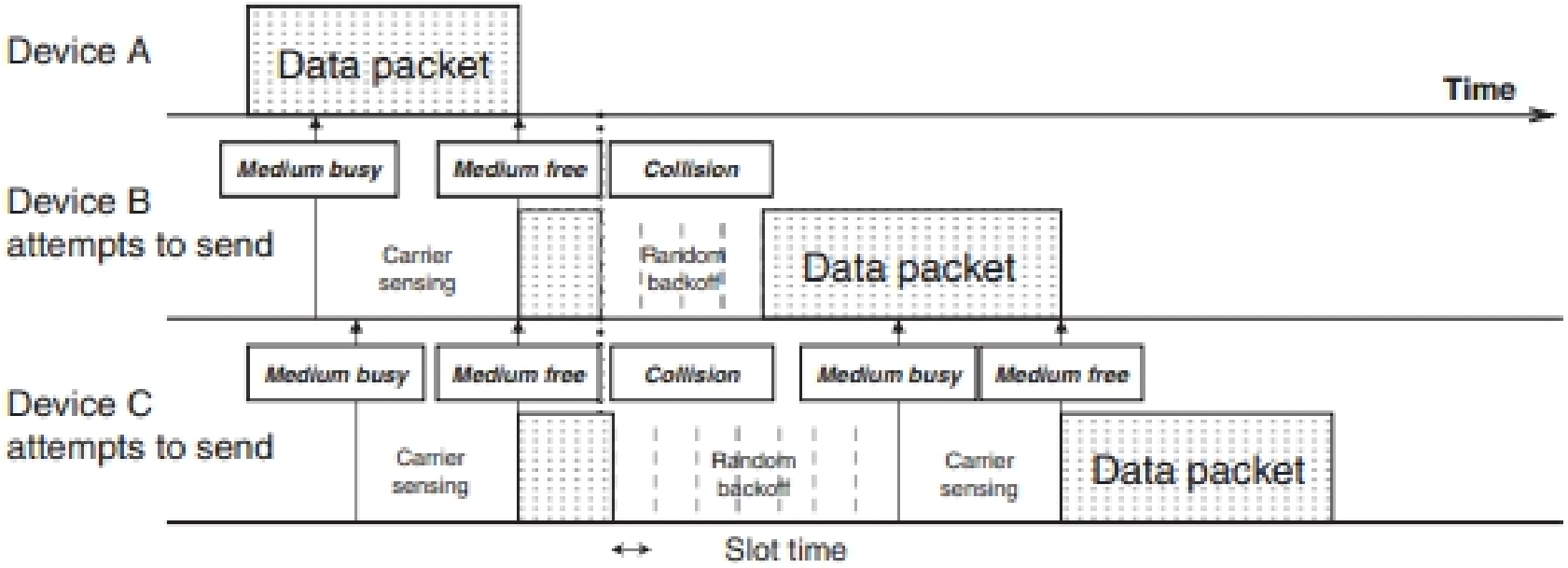


Figure 2-6: Ethernet CSMA/CD Timing

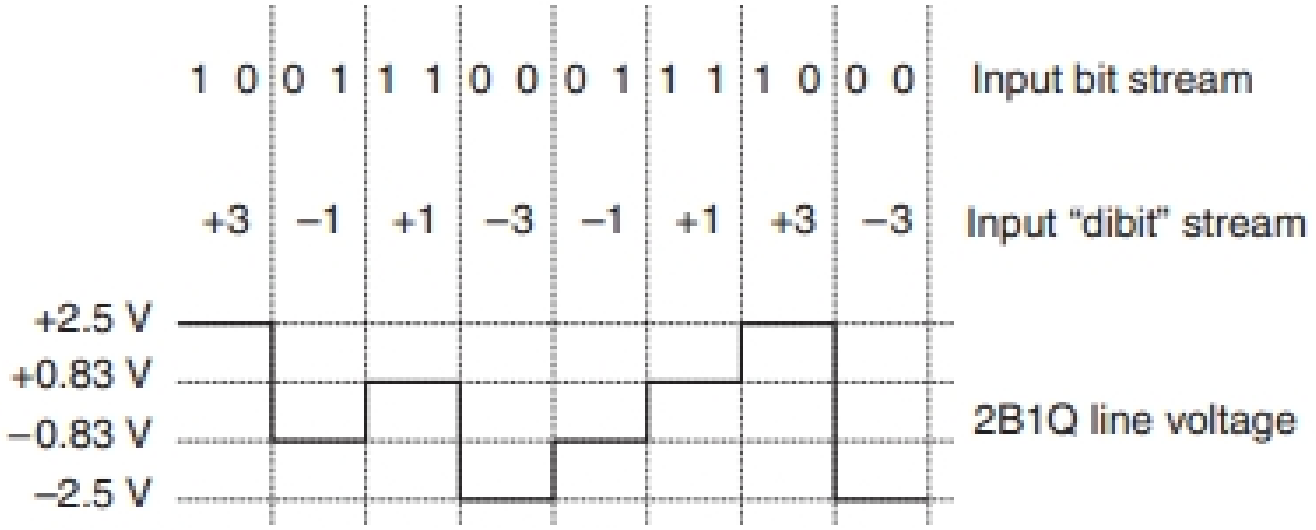


Figure 2-9: 2B1Q Line Code Using in ISDN

- two binary bits (2B)
- a single output symbol,known as a "quat" (1Q)

- IEEE 1394,Apple, 100Mbps(当时USB 12Mbps)。存储、光驱等设备及通信。

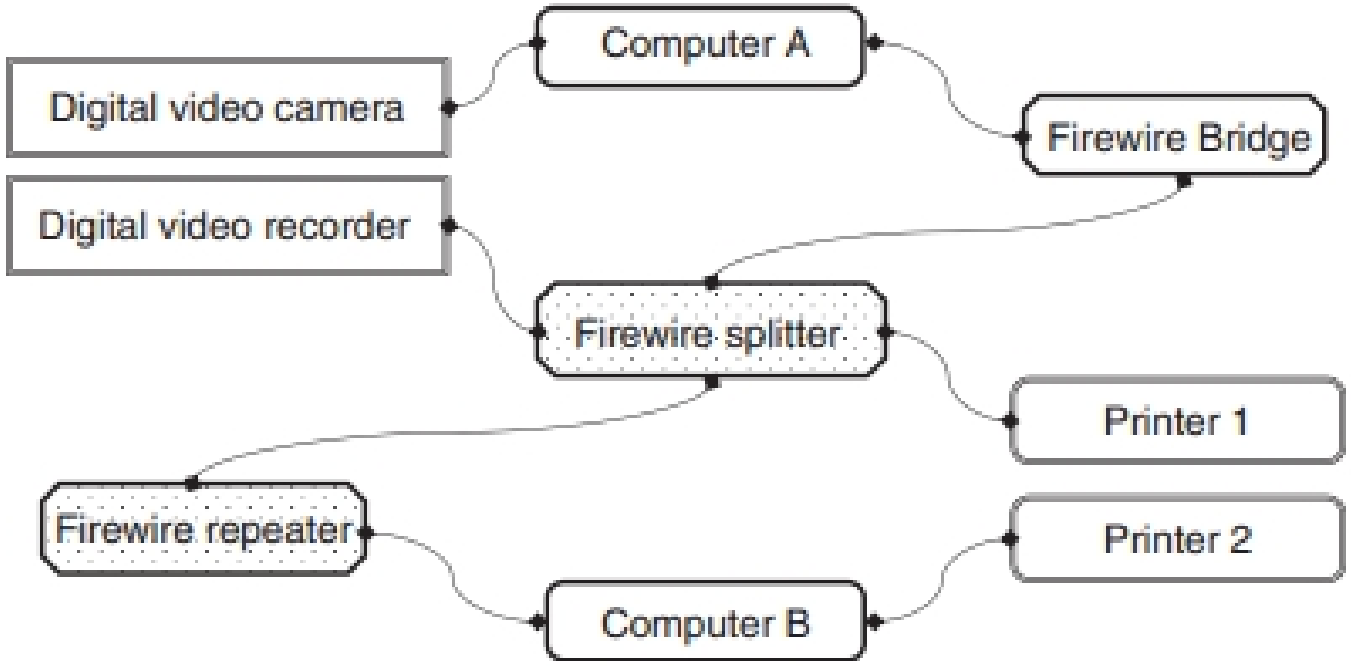


Figure 2-10: FireWire Network Topology: Daisy-chain and Tree Structures

- USB1.0 12Mbps
- USB2.0 480Mbps

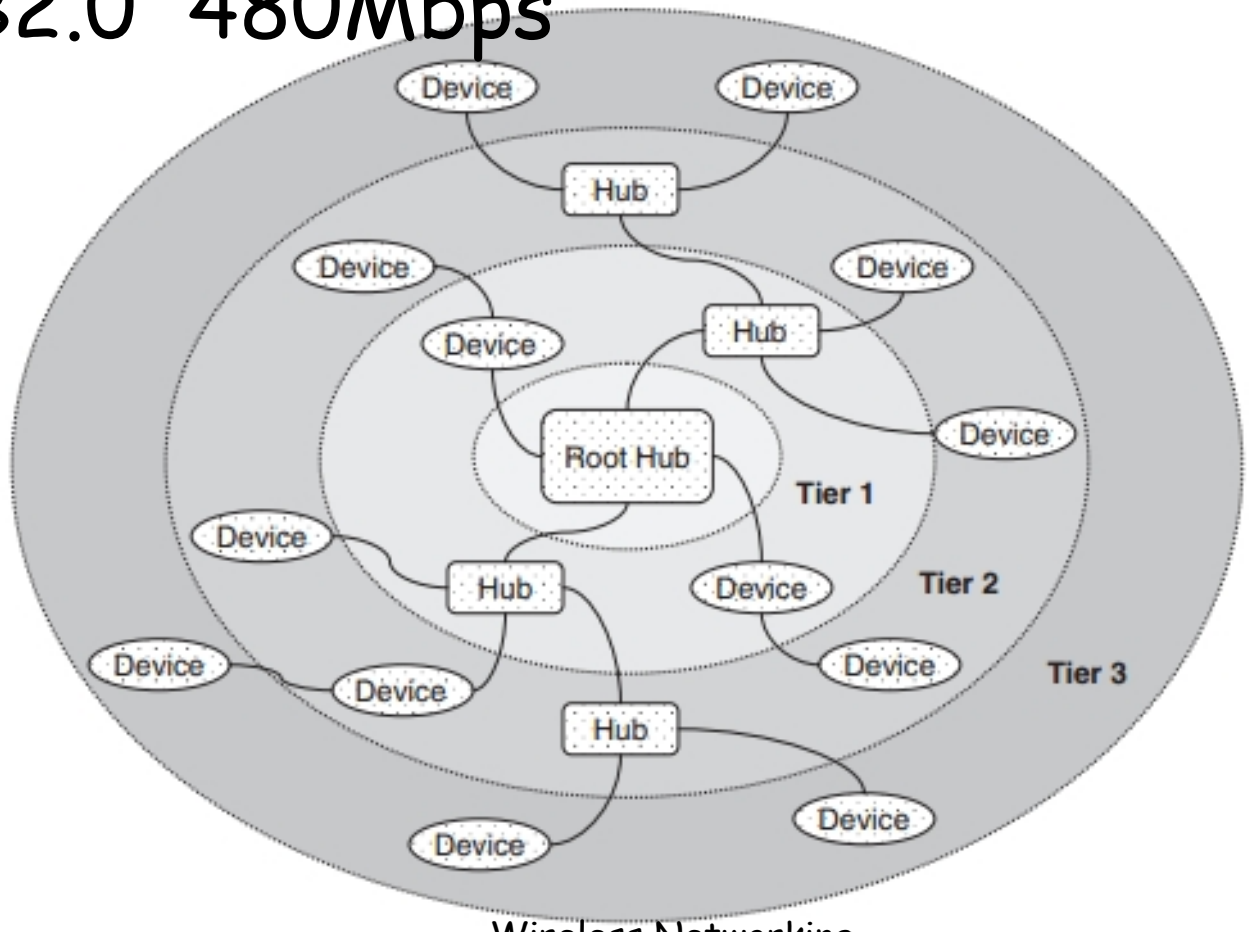
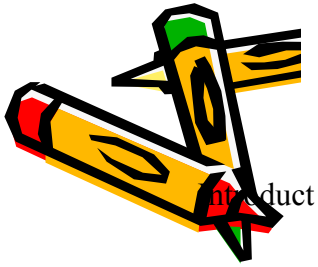


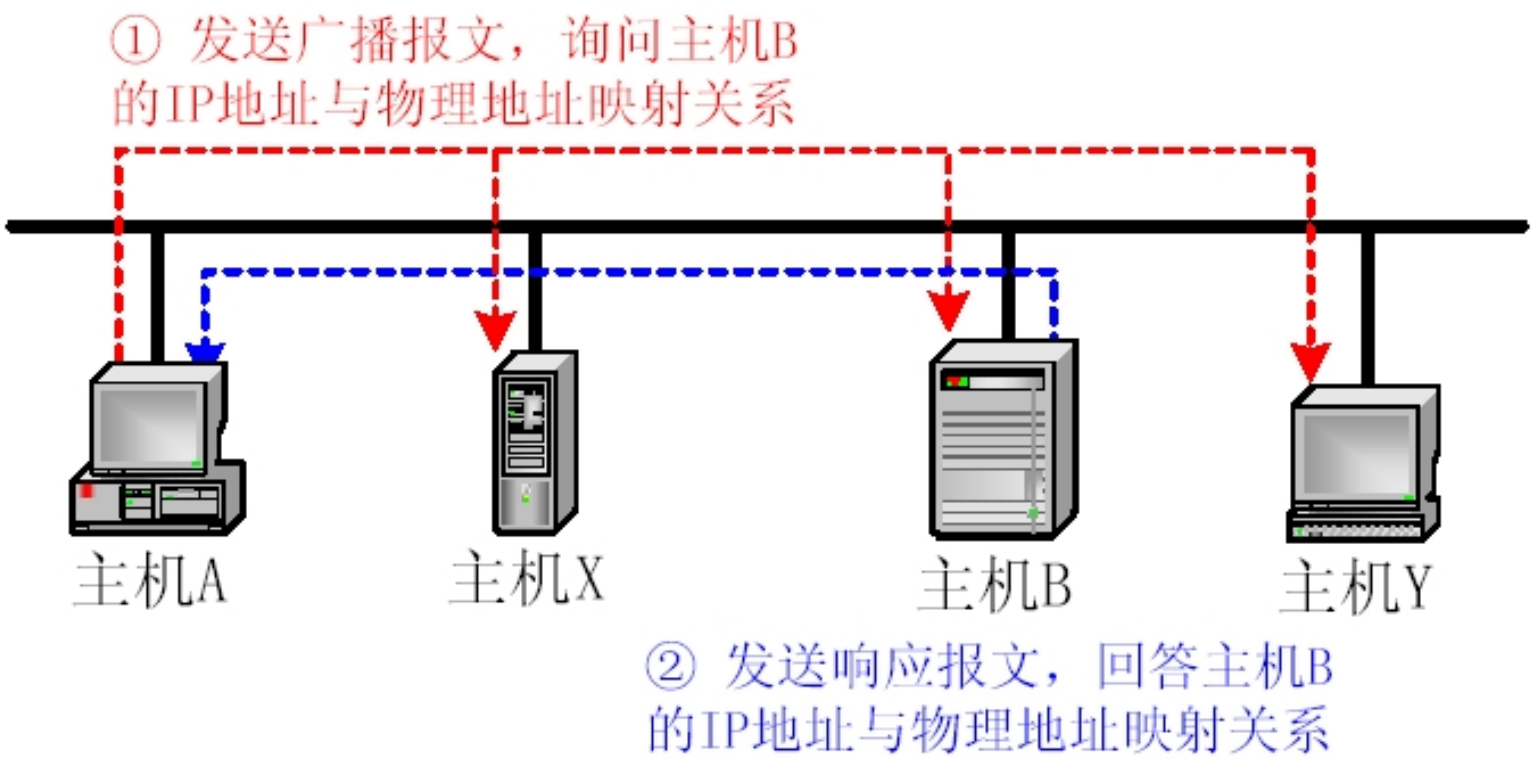
Figure 2-11: USB Network Topology - Daisy Chain and Tree Structures

Table 2-8: Aspects of PHY and Data Link Layer Wireless Technologies

Technology aspect	*Issues and considerations*
Spectrum	What part of the electromagnetic spectrum is used, what is the overall bandwidth available, how is this segmented into channels? What mechanisms are available to control utilised bandwidth to ensure coexistence with other users of the same spectrum?
Propagation	What power levels are permitted by regulatory authorities in the spectrum in question? What mechanisms are available to control the transmitted power or propagation pattern to minimise co-channel interference for other users, maximise effective range or utilise spatial diversity to increase throughput?
Modulation	How is encoded data carried on the physical medium, for example by modulating one or more carriers in phase and/or amplitude, or by modulating pulses in amplitude and/or position?
Data encoding	How are the raw bits of a data frame coded into symbols for transmission? What functions do these coding mechanisms serve, for example increasing robustness to noise or increasing the efficient use of available bandwidth?
Media access	How is access to the transmission medium controlled to ensure that the bandwidth available for data transmission is maximised and that contention between users is efficiently resolved? What mechanisms are available to differentiate media access for users with differing service requirements?



ARP的基本思想


① 发送广播报文，询问主机B
的IP地址与物理地址映射关系
主机A
主机X
主机B
主机Y
② 发送响应报文，回答主机B
的IP地址与物理地址映射关系

ARP协议漏洞

- 漏洞的根源就是ARP协议是无连接的

没有ARP的请求也可以ARP回复.最致命的就是操作系统收到这个请求后就会更新ARP缓存。

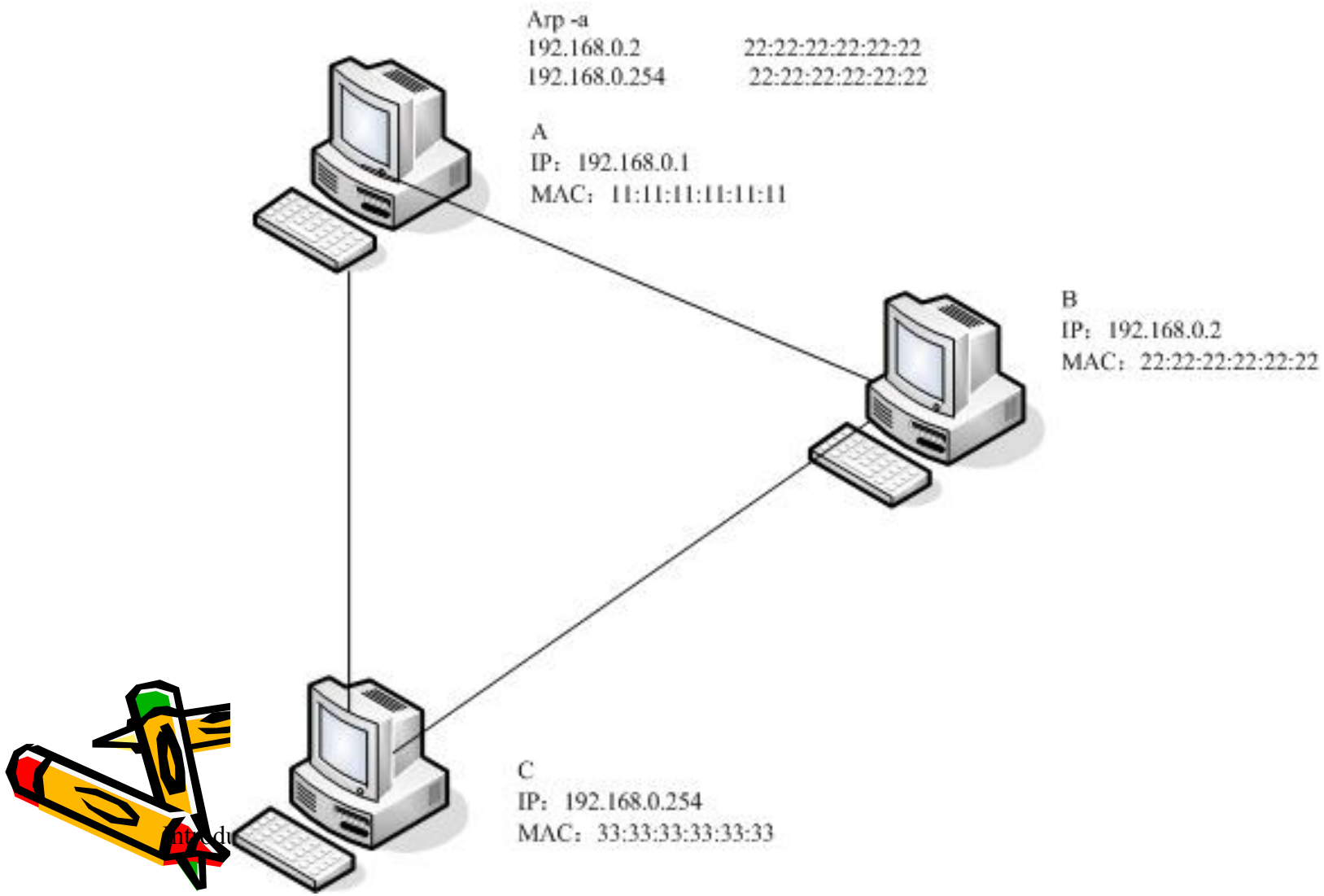
Solaris的特点。

ARP请求也可以伪造。

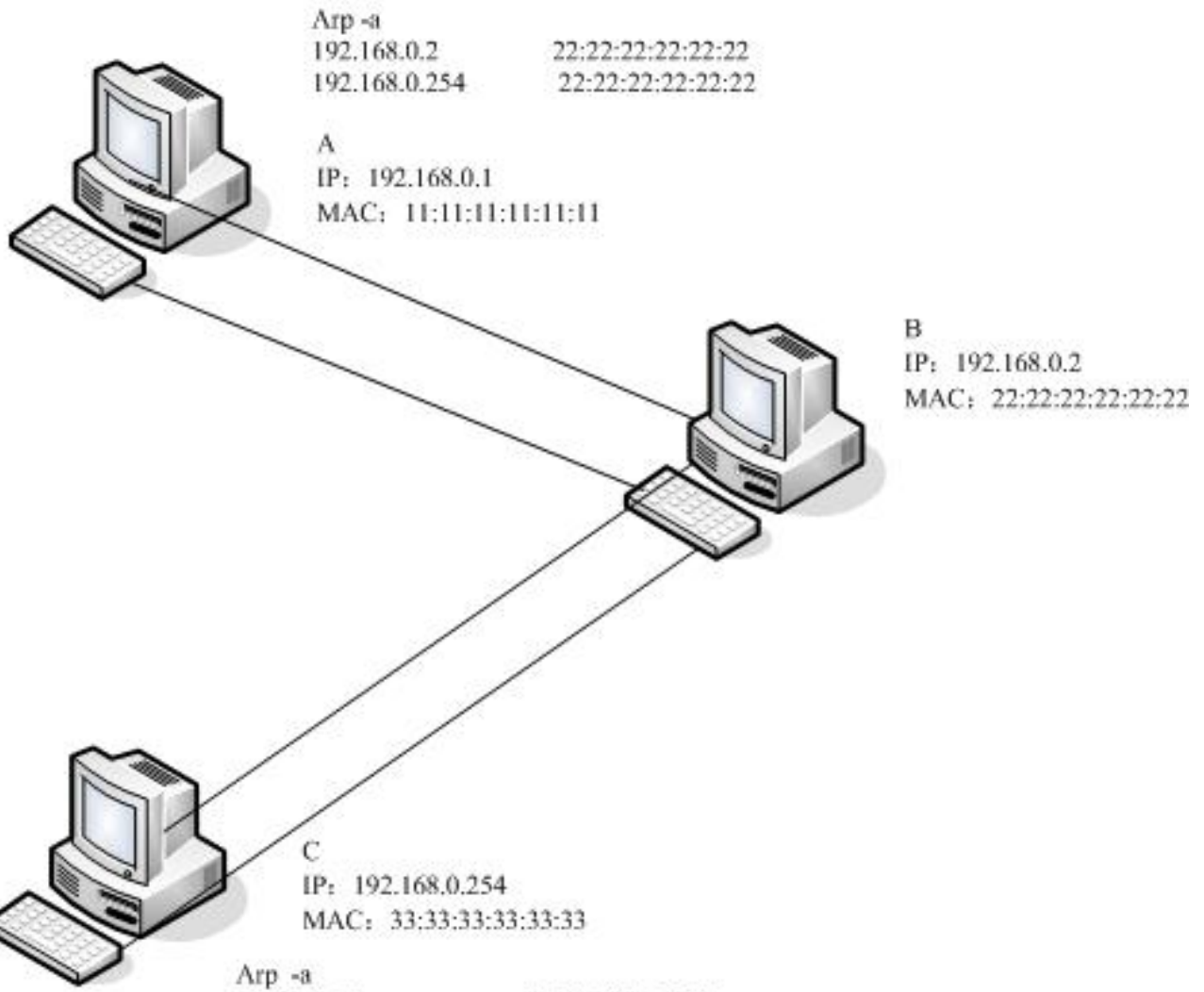
ARP主机的缓存中毒！

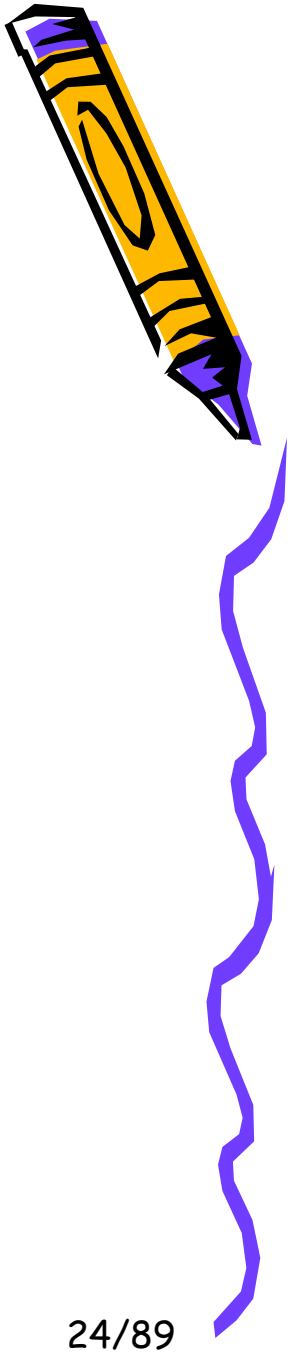
```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.1 --- 0x4
  Internet Address      Physical Address      Type
  222.27.192.31         00-d0-f8-e3-ba-e9     dynamic
  222.27.192.254        00-d0-f8-e3-ba-e9     dynamic
```

ARP的单向欺骗


Arp -a
192.168.0.2 22:22:22:22:22:22
192.168.0.254 22:22:22:22:22:22
A
IP：192.168.0.1
MAC：11:11:11:11:11:11
B
IP：192.168.0.2
MAC：22:22:22:22:22:22
C
IP：192.168.0.254
MAC：33:33:33:33:33:33

ARP的中间人攻击


Arp -a
192.168.0.2 22:22:22:22:22:22
192.168.0.254 22:22:22:22:22:22
A
IP：192.168.0.1
MAC：11:11:11:11:11:11
B
IP：192.168.0.2
MAC：22:22:22:22:22:22
C
IP：192.168.0.254
MAC：33:33:33:33:33:33
Arp -a
192.168.0.1 22:22:22:22:22:22
192.168.0.2 22:22:22:22:22:22



- IPv6 地址数目＝

  340，282，366，920，

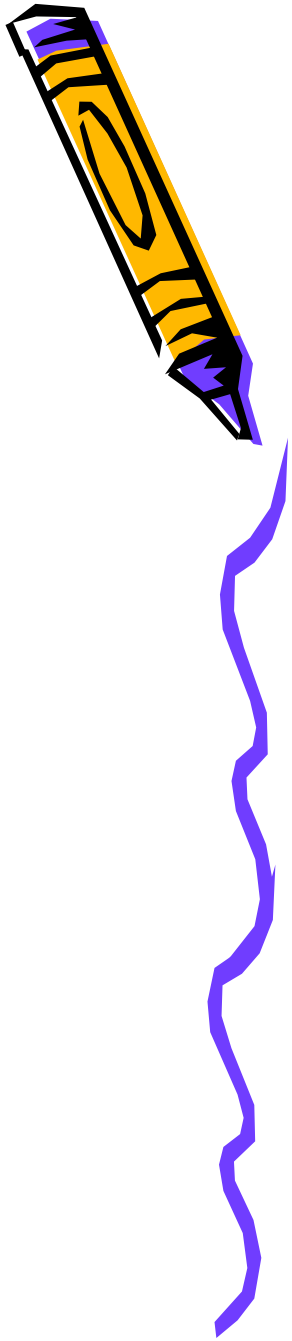
  938，463，463，374，

  607，431，768，211，456

地球上的每个人都可以拥有

5.7×10^{28}个IPv6地址。

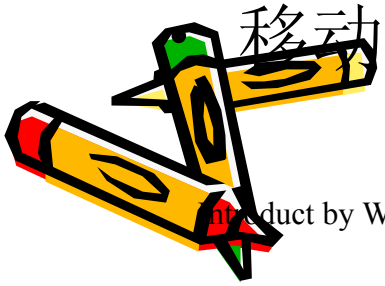
IPv6 - overview



- IPv6 把IP地址的长度增加到了16个字节
- IPv6简化了IP分组的首部格式
- IPv6增强了对进一步扩展的支持
- IPv6增强了对QoS (Quality of Service)的支持
- IPv6增强了对安全的支持
- IPv6增加了对 Anycast 通信方式的支持

IPv6带来的好处

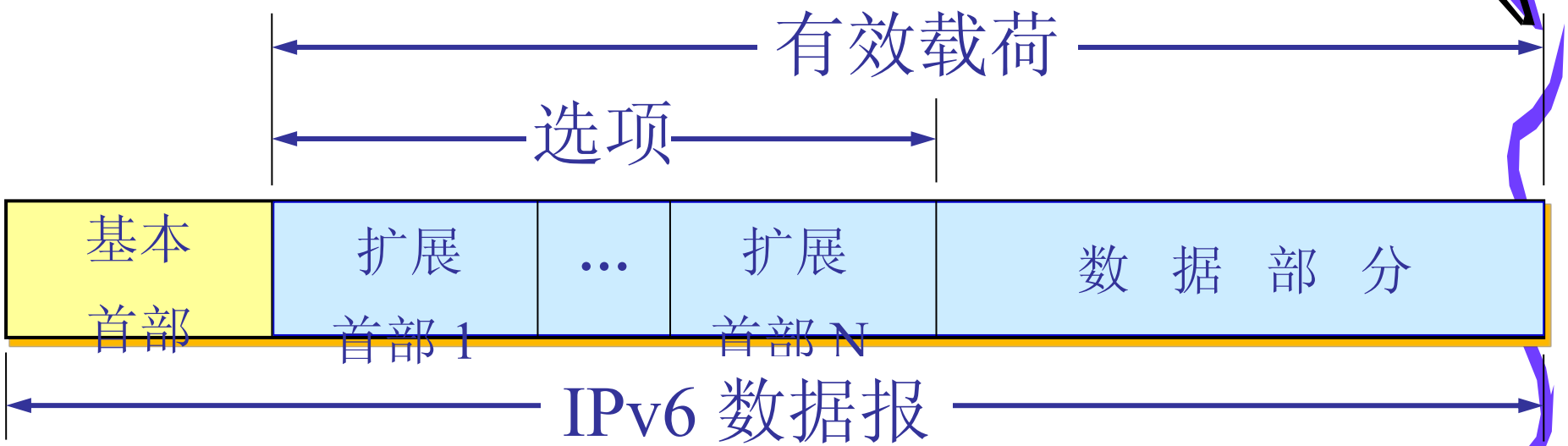
- 几乎无限的地址空间——地址长度由32位增加到128位
- 简单是美——简化固定的基本报头，提高处理效率
- 扩展为先——引入灵活的扩展报头，协议易扩展
- 即插即用——地址配置简化，自动配置
- 贴身安全——网络层的IPSec认证与加密，端到端安全
- 服务质量保证——新增流标记域
- 移动更便捷——Mobile IPv6

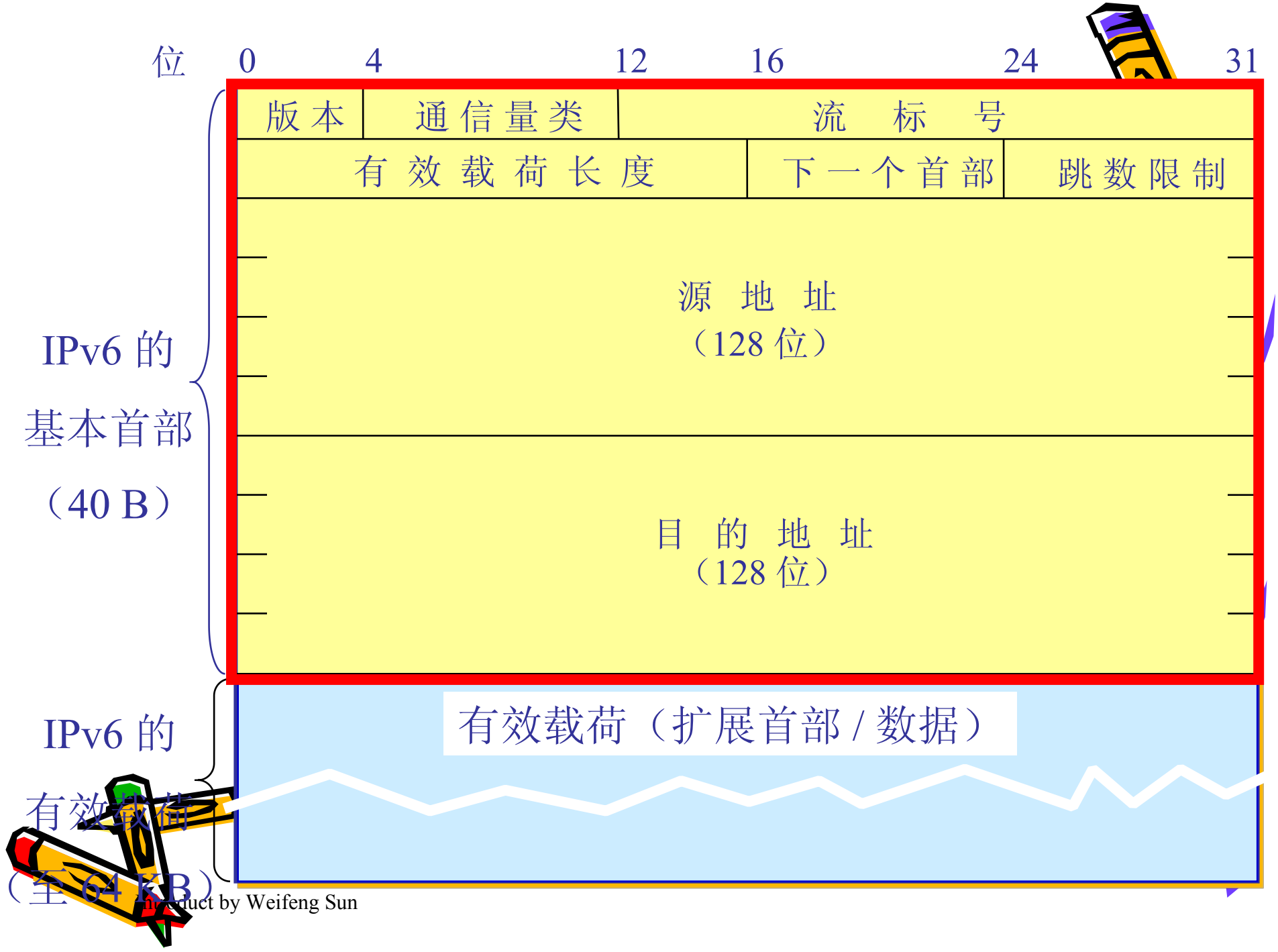


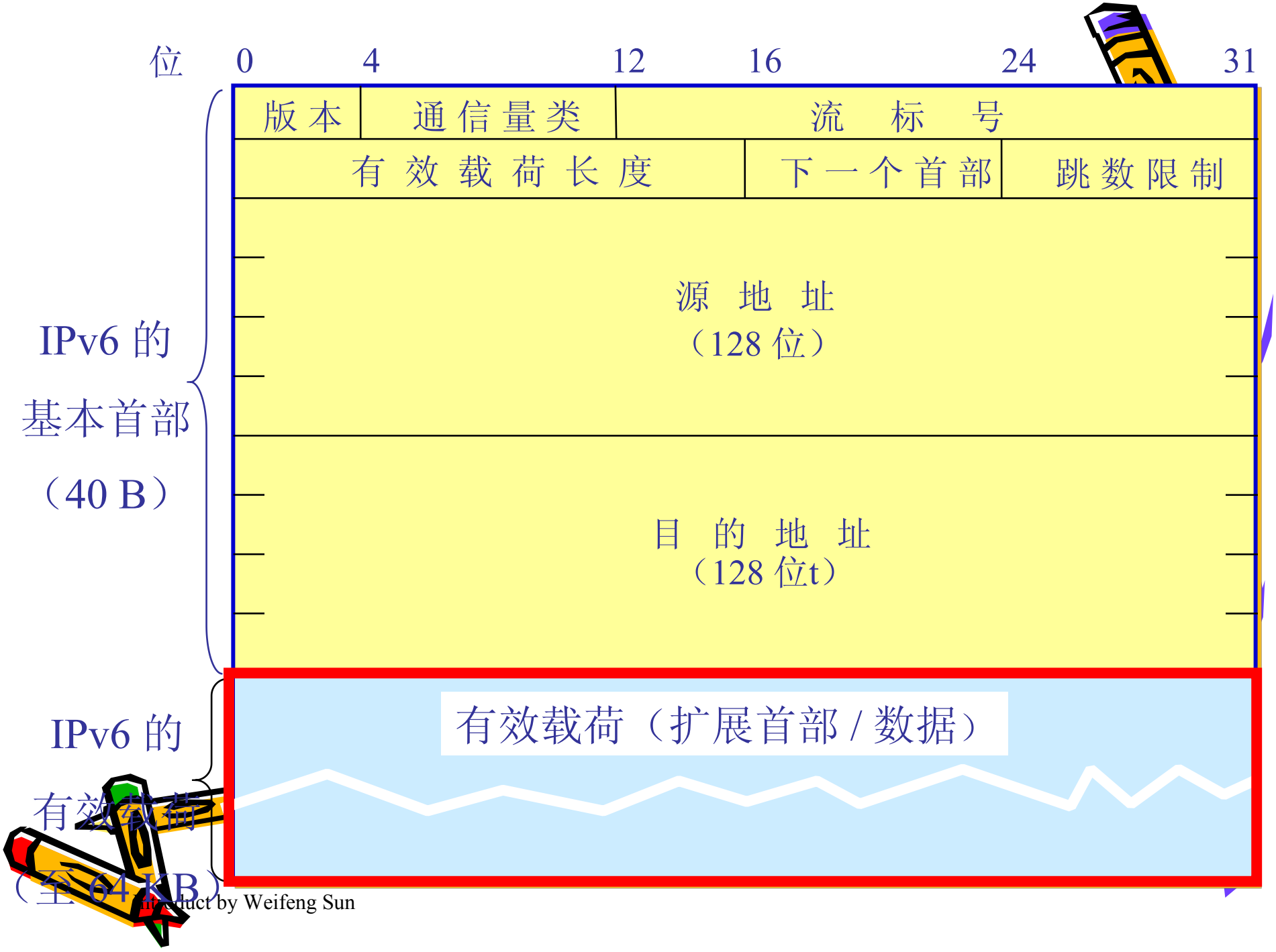
IPv6 数据报的首部

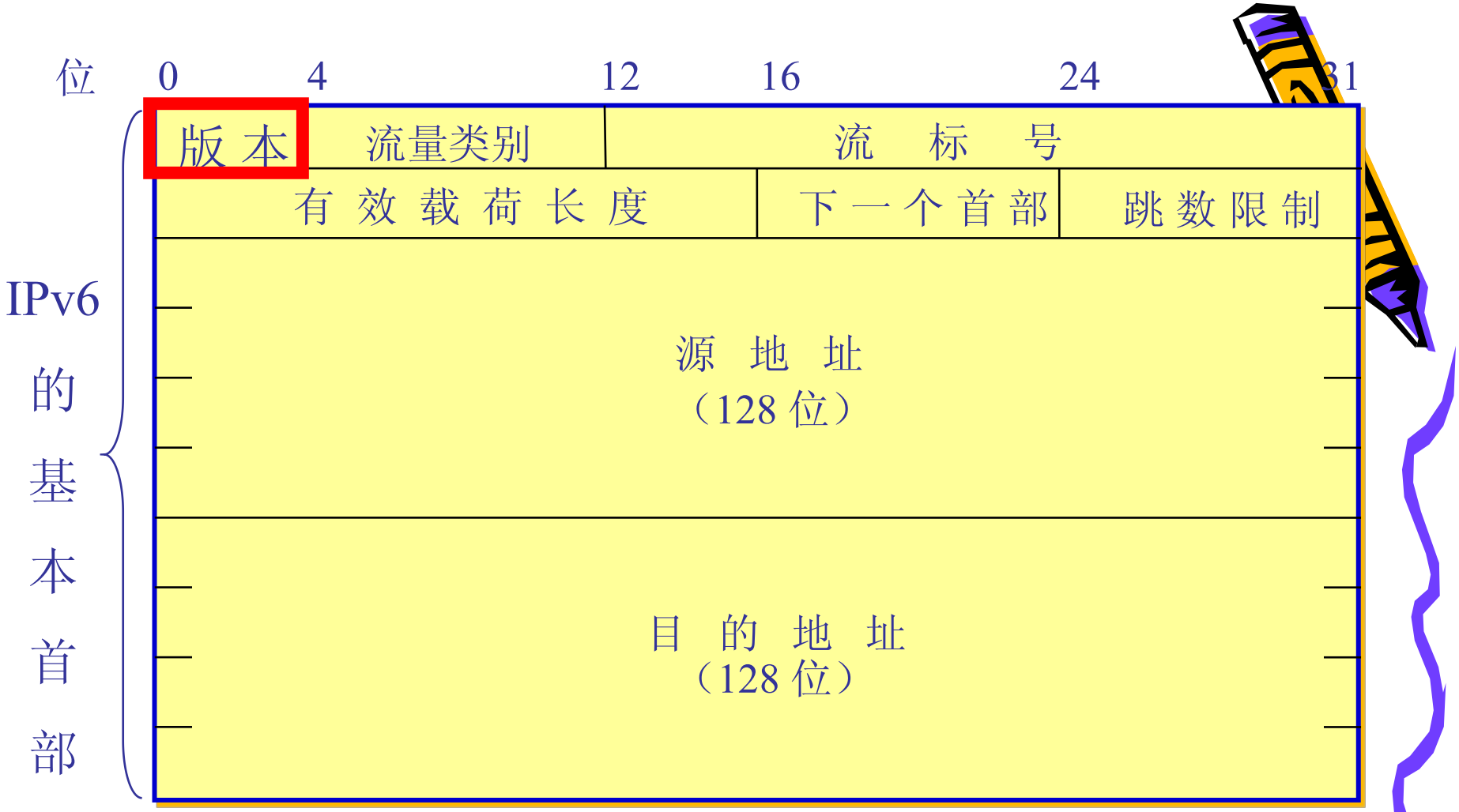
- IPv6 将首部长度变为固定的 40 字节，称为基本首部(base header)。
- 将不必要的功能取消了，首部的字段数减少到只有 8 个。
- 取消了首部的检验和字段，加快了路由器处理数据报的速度。
- 在基本首部的后面允许有零个或多个扩展首部。
- 所有的扩展首部和数据合起来叫做数据报的有效载荷(payload)或净负荷。

IPv6 数据报的一般形式

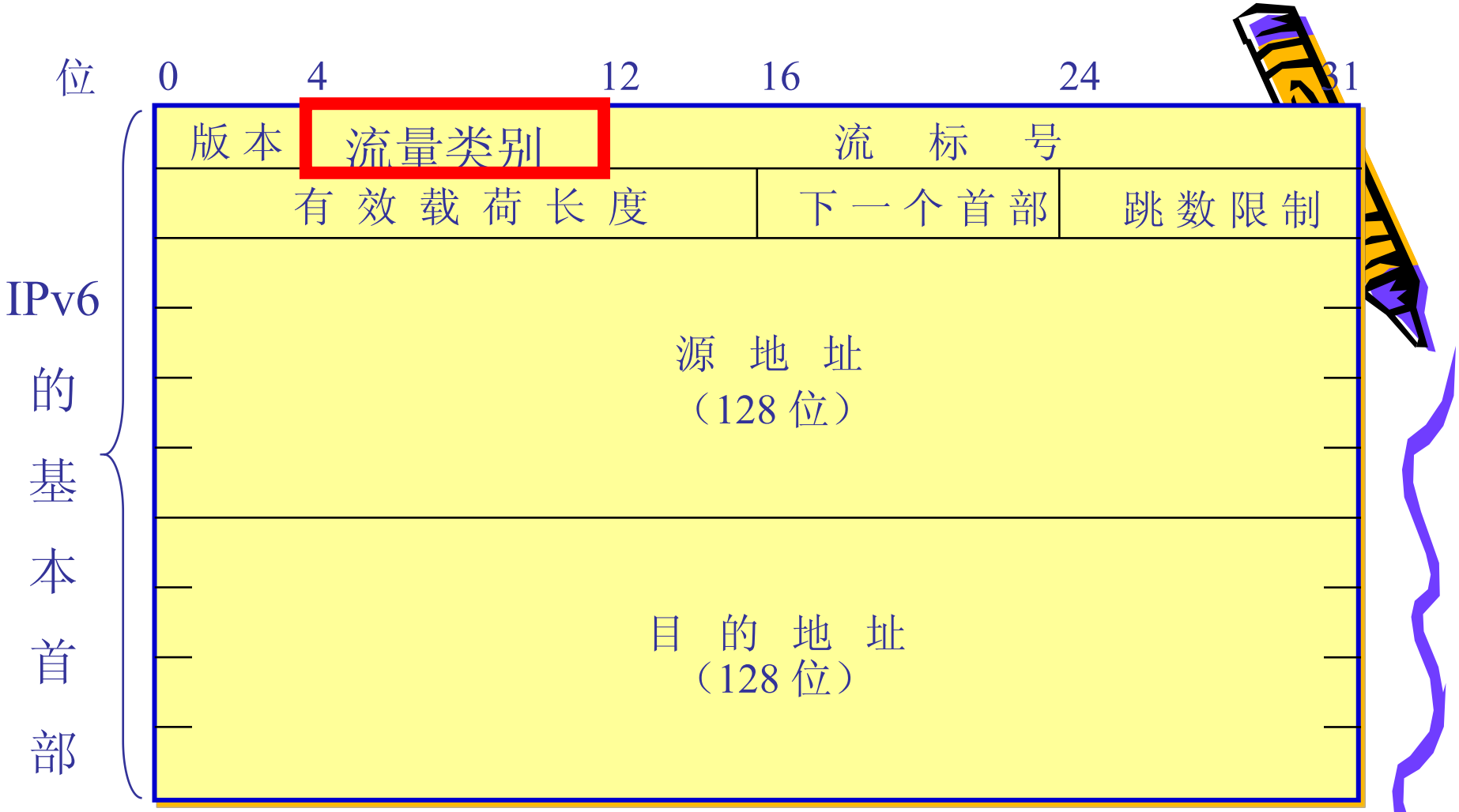




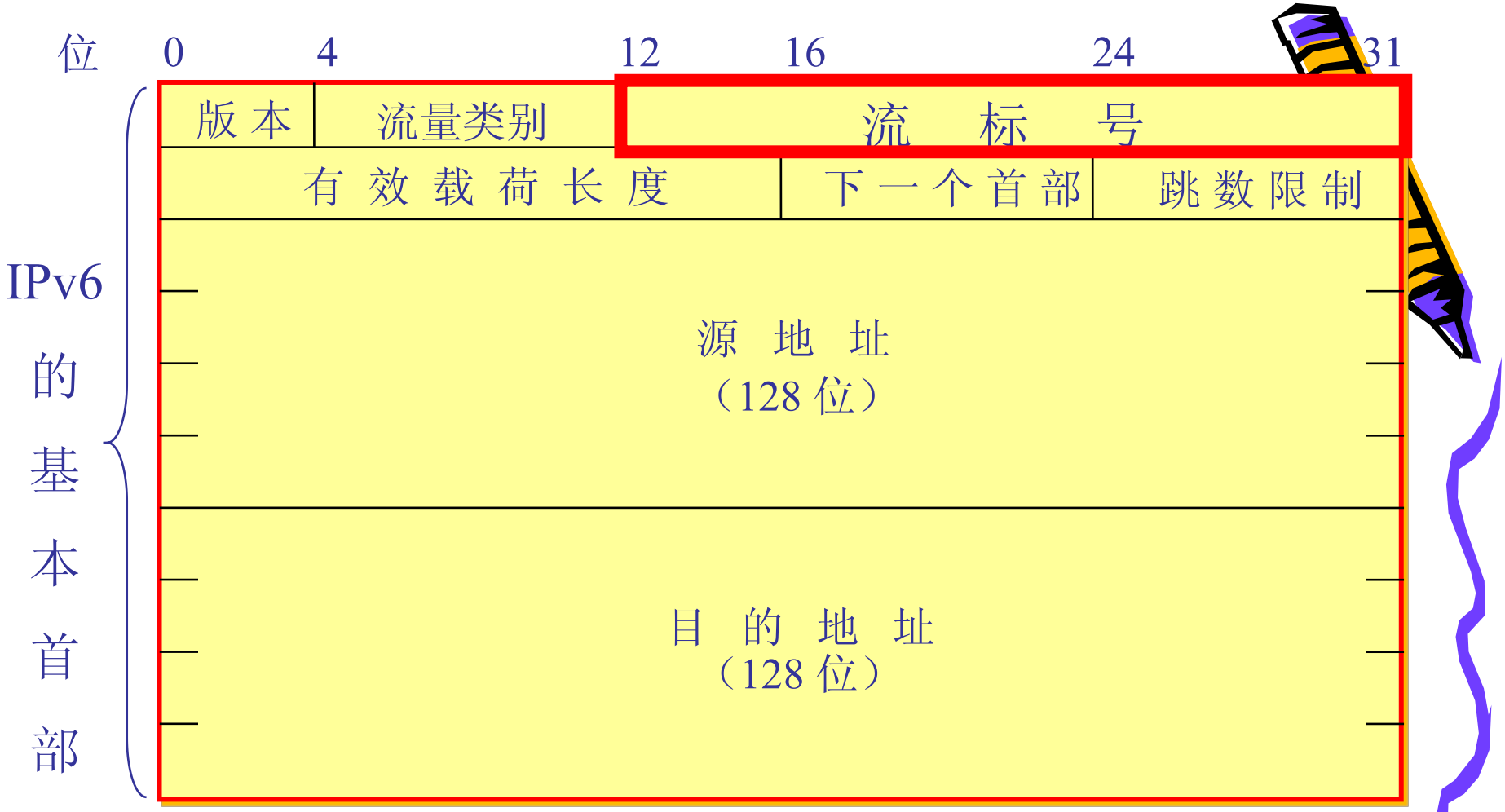

位
0
4
12
16
24
31
版本
通信量类
流 标 号
有效载荷长度
下一个首部
跳数限制
源 地 址
（128 位）
目 的 地 址
（128 位t）
IPv6 的
基本首部
（40 B）
有效载荷（扩展首部 / 数据）
IPv6 的
有效载荷
（至 64 KB）



版本(version)—— 4 位。它指明了协议的版本，对 IPv6 该字段总是 6。



流量类别(traffic class)—— 8 位。这是为了区分不同的 IPv6 数据报的类别或优先级。目前正在进行不同的流量类别性能的实验。



流标号(flow label)—— 20 位。“流”是互联网络上从特定源点到特定终点的一系列数据报，“流”所经过的路径上的路由器都保证指明的服务质量。

所有属于同一个流的数据报都具有同样的流标号。

有效载荷长度(payload length)—— 16 位。它指明 IPv6 数据报除基本首部以外的字节数（所有扩展首部都算在有效载荷之内）。其最大值是 64 KB。

下一个首部(next header)—— 8 位。它相当于 IPv4 的协议字段或可选字段。

跳数限制(hop limit)—— 8 位。源站在数据报发出时即设定跳数限制。路由器在转发数据报时将跳数限制字段中的值减1。

当跳数限制的值为零时，就要将此数据报丢弃。

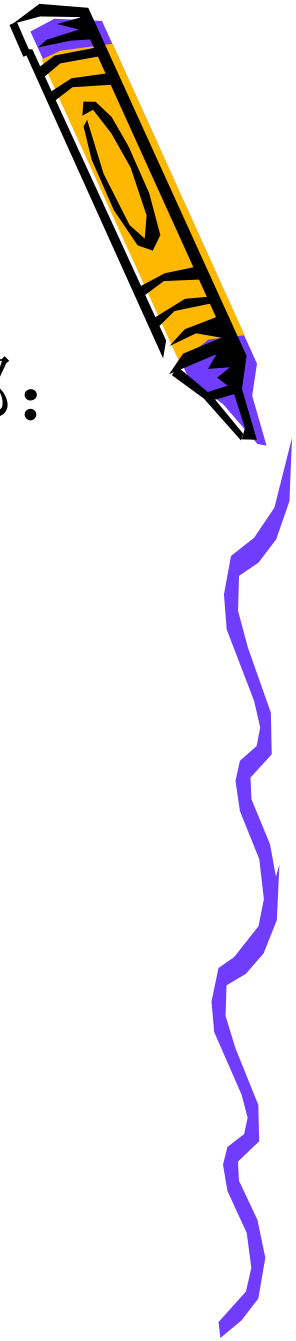
源地址—— 128 位。是数据报的发送站的 IP 地址。

目的地址—— 128 位。是数据报的接收站的 IP 地址。

IPv6 的扩展首部

- IPv6 把原来 IPv4 首部中选项的功能都放在扩展首部中，并将扩展首部留给路径两端的源站和目的站的主机来处理。
- 数据报途中经过的路由器都不处理这些扩展首部（只有一个首部例外，即逐跳选项扩展首部）。
- 这样就大大提高了路由器的处理效率。

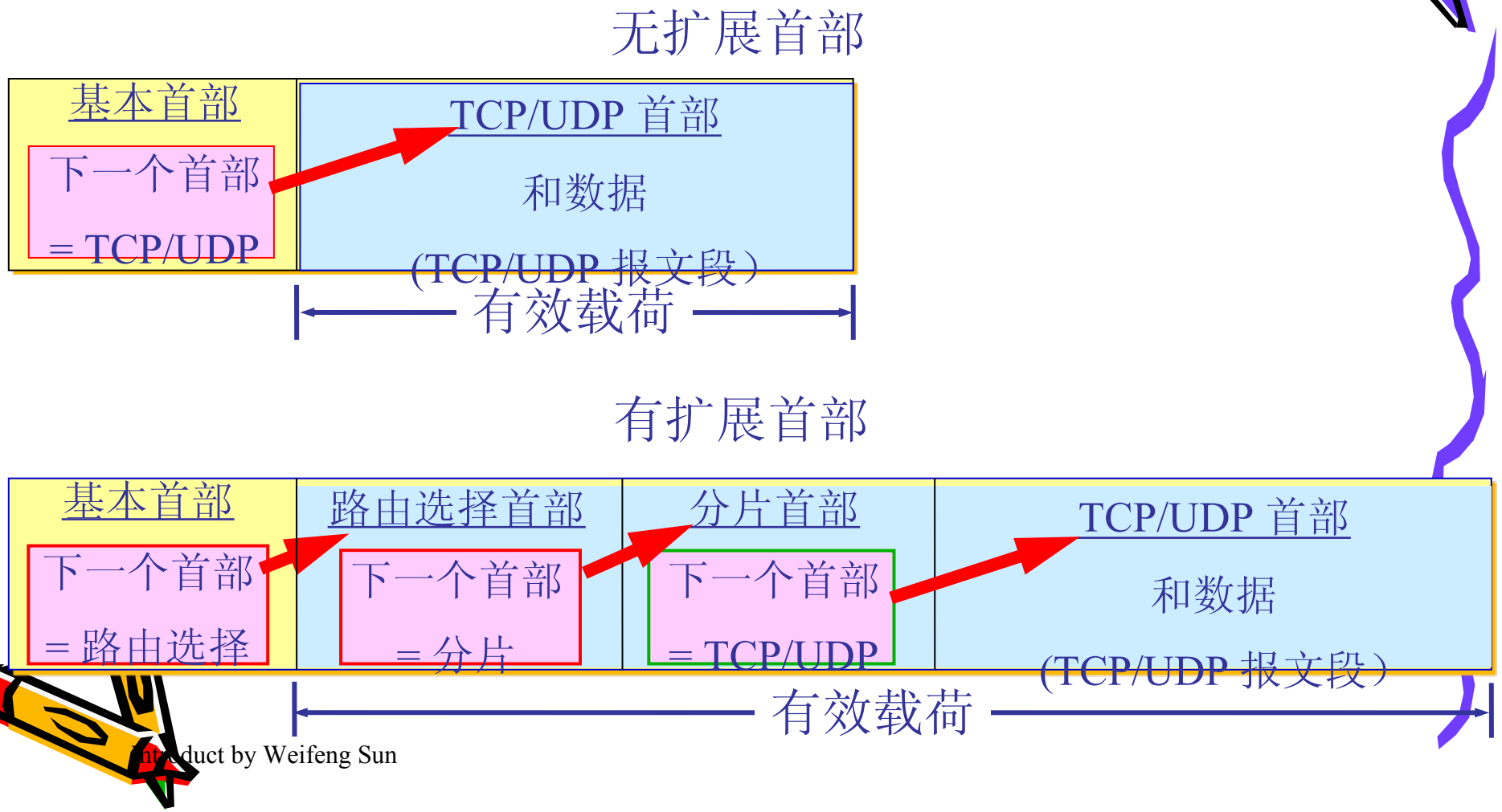
六种扩展首部



在 RFC 2460 中定义了六种扩展首部：

- 逐跳选项
- 路由选择
- 分片
- 鉴别
- 封装安全有效载荷
- 目的站选项

IPv6 的扩展首部


无扩展首部
基本首部
下一个首部
= TCP/UDP
TCP/UDP 首部
和数据
(TCP/UDP 报文段)
有效载荷
有扩展首部
基本首部
下一个首部
= 路由选择
路由选择首部
下一个首部
= 分片
分片首部
下一个首部
= TCP/UDP
TCP/UDP 首部
和数据
(TCP/UDP 报文段)
有效载荷

IPv6 的地址空间

IPv6 数据报的目的地址可以是以下三种基本类型地址之一：

(1) 单播(unicast)　单播就是传统的点对点通信。

(2) 多播(multicast)　多播是一点对多点的通信。

(3) 任播(anycast)　这是 IPv6 增加的一种类型。任播的目的站是一组计算机，但数据报在交付时只交付其中的一个，通常是距离最近的一个。

冒号十六进制记法
(colon hexadecimal notation)

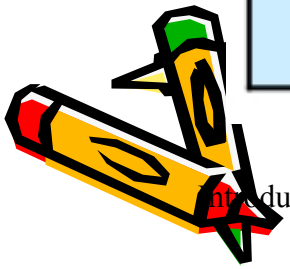
- 每个 16 位的值用十六进制值表示，各值之间用冒号分隔。

68E6:8C64:FFFF:FFFF:0:1180:960A:FFFF

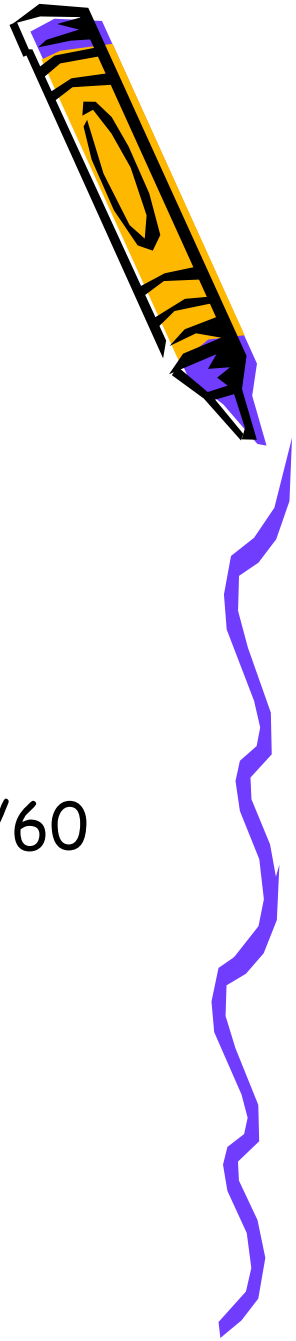
- 零压缩(zero compression)，即一连串连续的零可以为一对冒号所取代。
- FF05:0:0:0:0:0:0:B3　　可以写成：
- FF05::B3

常用IPv6地址类型及格式

地址类型		IPv6前缀标识
单播地址	未指定地址	::/128
	环回地址	::1/128
	链路本地地址	FE80::/10
	站点本地地址	FEC0::/10
	全球单播地址	2000::/3
组播地址		FF00::/8
任播地址		从单播地址空间中进行分配，使用单播地址的格式



点分十进制记法的后缀



- 0:0:0:0:0:0:128.10.2.1

  再使用零压缩即可得出： ::128.10.2.1
- CIDR 的斜线表示法仍然可用。
- 60 位的前缀 12AB00000000CD3 可记为：

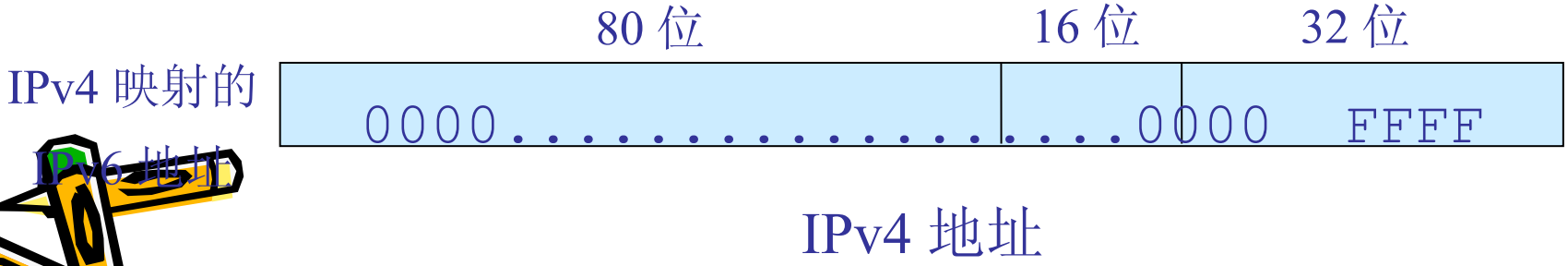
12AB:0000:0000:CD30:0000:0000:0000:0000/60

或12AB::CD30:0:0:0:0/60

或12AB:0:0:CD30::/60

前缀为 0000 0000 的地址

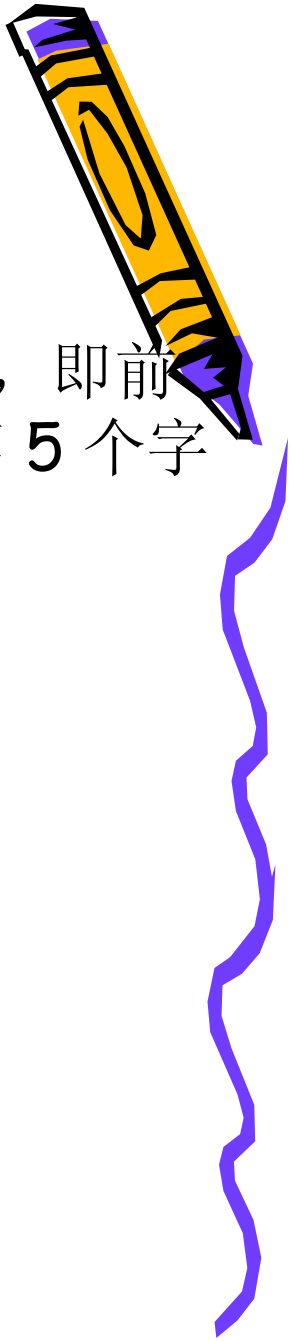
- 前缀为 0000 0000 是保留一小部分地址与 IPv4 兼容的，这是因为必须要考虑到在比较长的时期 IPv4和 IPv6 将会同时存在，而有的结点不支持 IPv6。“IPv4映射的IPv6地址”
- 因此数据报在这两类结点之间转发时，就必须进行地址的转换。



Changes from IPv4

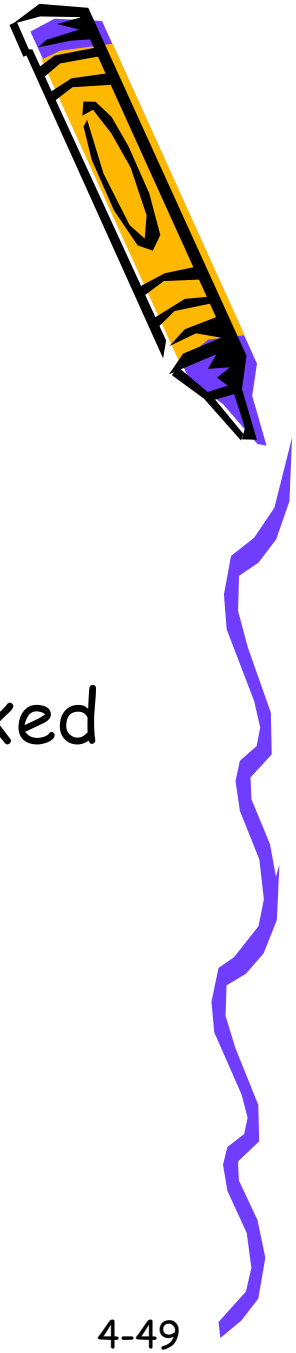
- *Header Length*
  - *使用 Fixed Header : 40 bytes*
- *3 Flag Bits (0, DF, MF), Fragment Offset*
  - *分段有关信息被移动到扩展首部*
- *Checksum:* removed entirely to reduce processing time at each hop
- *Options:* allowed, but outside of header, indicated by "Next Header" field
  - 改变为扩展首部

ICMPv6



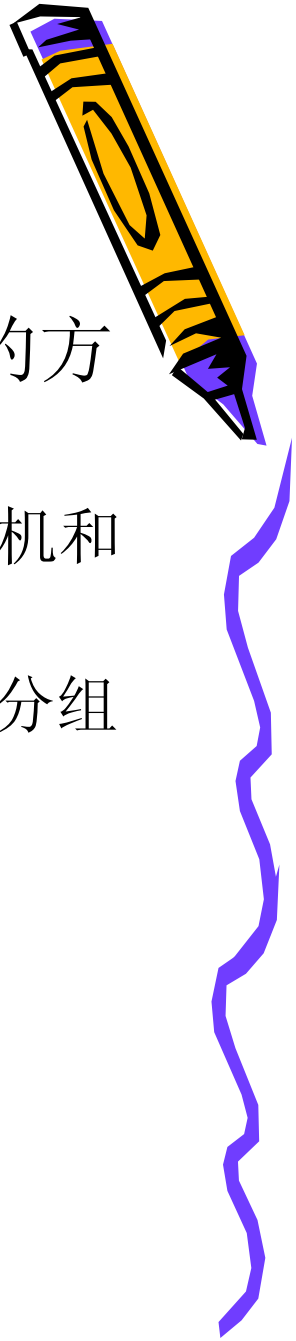
- ICMPv6 的报文格式和 IPv4 使用的 ICMP 的相似，即前 4 个字节的字段名称都是一样的。但 ICMPv6 将第 5 个字节起的后面部分作为报文主体。
  - additional message types, e.g. "Packet Too Big"
  - multicast group management functions
- ICMPv6 的报文划分为四大类
  - 差错报告报文
  - 提供信息的报文
  - 多播听众发现报文
  - 邻站发现报文

Transition From IPv4 To IPv6



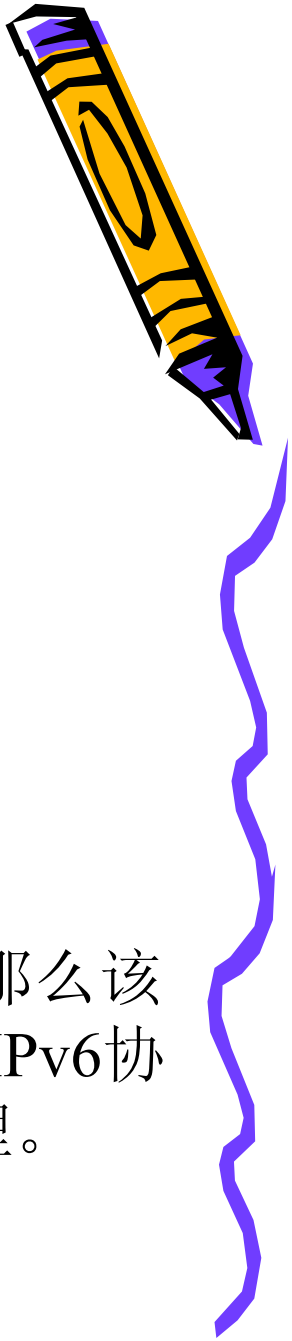
- Not all routers can be upgraded simultaneous
  - no "flag days"
  - How will the network operate with mixed IPv4 and IPv6 routers?

IPv6 - Transition



- RFC 2893 中提出了两种由IPv4向IPv6转变的方法：
  - Dual IP Layer (又称Dual Stack，双协议栈): 在主机和路由器上同时实现IPv4和IPv6两种协议.
  - Tunneling（隧道技术）: 把IPv6分组封装在IPv4分组中传送。

IPv6 - Dual IP Layer

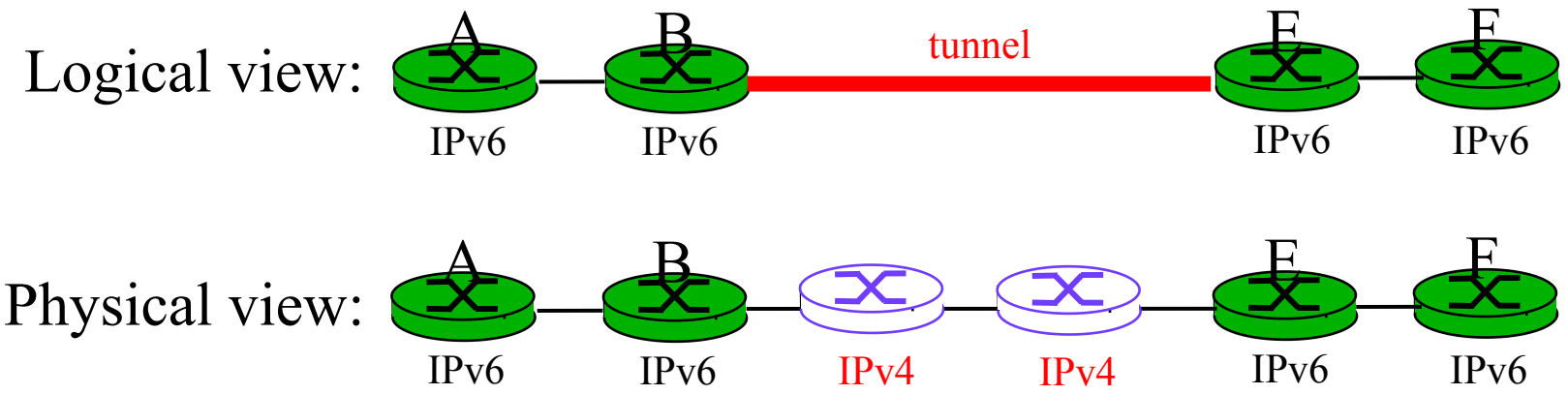


应用程序	
TCP/UDP协议	
IPv6协议	IPv4协议
数据链路层	
物理层	

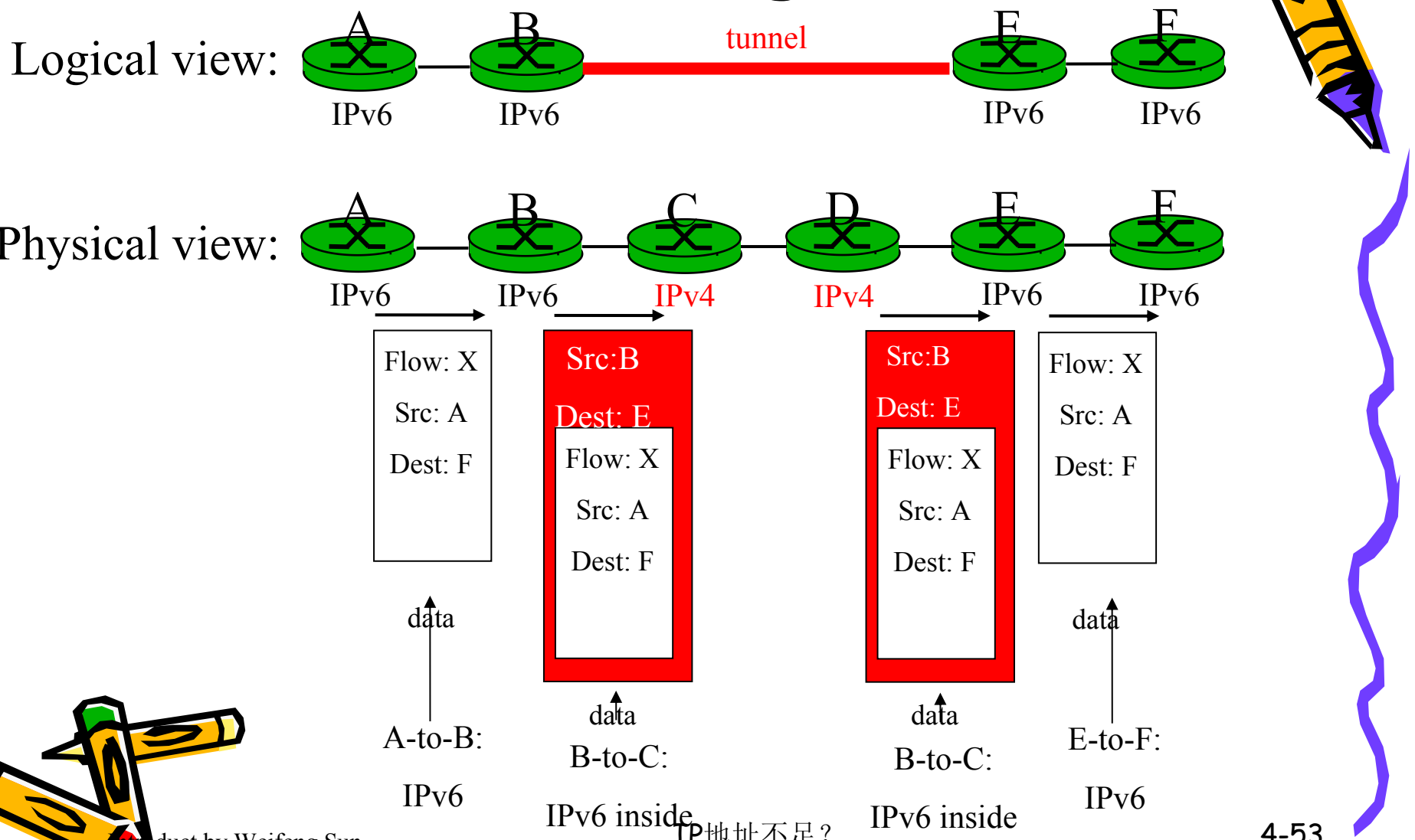
Dual Stack (双协议栈):

如果一台主机同时支持IPv6和IPv4两种协议，那么该主机既能与支持IPv4协议的主机通信，又能与支持IPv6协议的主机通信，这就是双协议栈技术的工作机理。

Tunneling

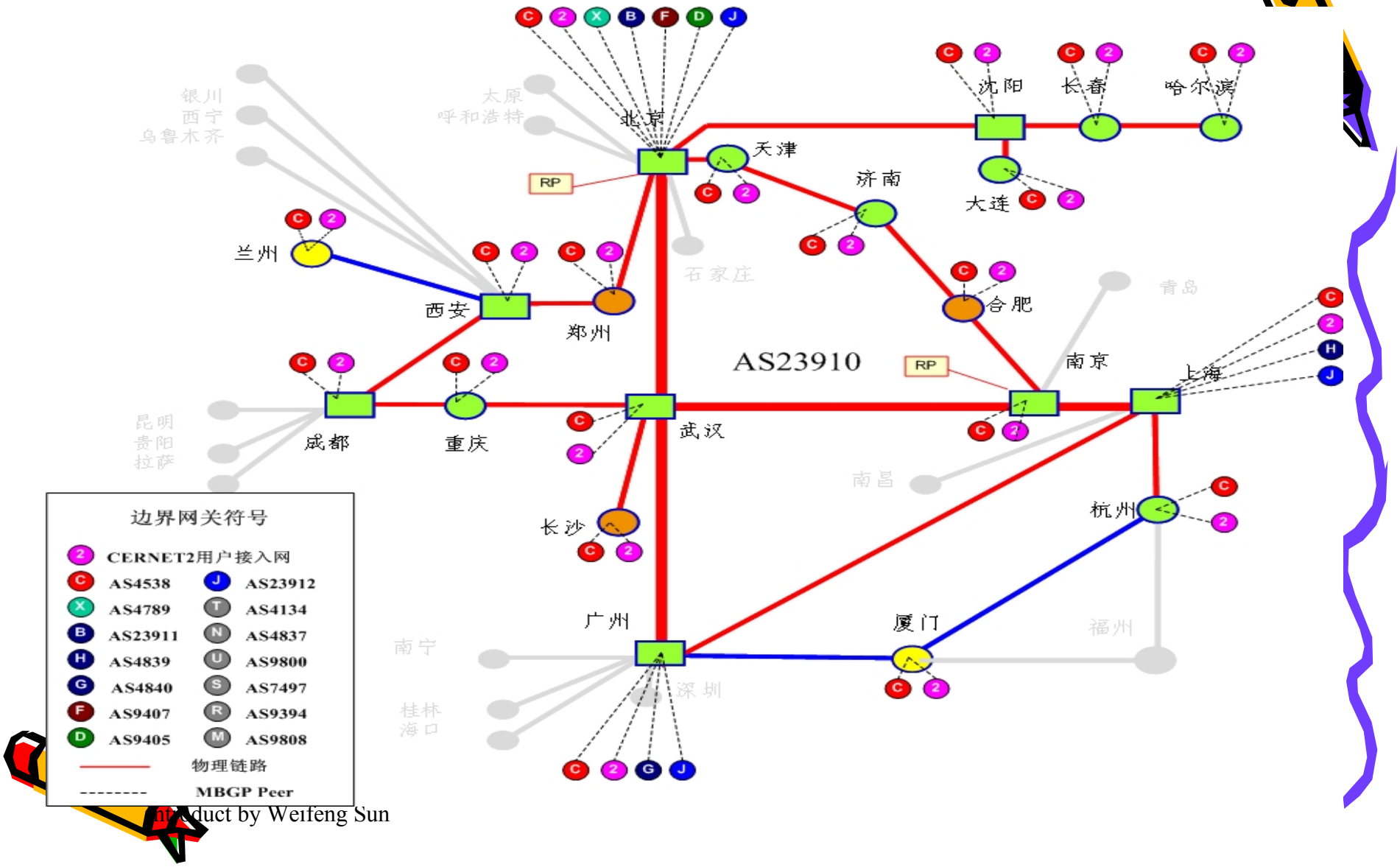

Logical view:
A
B
tunnel
E
F
IPv6
IPv6
IPv6
IPv6
Physical view:
A
B
E
F
IPv6
IPv6
IPv4
IPv4
IPv6
IPv6

Tunneling



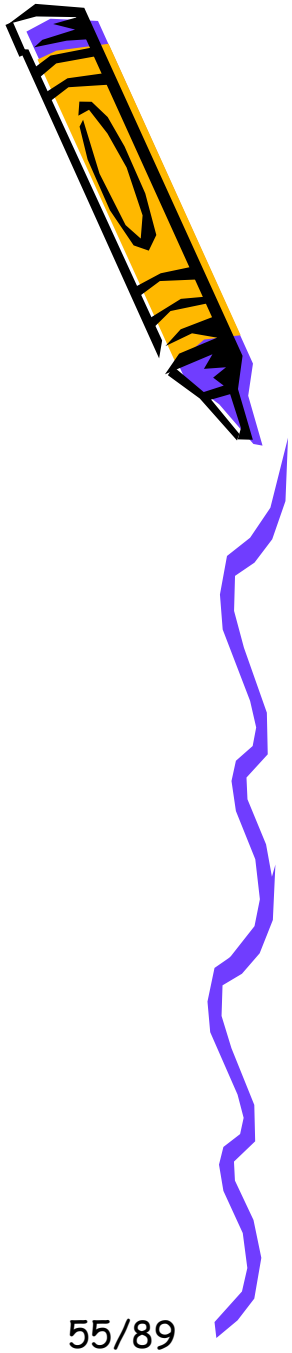
IP地址不足？

CERNET2 Backbone



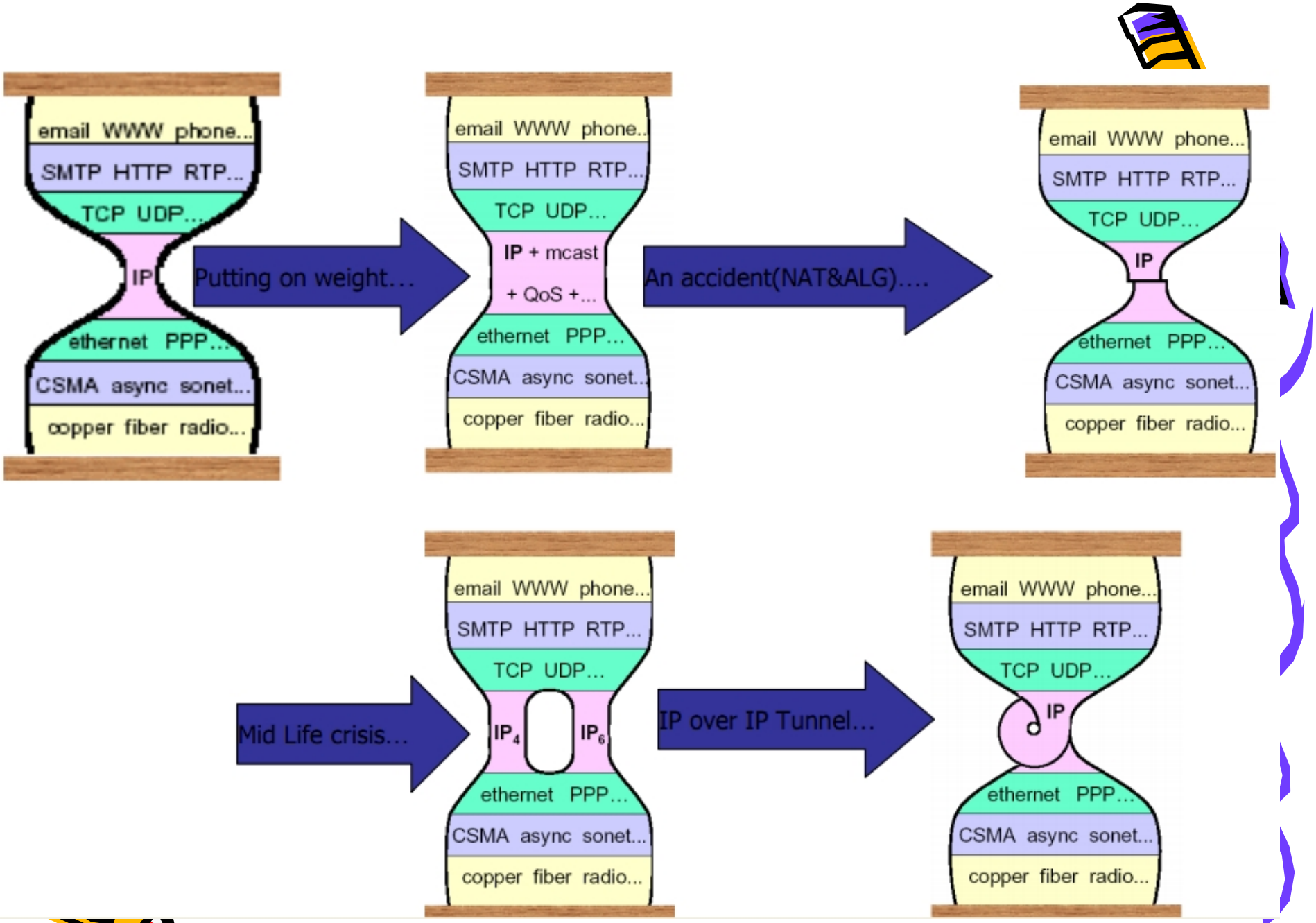
Introduct by Weifeng Sun

IPv6的问题？



- DNSv6？
  - DNS翻译？
- 控制不了
  - 无法通过IP查地理位置

- IPv4快还是IPv6快？


email WWW phone...
SMTP HTTP RTP...
TCP UDP...
IP
ethernet PPP...
CSMA async sonet...
copper fiber radio...
Putting on weight...
email WWW phone...
SMTP HTTP RTP...
TCP UDP...
IP + mcast
+ QoS +...
ethernet PPP...
CSMA async sonet...
copper fiber radio...
An accident(NAT&ALG)....
email WWW phone...
SMTP HTTP RTP...
TCP UDP...
IP
ethernet PPP...
CSMA async sonet...
copper fiber radio...
Mid Life crisis...
email WWW phone...
SMTP HTTP RTP...
TCP UDP...
IP4
IP6
ethernet PPP...
CSMA async sonet...
copper fiber radio...
IP over IP Tunnel...
email WWW phone...
SMTP HTTP RTP...
TCP UDP...
IP
ethernet PPP...
CSMA async sonet...
copper fiber radio...