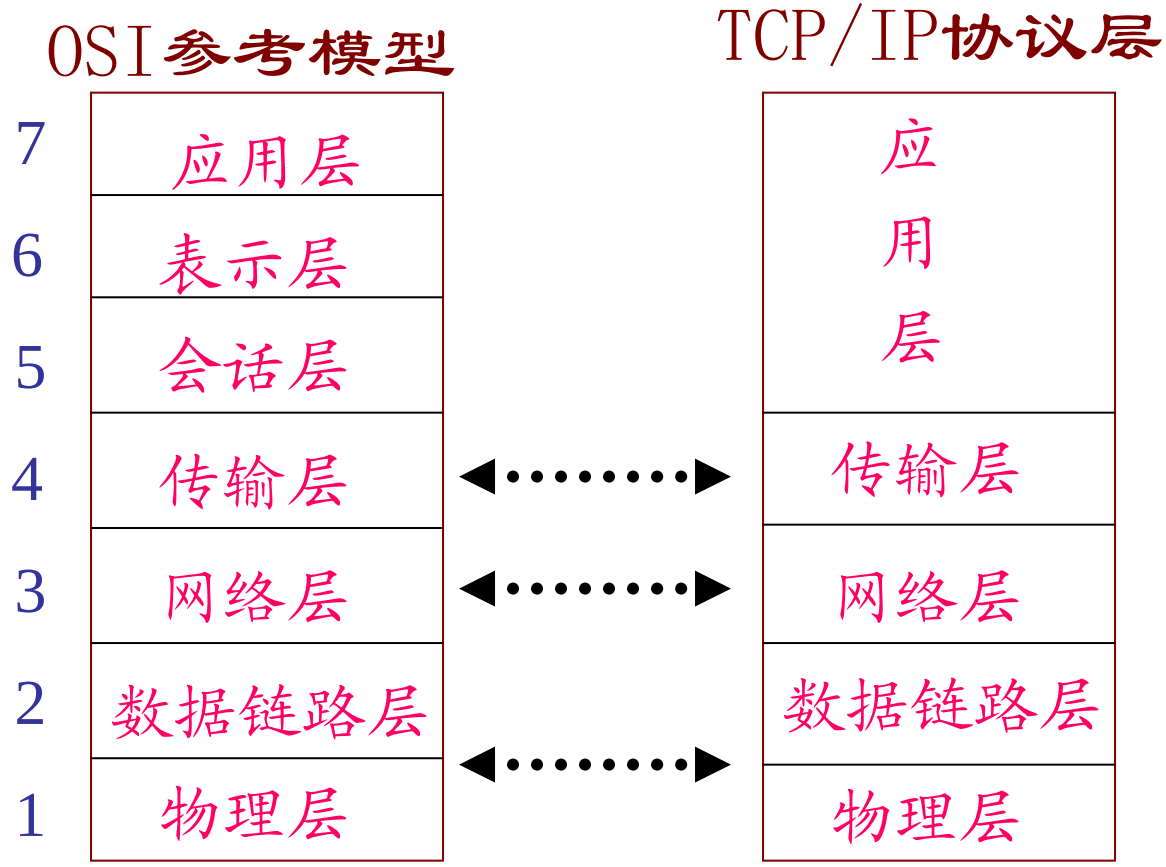
# 培训目标

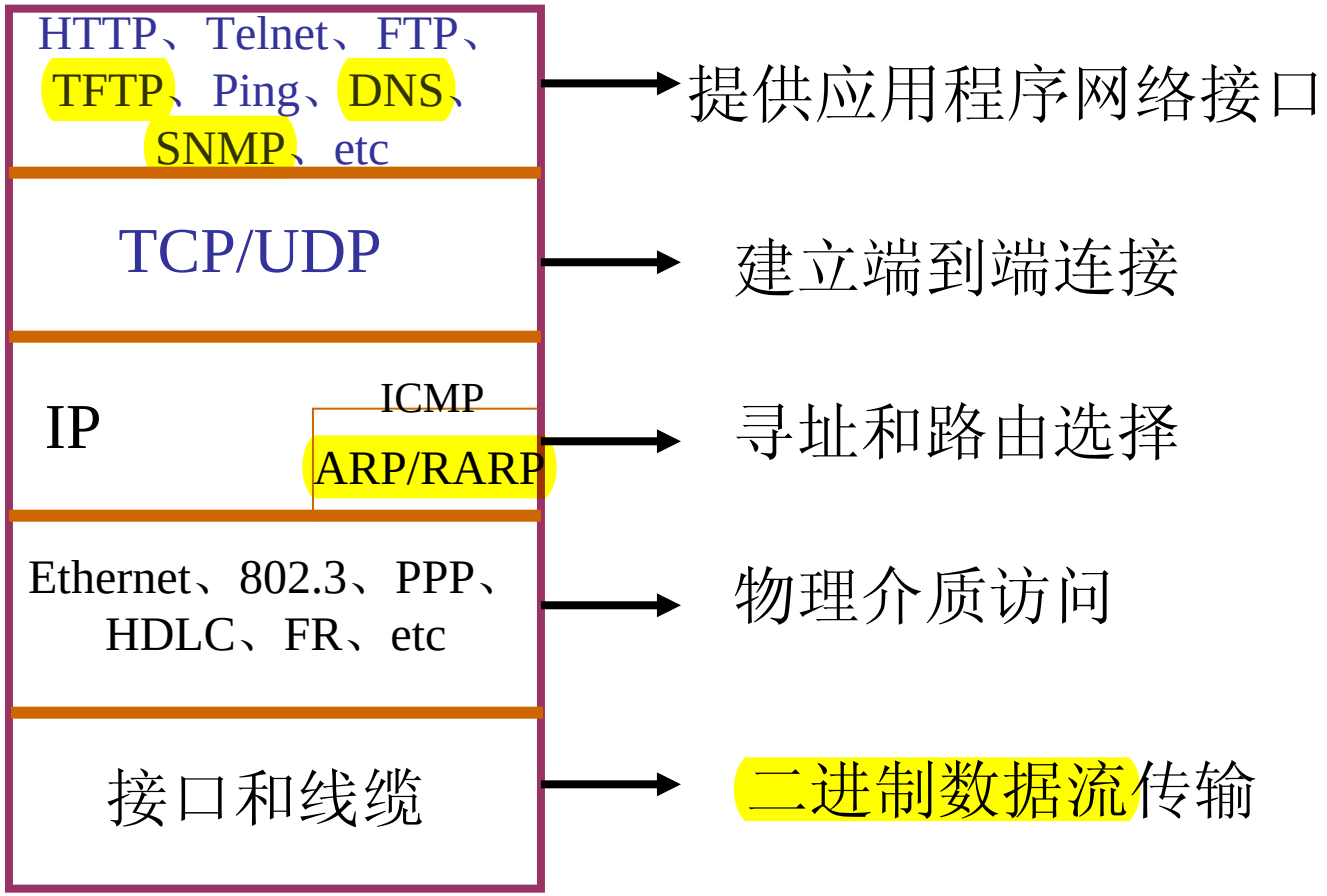
- TCP/IP协议与OSI参考模型
- TCP/IP各层协议原理
- IP地址介绍
- 子网规划原则及举例
- 城域网IP地址规划

# TCP/IP协议与OSI参考模型

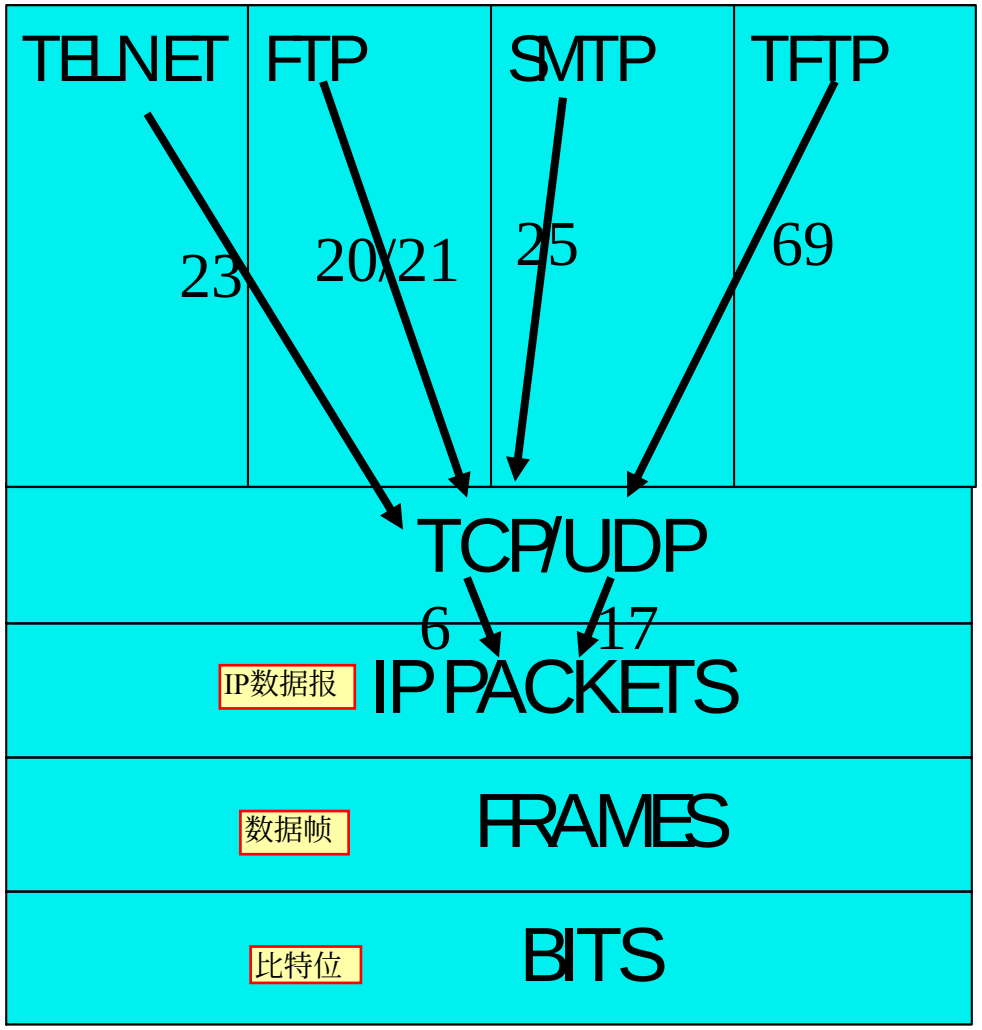



TCP/IP协议具有简单的分层设计
与OSI参考模型有清晰的对应关系。

# TCP/IP协议栈



# TCP/IP协议数据封装




应用层

传输层

网络层

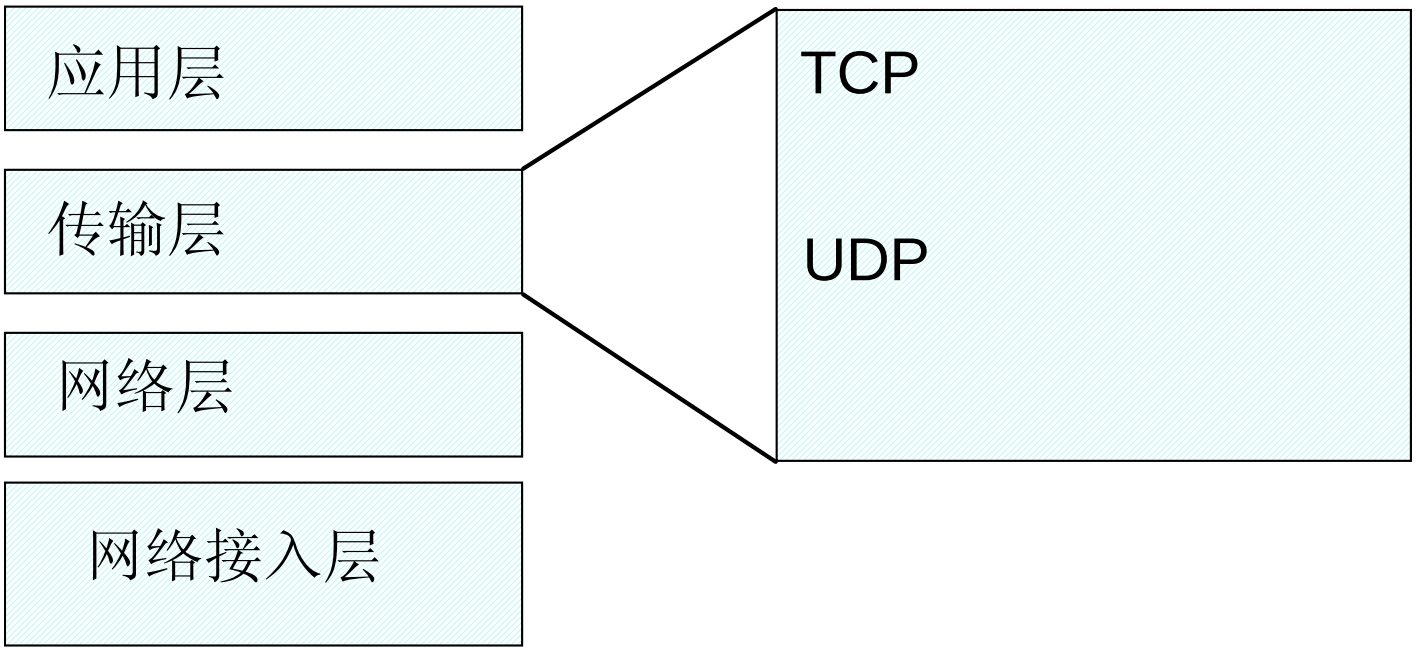
数据链路层

物理层

# 应用层

- 文件传输：
  - FTP、TFTP
- 邮件服务：
  - SMTP、POP3
- 网络管理：
  - SNMP、Telnet、Ping、Tracert
- 网络服务：
  - HTTP、DNS、WINS

# 传输层协议概述



# TCP/UDP报文

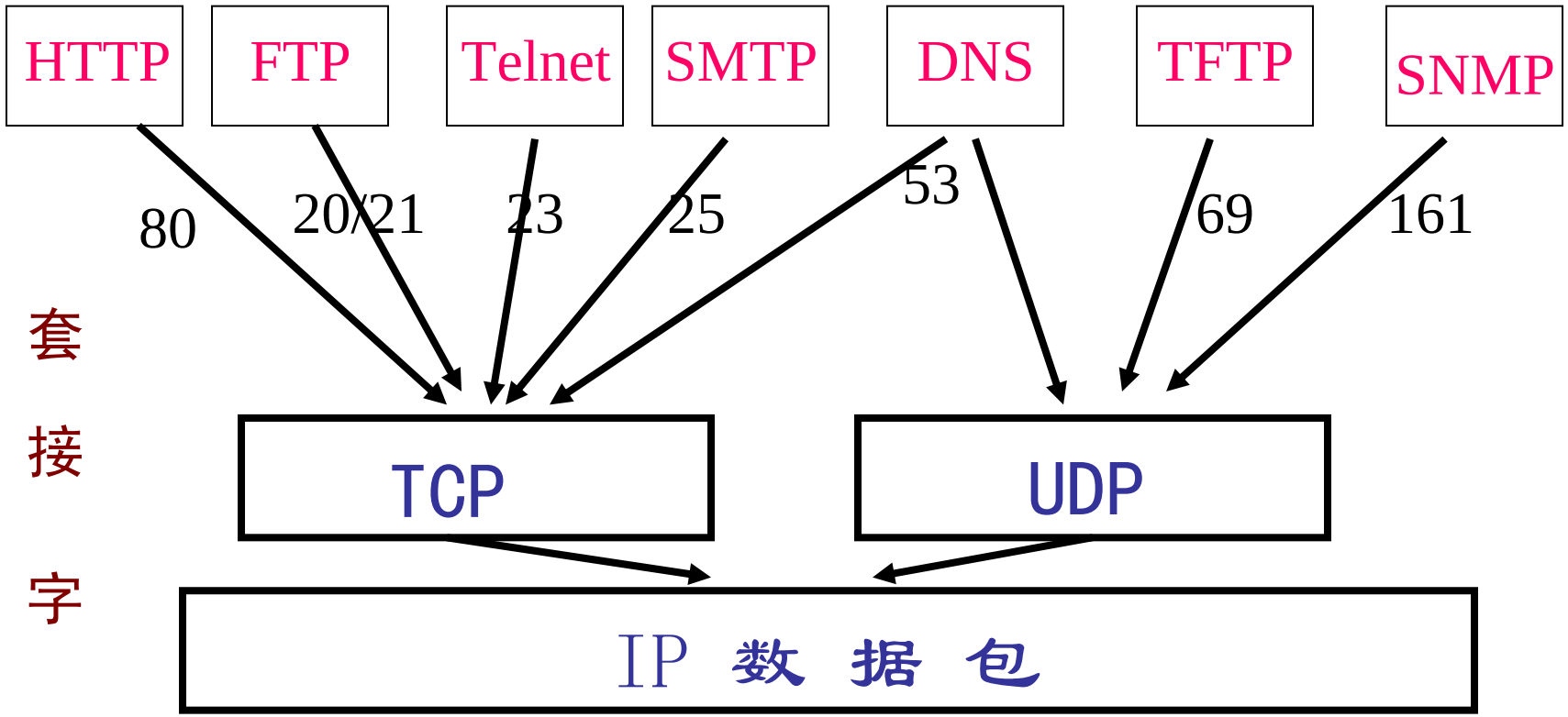
## TCP报文格式

| 源端口 | 目的端口 | 序列号 | 确认号 | 偏移量 |
|---|---|---|---|---|
| 标志 | 窗口 | 校验和 | 选项 | 数据 |

## UDP报文格式

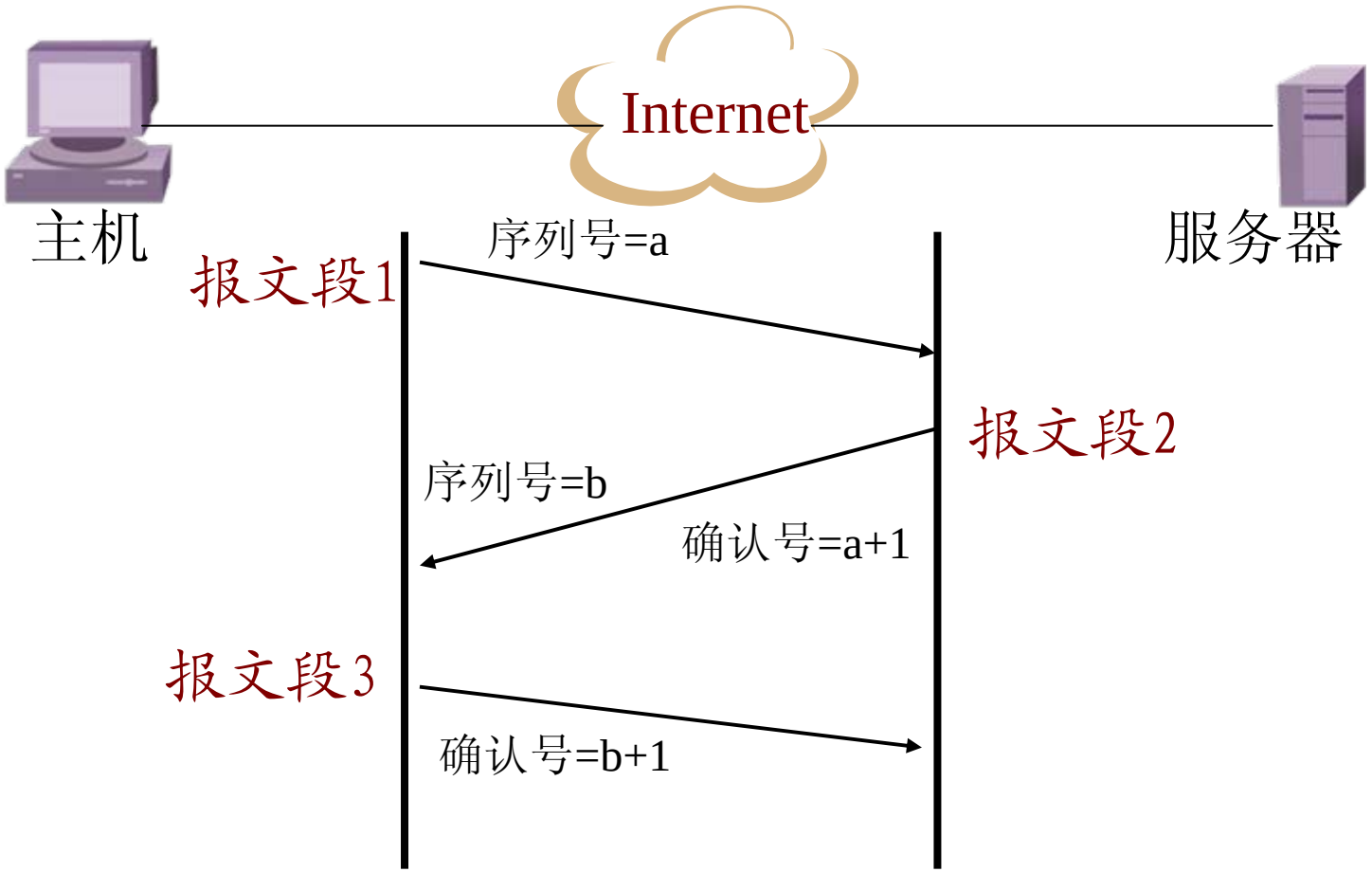
| 源端口 | 目的端口 | 长度 | 校验和 | 数据…… |
|---|---|---|---|---|

# 端 口 号

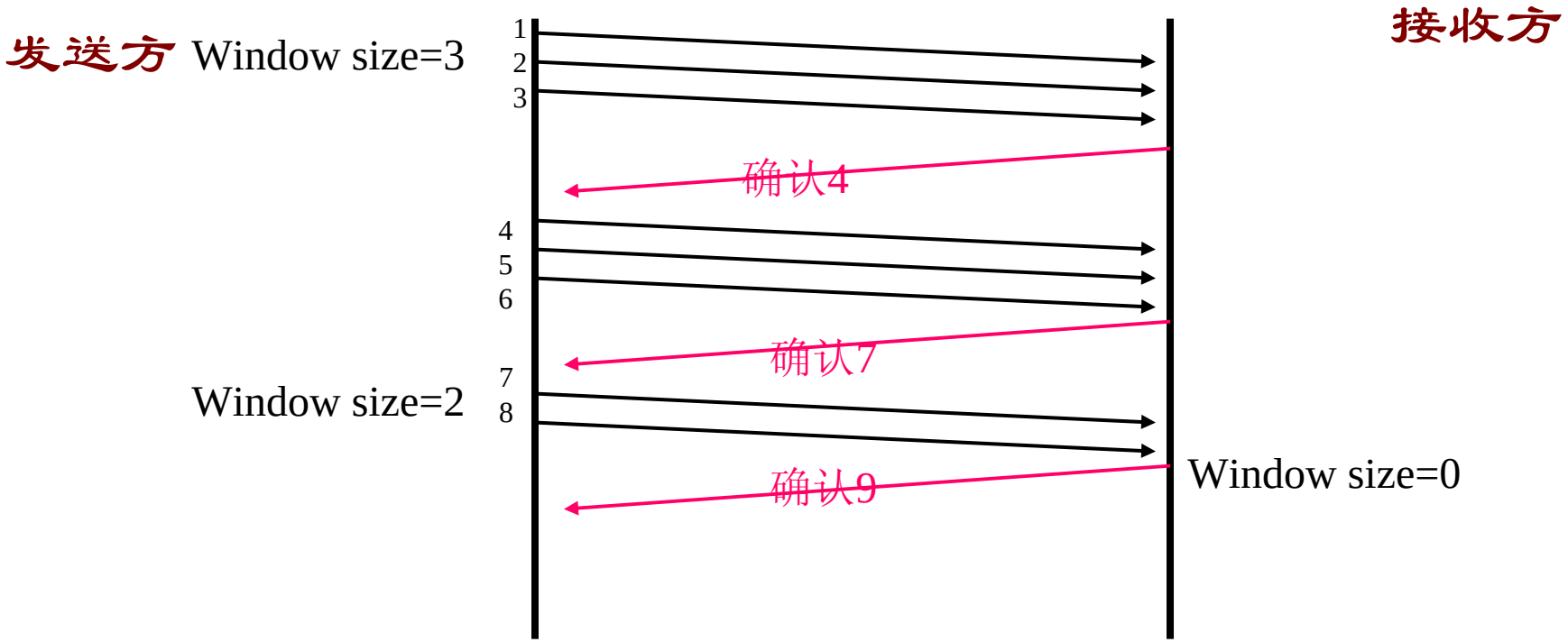



传输层协议用端口号来标示和区分各种应用程序

# TCP连接

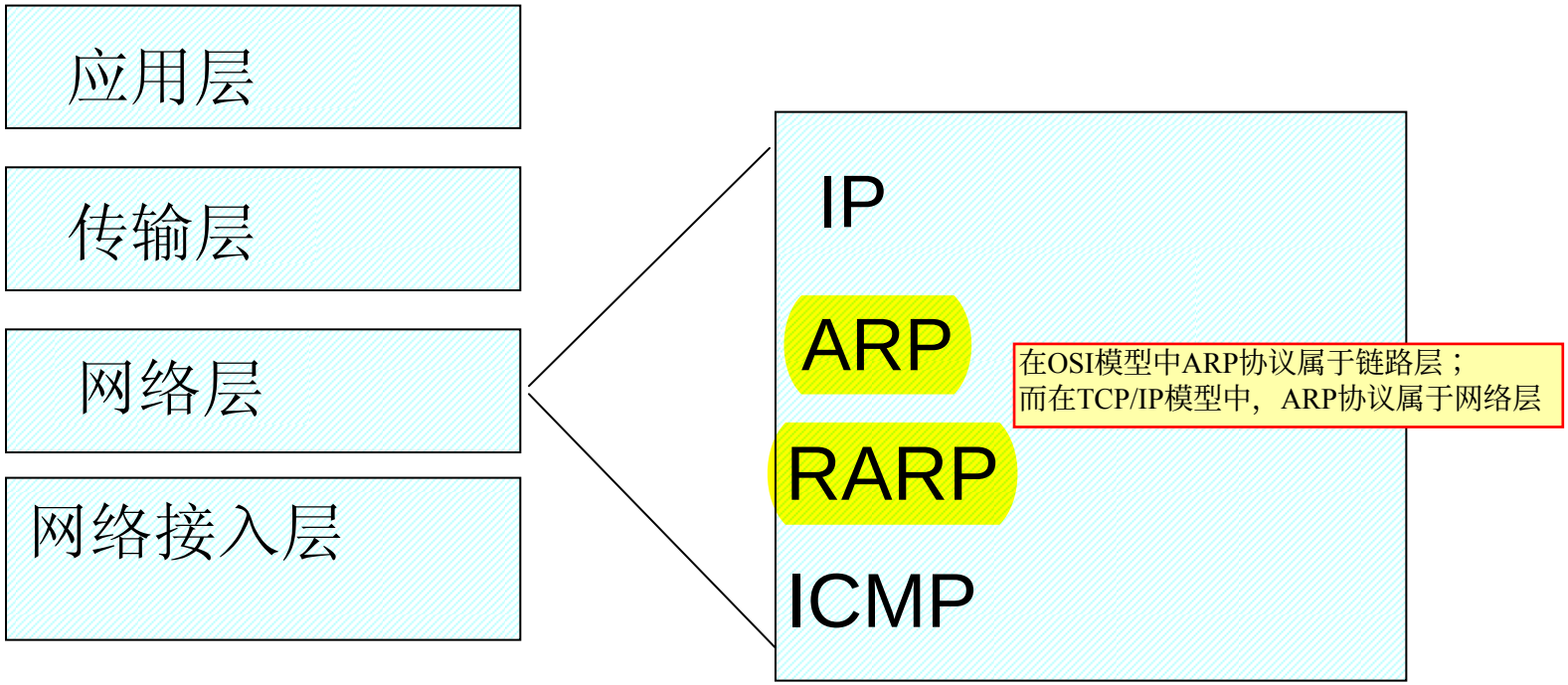


# 滑动窗口

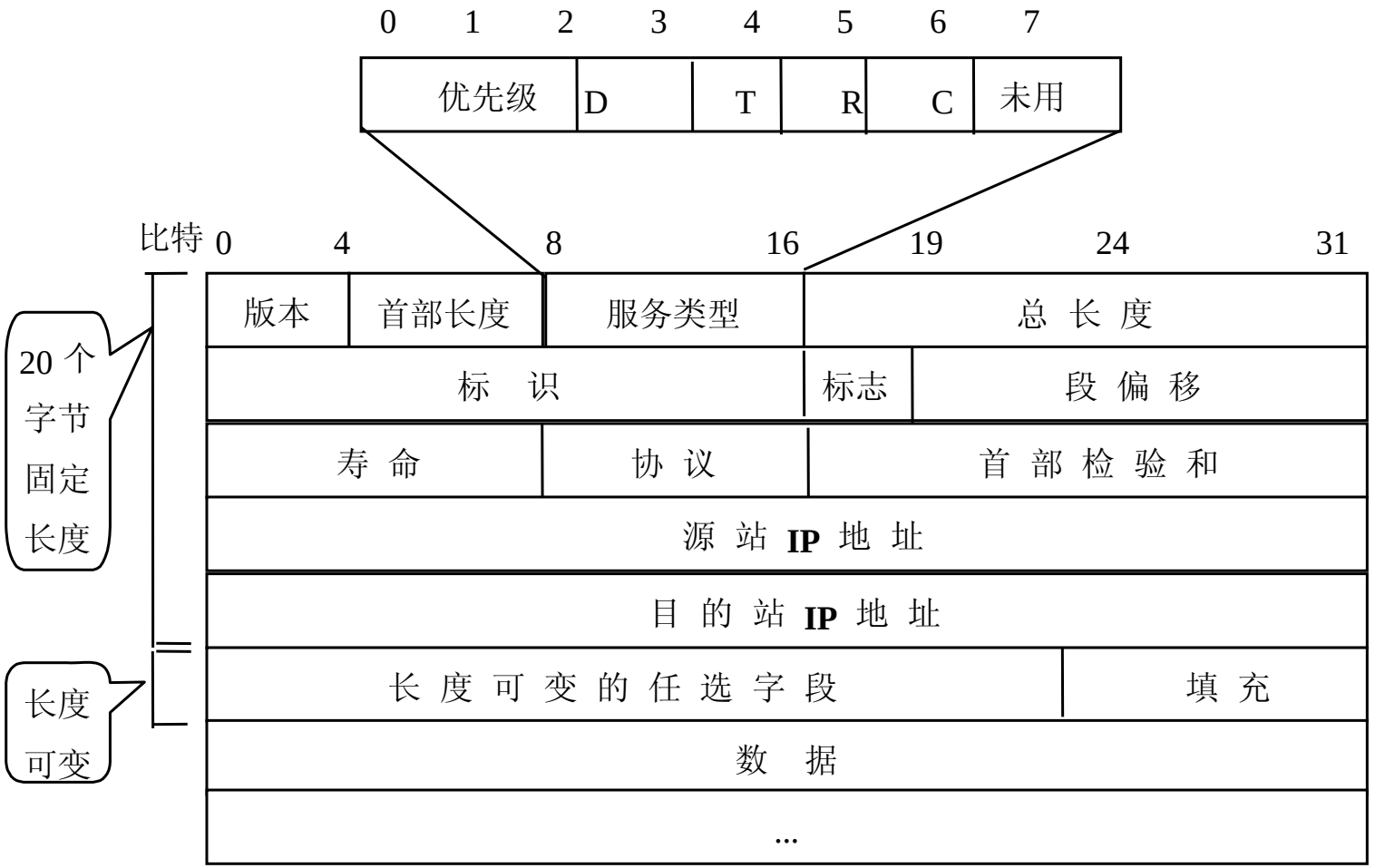



滑动窗口机制通过动态调整窗口大小来实现流量控制

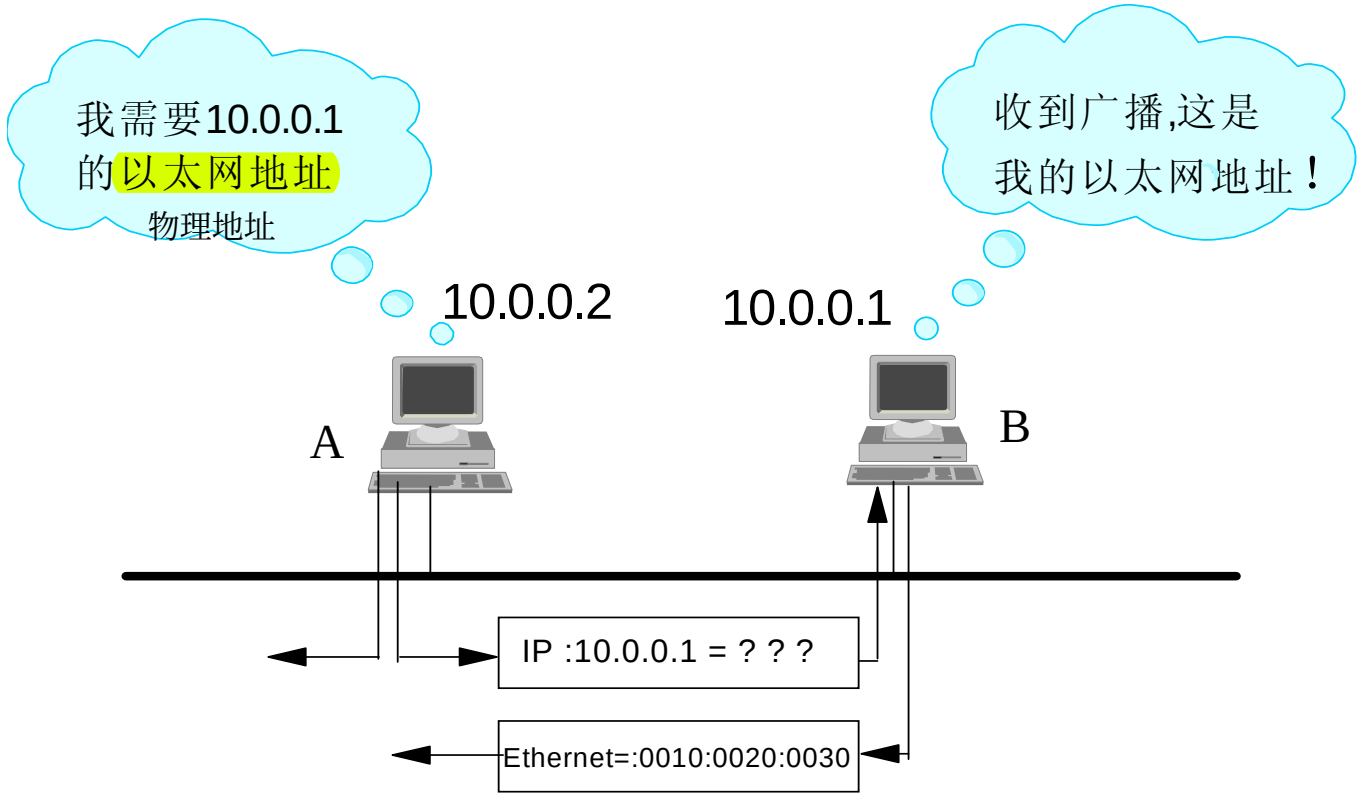
# 网络层协议概述


应用层
传输层
网络层
网络接入层
IP
ARP
RARP
ICMP
在OSI模型中ARP协议属于链路层；
而在TCP/IP模型中，ARP协议属于网络层

# IP协议

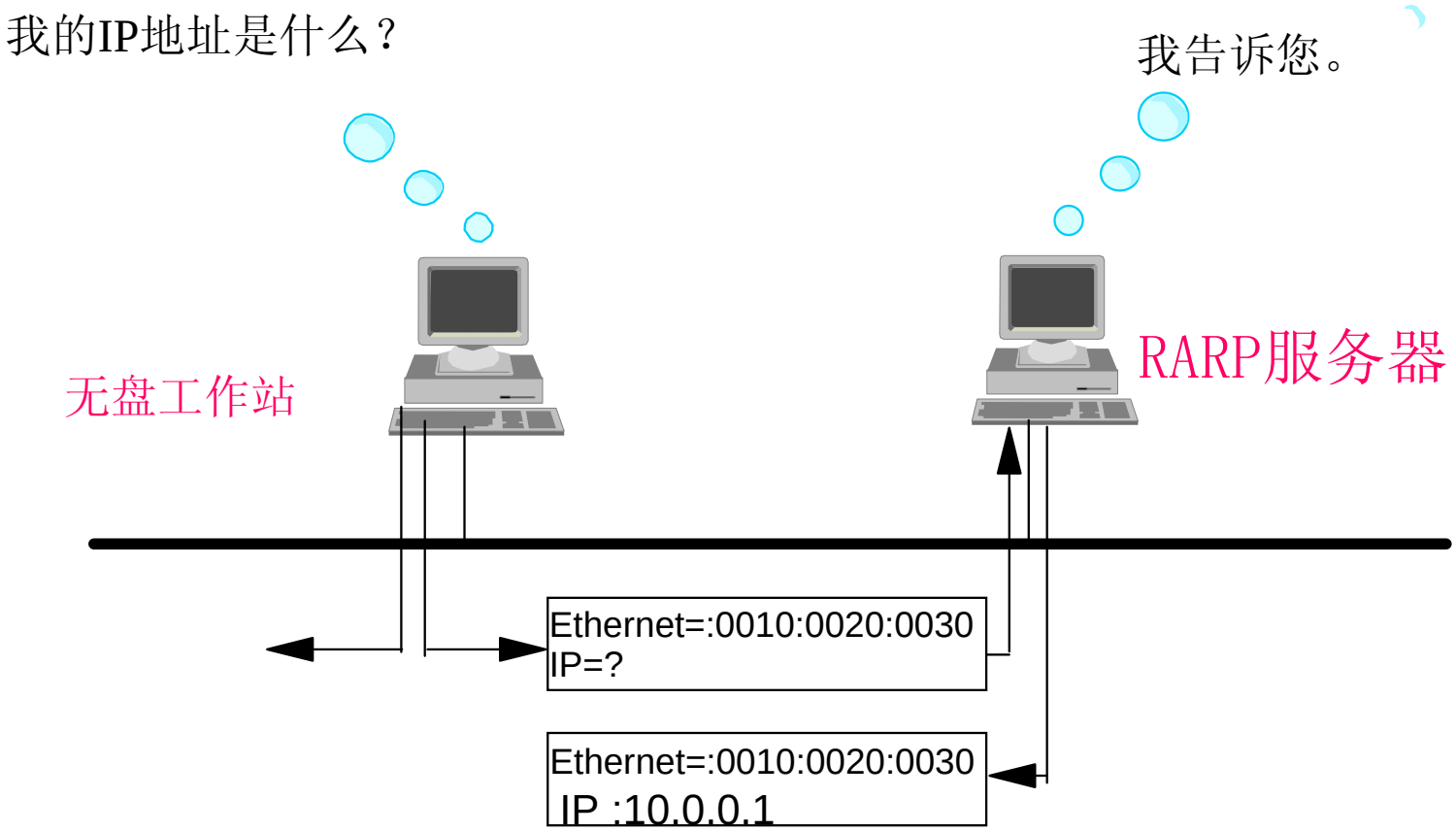


# ARP—地址解析协议

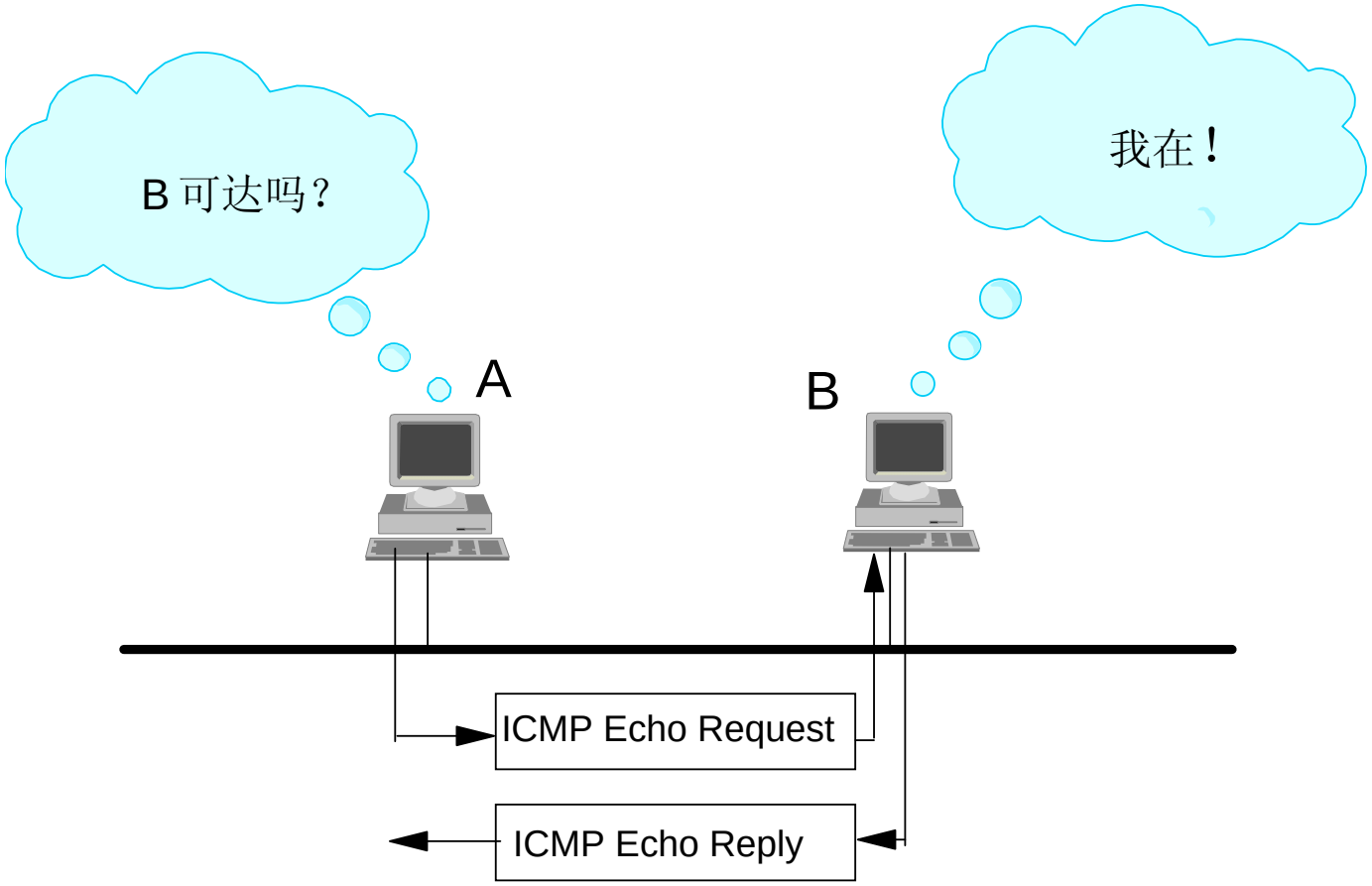



- 映射IP地址到MAC地址
- 本地ARP： ARP高速缓存

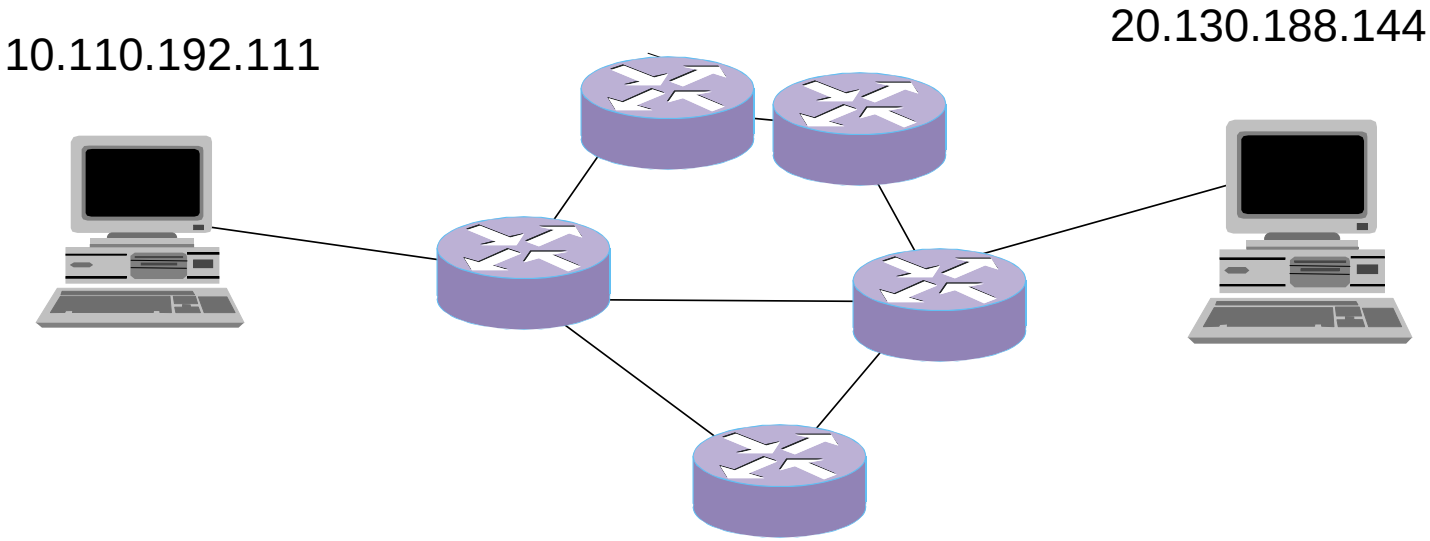
# RARP—反向地址解析协议



# ICMP协议



# IP地址介绍




- IP地址唯一地标示一台网络设备；
- 私有IP地址

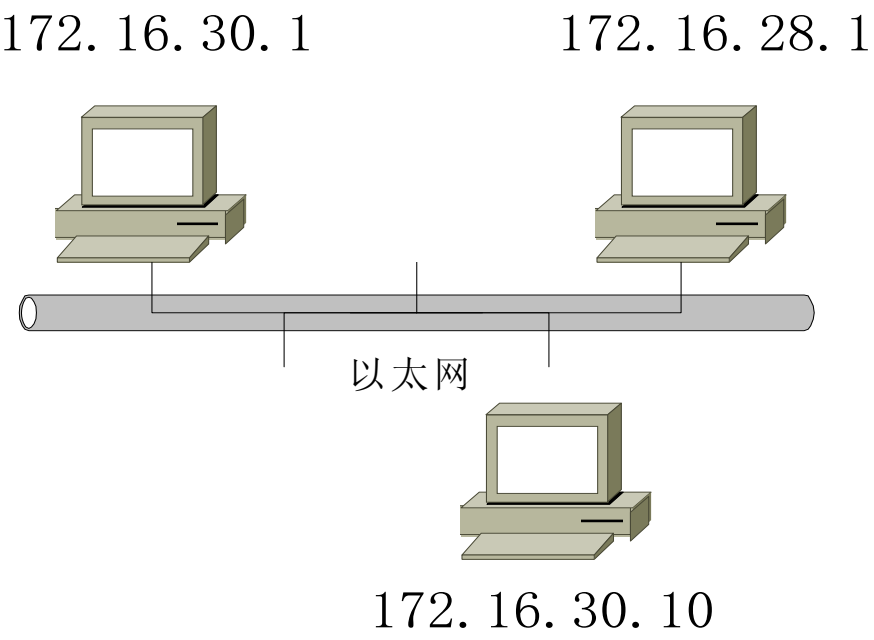
# IP地址类型

# 特殊IP地址

| 网络部分 | 主机部分 | 地址类型 | 用 途 |
| --- | --- | --- | --- |
| Any | 全“0” | 网络地址 | 代表一个网段 |
| Any | 全“1” | 广播地址 | 特定网段的所有节点 |
| 127 | any | 回环地址 | 回环测试 |
| 全“0” | | 所有网络 | 华为Quidway路由器<br>用于指定默认路由 |
| 全“1” | | 广播地址 | 本网段所有节点 |

# 无子网编址

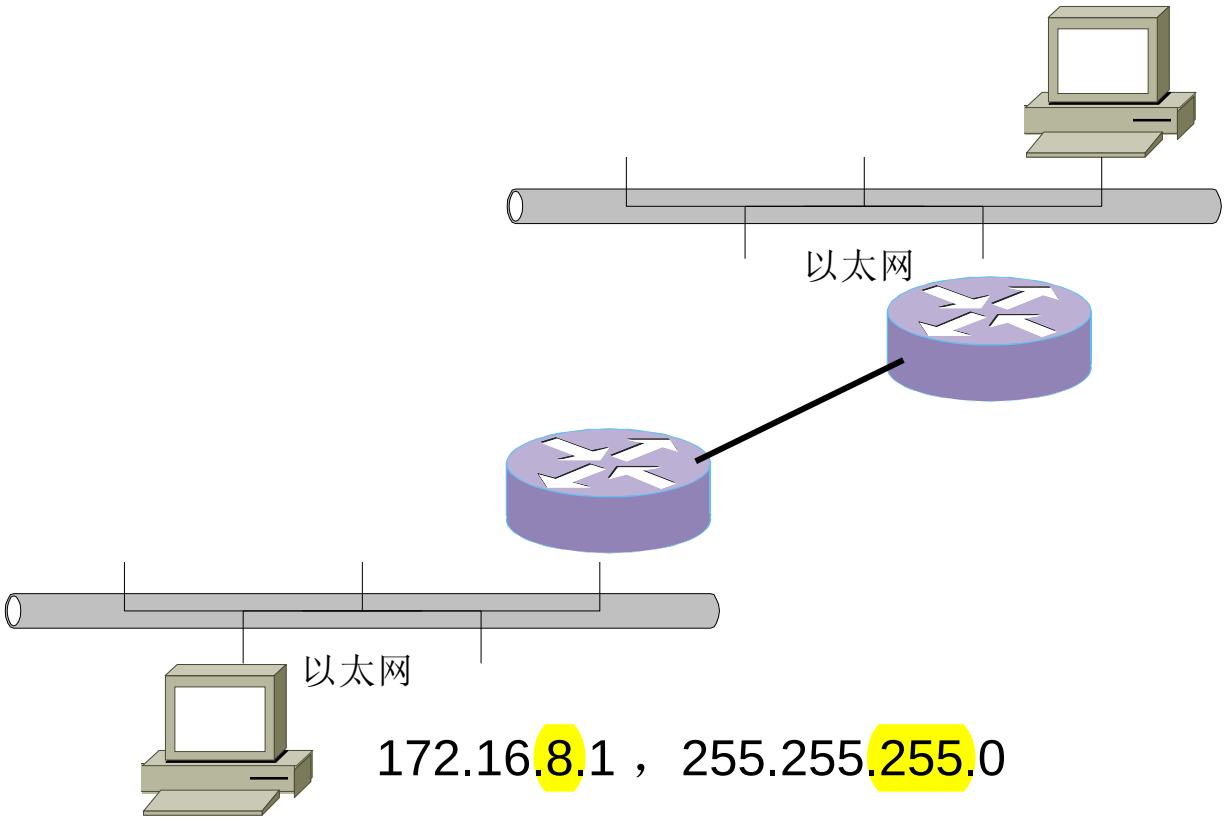
无子网编址是指使用自然掩码，不对网段进行细分。比如：**B类网段172.16.0.0，采用255.255.0.0**作为掩码。



# 带子网编址

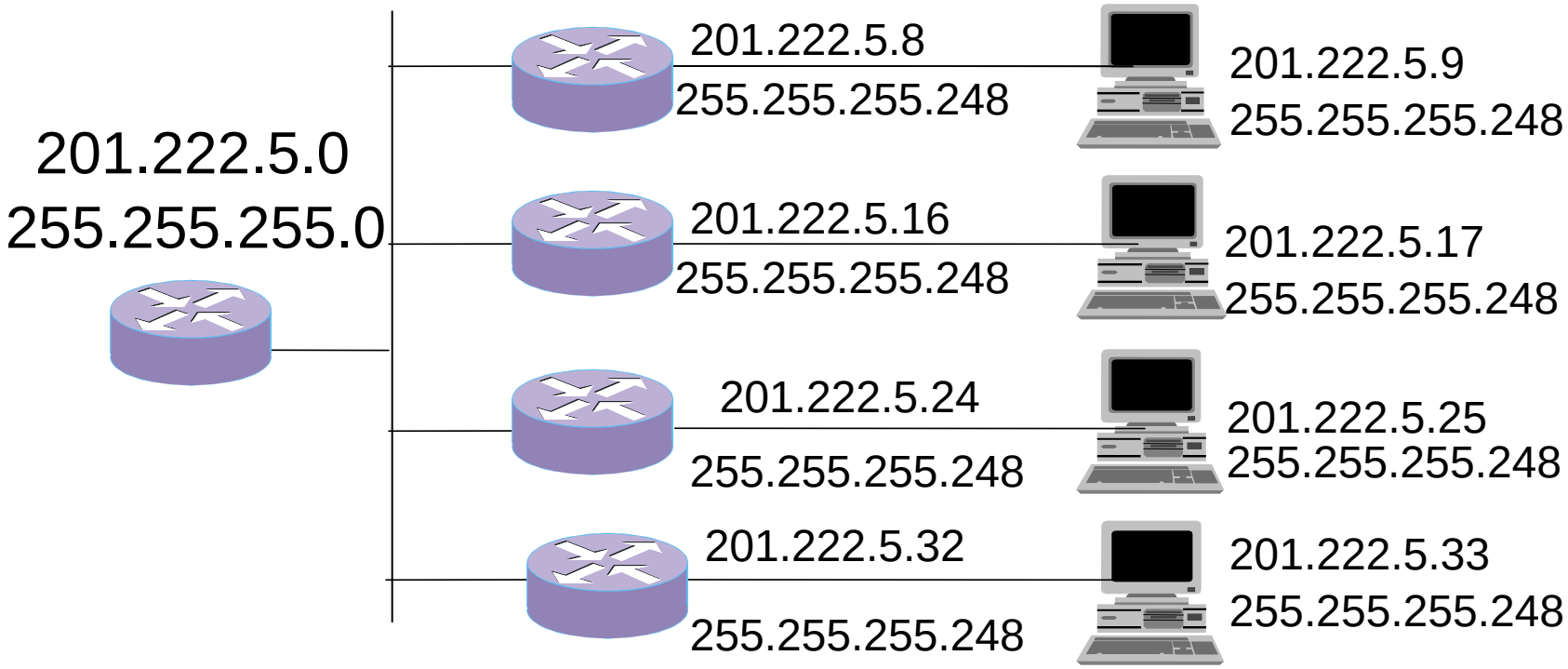
B类网段172.16.0.0

172.16.4.1，255.255.255.0




172.16.8.1 ， 255.255.255.0

# 子网规划



# B类子网规划实例

| | |
|---|---|
| 子网地址 | 172.16.2.0 |
| 主机地址 | 172.16.2.1-172.16.2.254 |
| 广播地址 | 172.16.2.255 |

| | |
|---|---|
| IP主机地址 | 172.16.2.120 |
| 子网掩码 | 255.255.255.0 |

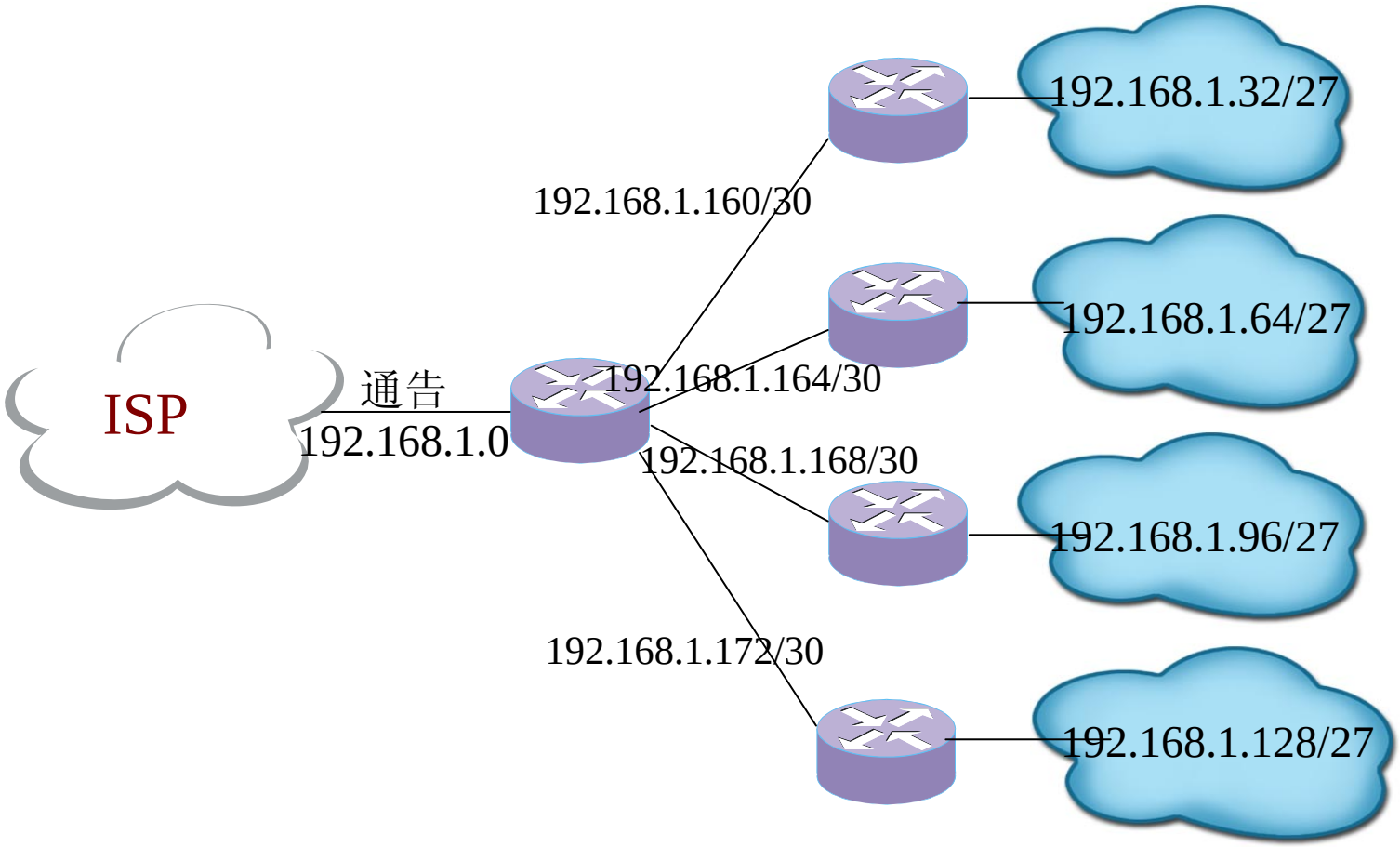
# C类子网规划实例

| | |
|---|---|
| 子网地址 | 192.168.5.120 |
| 主机地址 | 192.168.5.121-192.168.5.126 |
| 广播地址 | 192.168.5.127 |

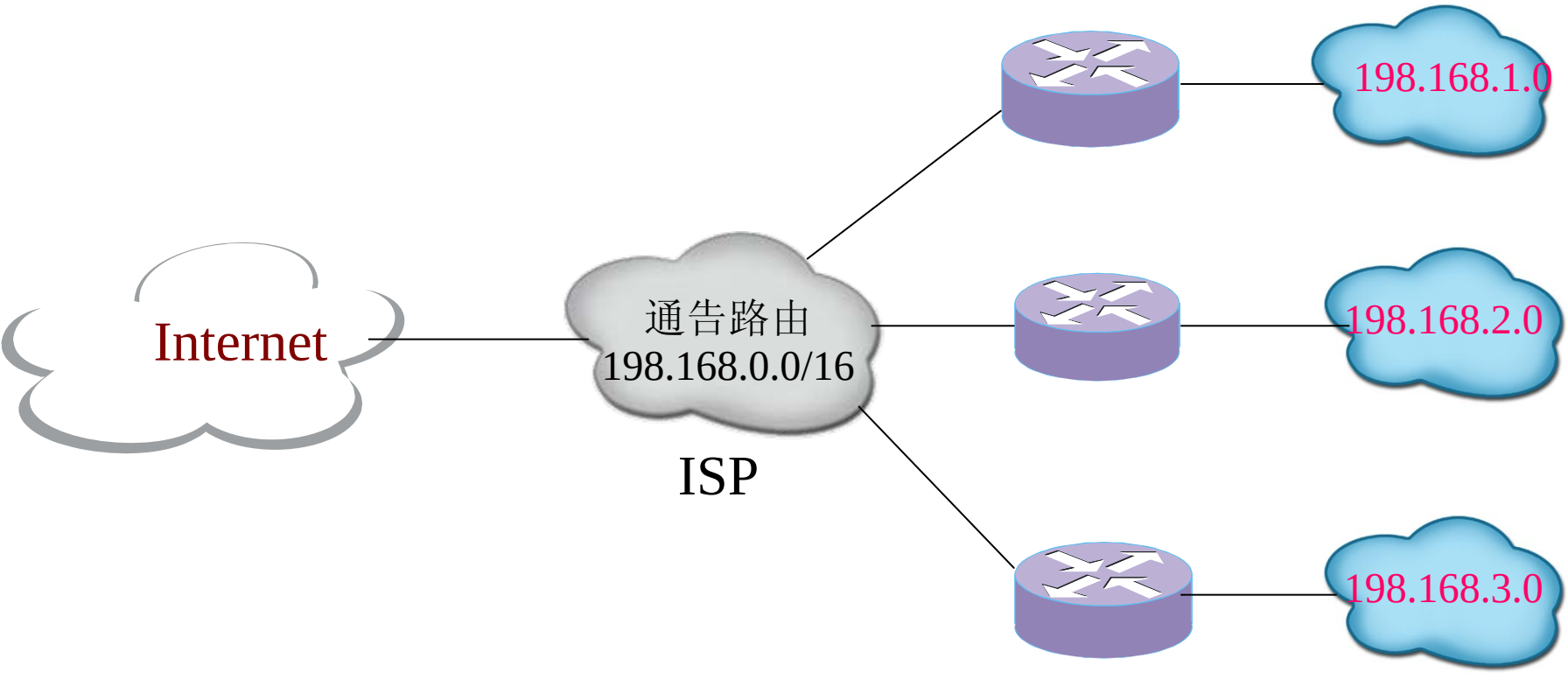
| | |
|---|---|
| IP主机地址 | 192.168.5.121 |
| 子网掩码 | 255.255.255.248 |

| 子网位数 | 子网掩玛 | 子网数 | 每一子网主机数 |
|---|---|---|---|
| 2 | 255.255.255.192 | 2 | 62 |
| 3 | 255.255.255.224 | 6 | 30 |
| 4 | 255.255.255.240 | 14 | 14 |
| 5 | 255.255.255.248 | 30 | 6 |
| 6 | 255.255.255.252 | 62 | 2 |

# 变长子网掩码（VLSM)


ISP
通告
192.168.1.0
192.168.1.160/30
192.168.1.164/30
192.168.1.168/30
192.168.1.172/30
192.168.1.32/27
192.168.1.64/27
192.168.1.96/27
192.168.1.128/27

# 无类域间路由（CIDR)



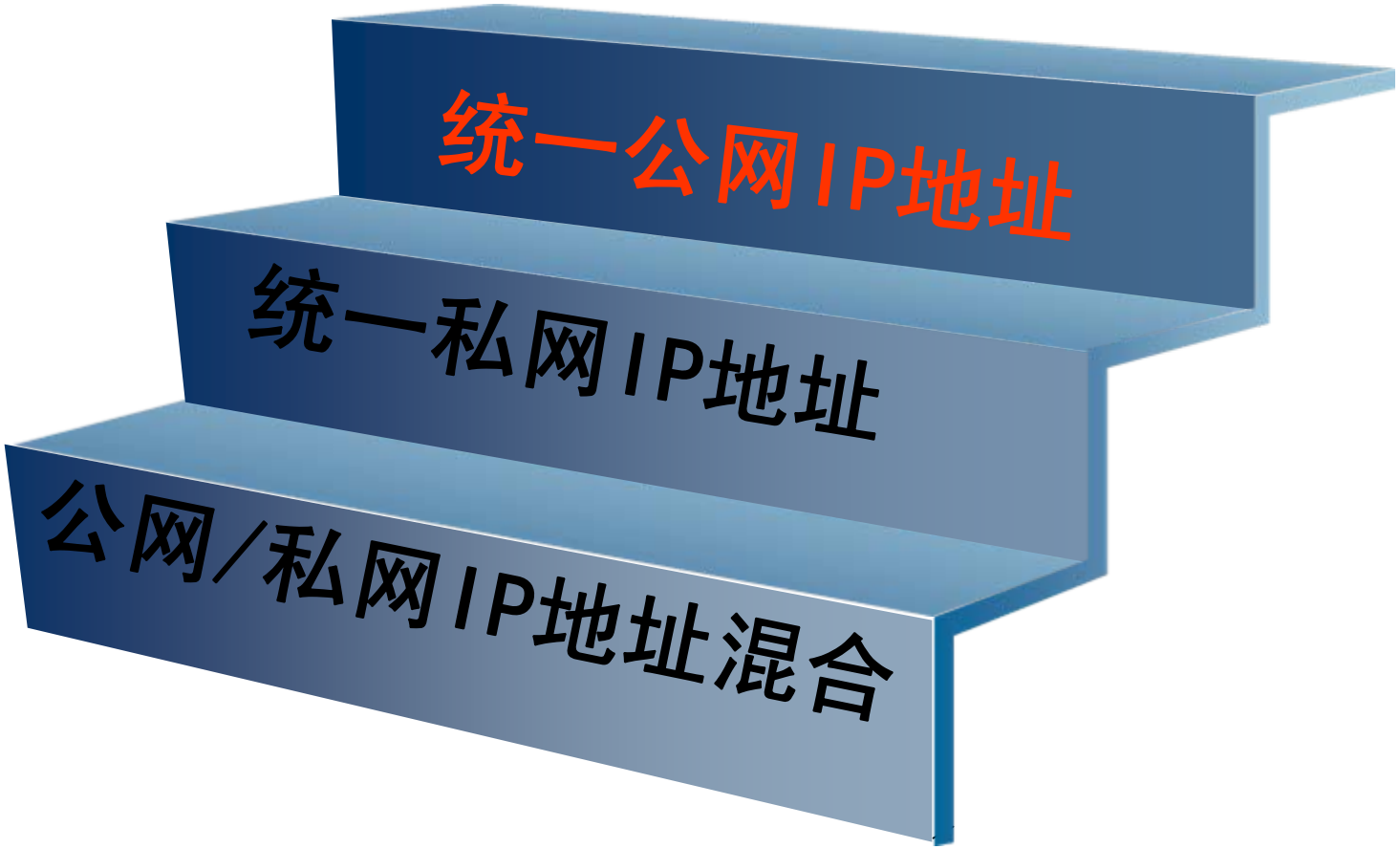

CIDR减少了路由表的规模，增大了网络的可扩展性

HUAWEI

# 基本概念小结

- TCP/IP协议栈与OSI参考模型比较
- TCP/IP协议栈各层主要协议介绍
- IP子网规划原理
- IP子网规划实例

# 城域网IP地址规划



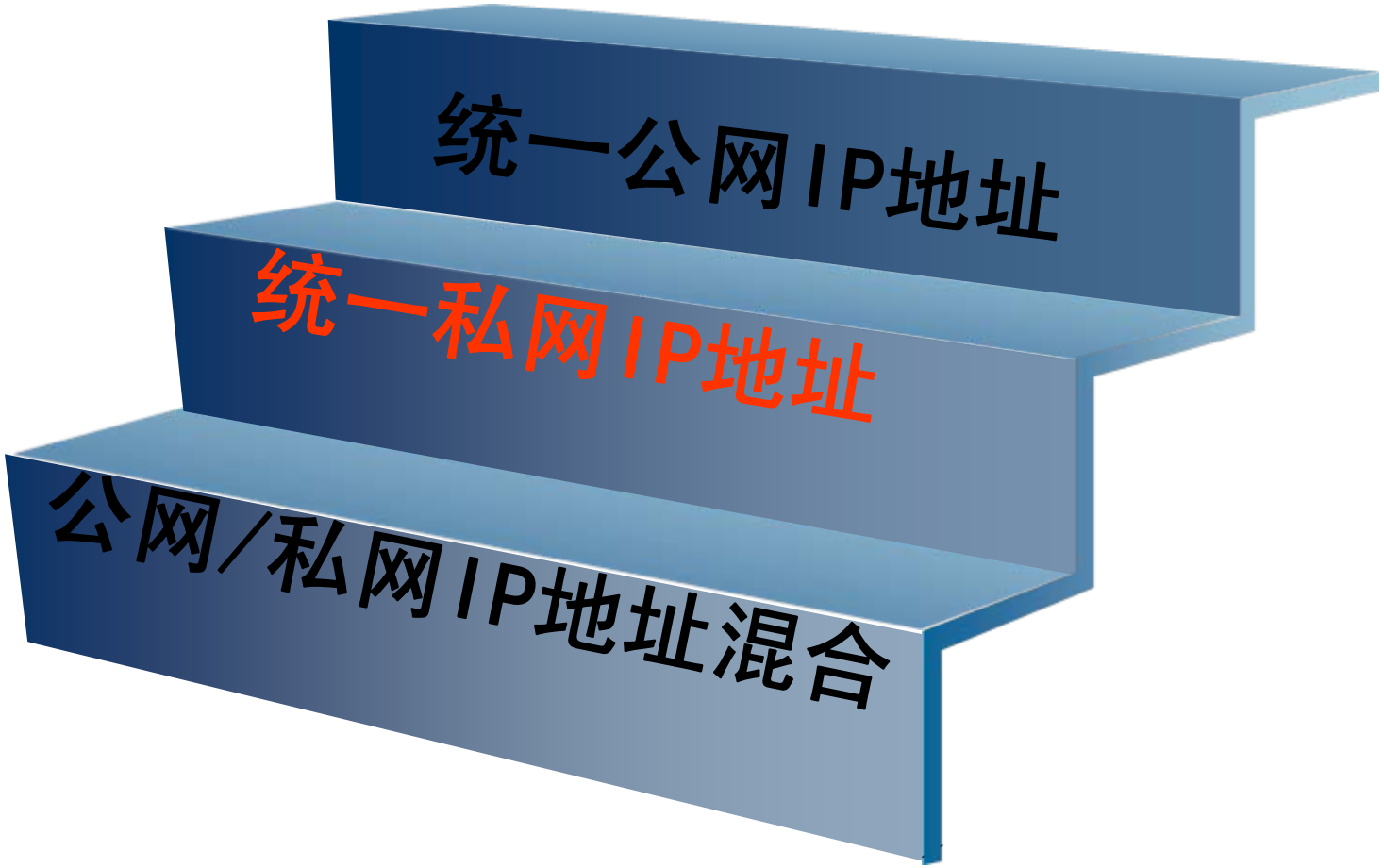
# 统一公网IP地址

统一公网**IP**地址是一种最理想模式，存在问题：

1. 需要大量公网**IP**地址
2. 公网**IP**地址资源利用率低

目前不可能采用这种模式，有待**IPV6**的应用解决。

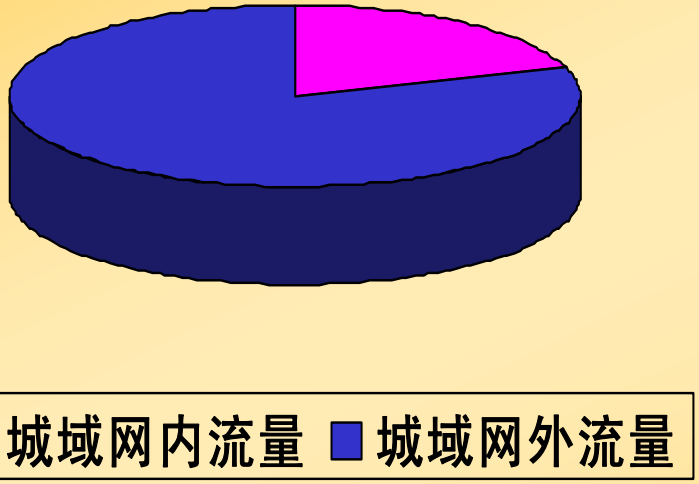
# 城域网IP地址规划



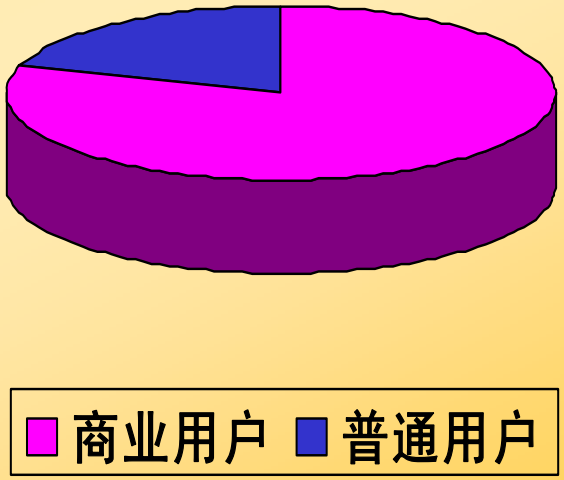
# 城域网流量特性

城域网内80%的流量在城域网内；
商业用户占流向城域网外流量的80%.

城域网流量统计




流向城域网外流量统计




解决好城域网内部流量和大客户的流量可以大大提高网络的效率

# 统一私网IP地址规划原则

1. 唯一性

网络地址保持唯一性。

2. 简单性

地址分配简单易管理，避免在主干上采用复杂的掩码方式。

3. 连续性

为同一网络区域分配连续的网络地址，便于缩减路由表的表项，提高路由器的处理效率。

4. 可扩充性

为同一网络区域分陪的网络地址预留一定容量的IP地址，便于以后扩容后仍然保持地址的连续性。

5. 灵活性

IP地址的规划考虑不同的宽带接入方式以及路由协议。

# 统一私网IP地址规划

1. 公用私网地址

   10.0.0.0 —— 10.255.255.255（一个A类地址16581375）

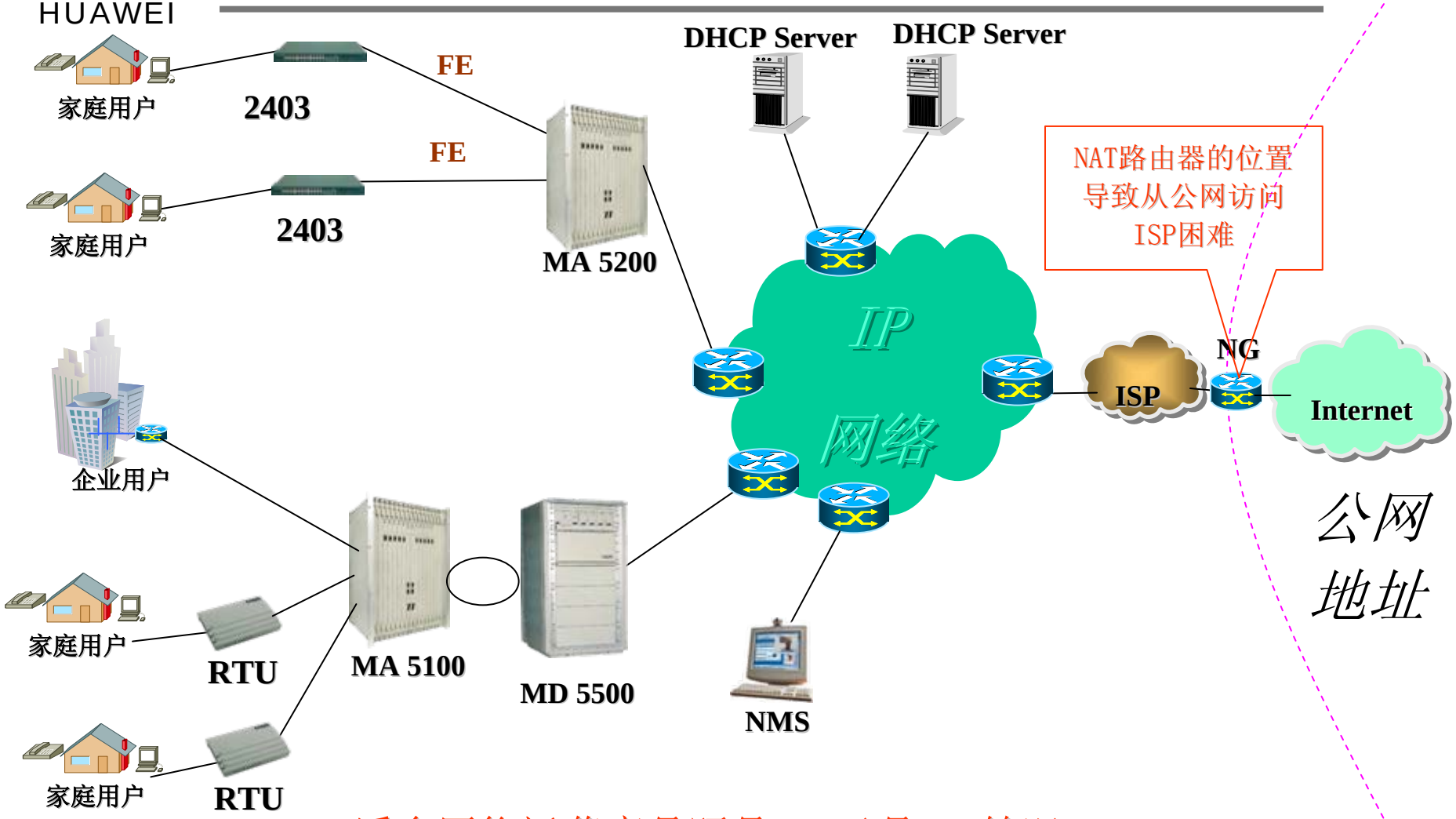
   172.16.0.0 —— 172.31.255.255（15个B类地址975375）

   192.168.0.0 —— 192.168.255.255（1个B类地址65025）

2. 建议城域网内采用上面三个段公用私网地址，有利于NG（NAT关口局）地址转换

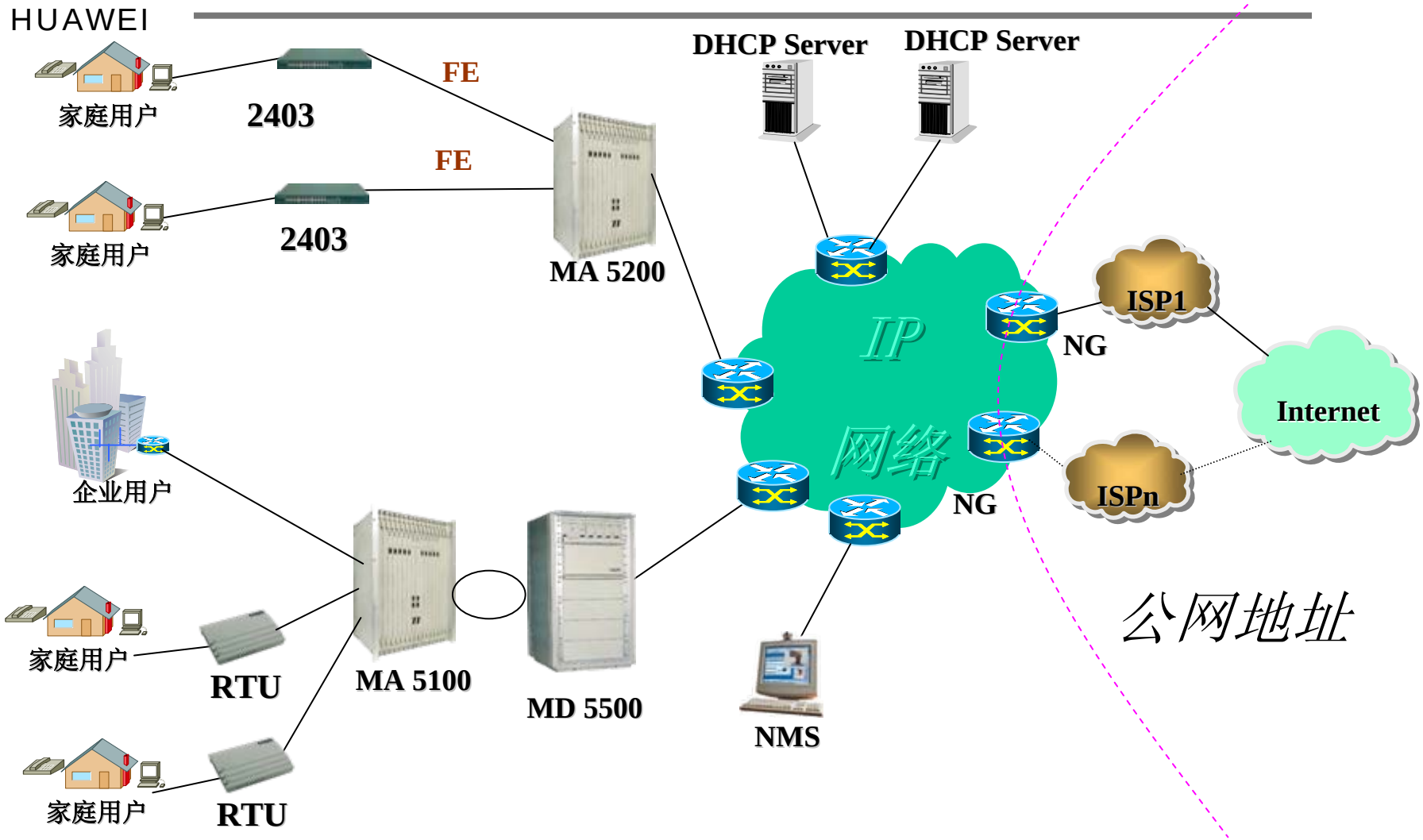
3. 公用私网地址数量：17621775个

# 统一私网IP地址示意图（一）




*适合网络运营商是既是NSP又是ISP情况*

# 统一私网IP地址示意图（二）



# 统一私网IP地址分类（PPPOE/WEB）

1. **用户IP地址**

驻地网中有效的、分配给本地主机的IP地址——IP地址容量最大的部分，要结合各局实际情况进行实际规划。

2. **网络IP地址**

骨干网中设备及外设使用的IP地址——网络中的公共资源地址

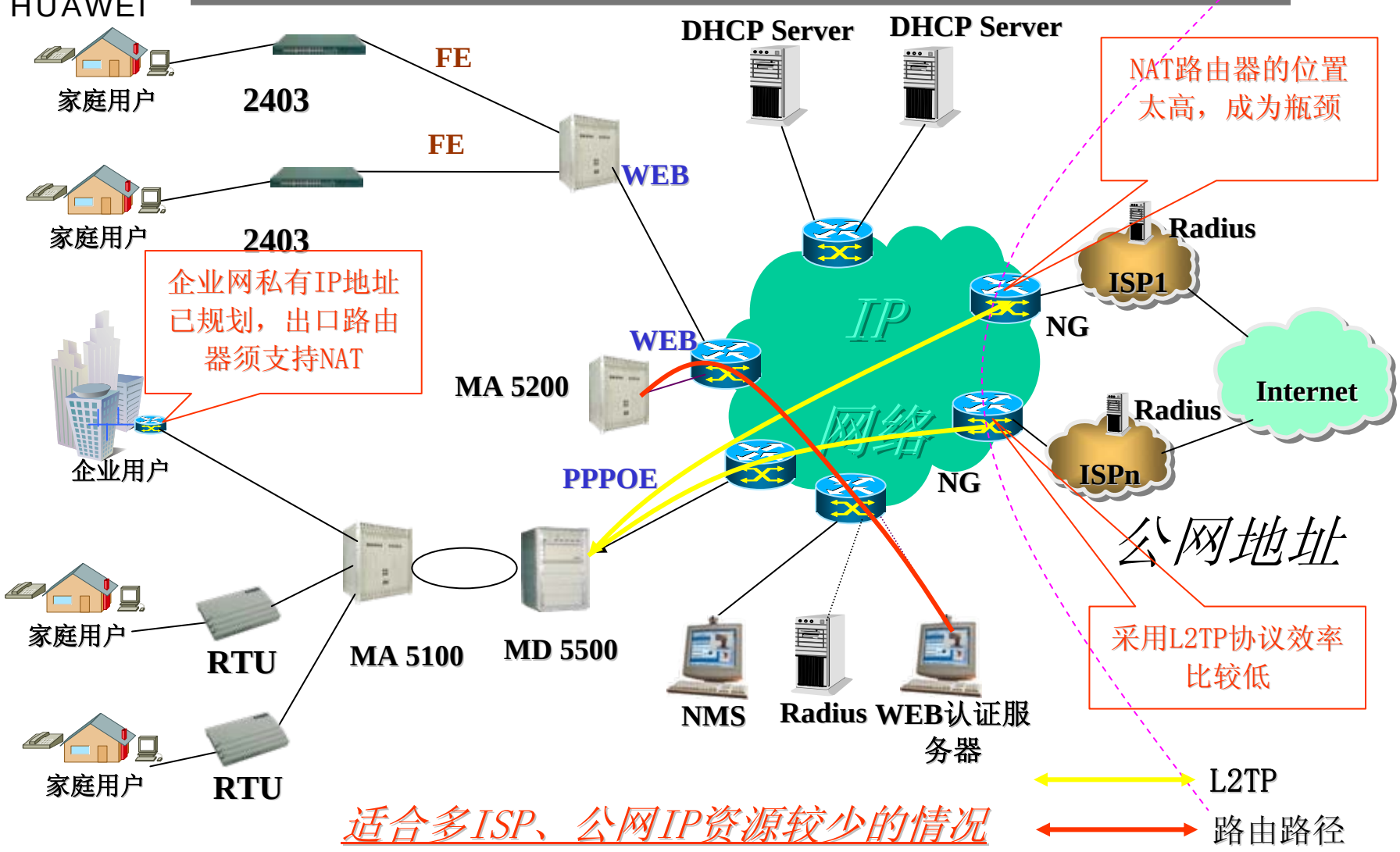
3. **管理IP地址**

设备管理使用的IP地址——保证设备网管的安全性

4. **上网IP地址**

各ISP分配地址处于不同段——采用源地址路由或L2TP协议到达多ISP

# 统一私网IP地址示意图（PPPOE/WEB）



# 统一私网IP地址优势

1. 容易进行地址规划，便于管理；
2. 同一网络区域内地址连续，提高了路由器的处理效率；
3. 采用NG能充分利用公网IP地址资源；
4. 城域网内部业务不受NAT功能影响。

# 统一私网IP地址弱势

1. NAT路由器的位置太高，成为瓶颈（主要流量来自于企业等大客户）；
2. 企业网/校园网私有IP地址无法与整个城域网共同规划，地址经过两次NAT才能进Internet；
3. NG会屏蔽一些已有业务（公网），需要进行会话层解析，但会导致NG性能下降
4. 采用远程网管方式必须进行会话层解析

# NAT的分类

1. 传统NAT包括单向NAT、双向NAT和二次NAT
2. 单向NAT主要解决私有网络访问Internet，只允许出境会话
3. 双向NAT允许入境会话，但仍然不允许地址会话两端的网络地址重叠。双向NAT通过DNS-ALG工作，要求域名规划不冲突。
4. 二次NAT对IP报进行源地址和目的地址两次转换，允许会话地址两端的地址重叠

# NAT影响的业务

由于报文中包含**IP**地址信息，**NAT**必须支持会话层

解析才能支持以下业务：

- FTP
- ICQ/QICQ
- VOIP
- SNMP
- DNS

✸✸

这些应用的特征包括：

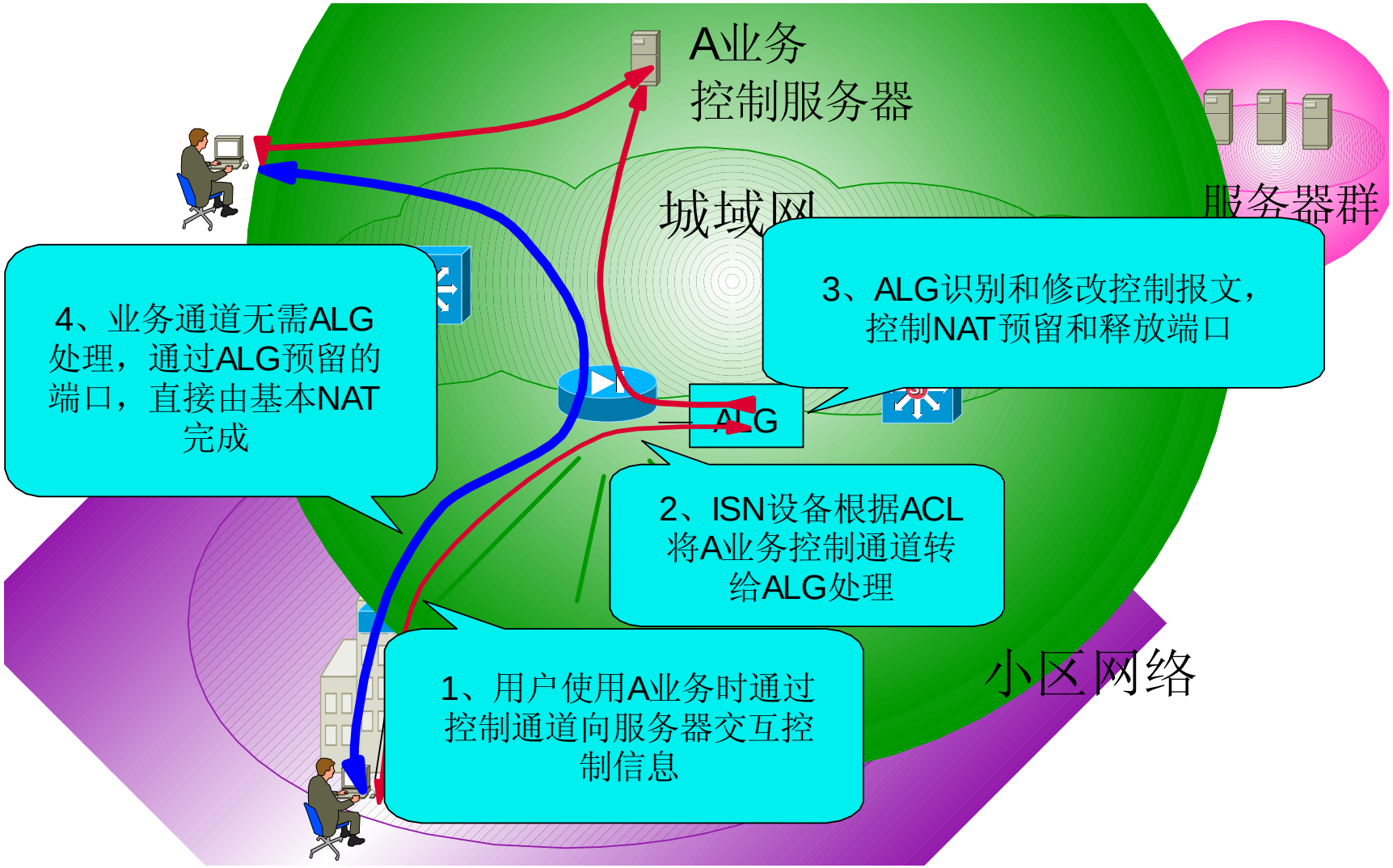
•需要直接的端到端的会话

•在应用层数据中传递了IP地址/端口号

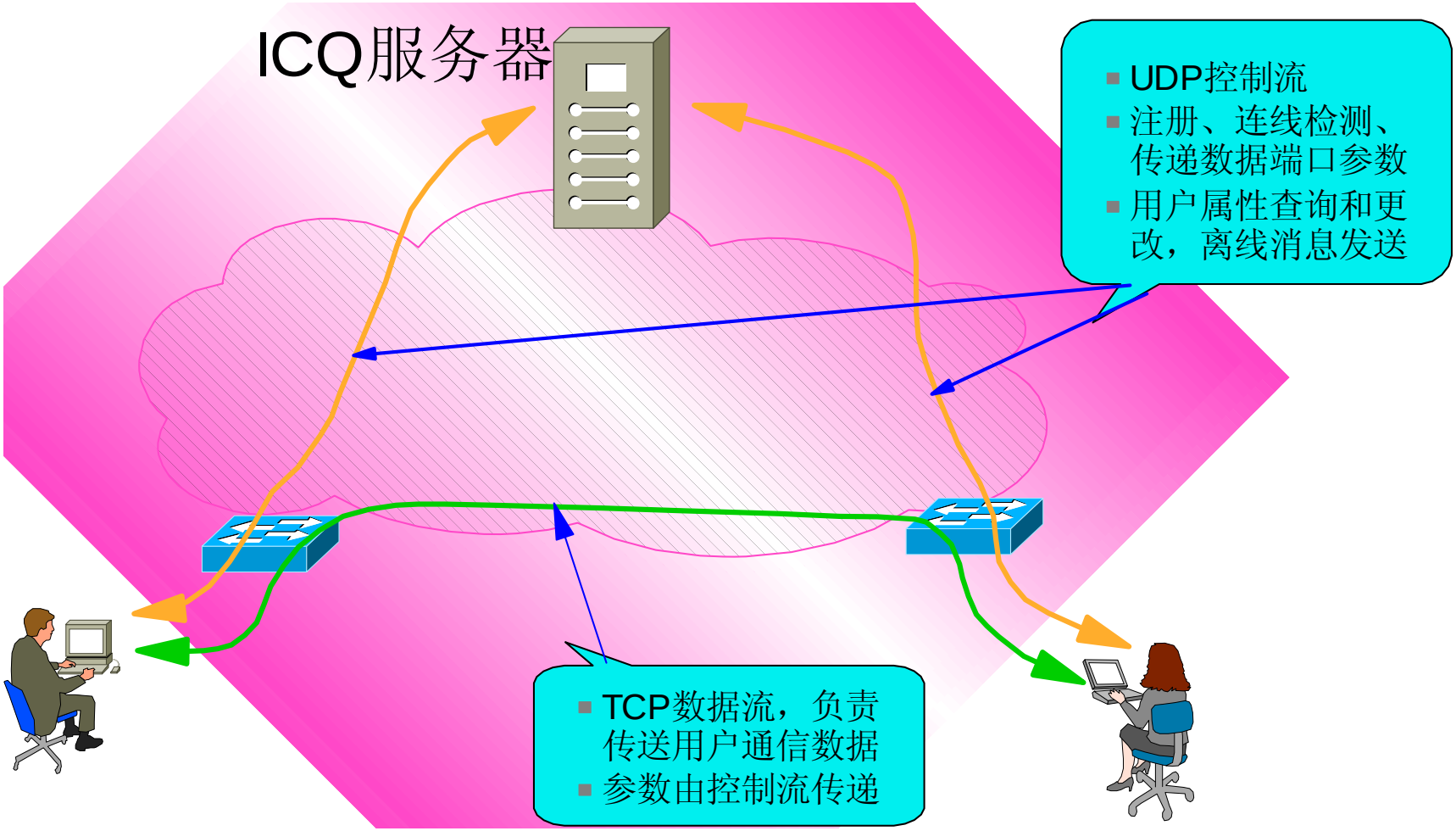
# ALG

- IETF在相关RFC中，针对这一问题提出了ALG的概念
- ALG基本实施策略
  - 截获应用控制报文
  - 根据报文语义，添加NAT端口绑定Cache表项，创建由外向内的“ 通道”
  - 更改控制报文，使之包含刚分配的合法地址/端口
- ALG实施可行性分析
  - 由于大部分应用随机产生的数据连接端口信息都由控制流携带，因此只需处理控制报文即可
  - 一般控制流量都不大，不会产生CPU流量过载问题
  - 对系统硬件没有影响。主要的复杂工作在于高层软件，需要对各种应用控制流进行识别

# NAT和ALG的配合


A业务
控制服务器
城域网
服务器群
ALG
4、业务通道无需ALG处理，通过ALG预留的端口，直接由基本NAT完成
3、ALG识别和修改控制报文，控制NAT预留和释放端口
2、ISN设备根据ACL将A业务控制通道转给ALG处理
1、用户使用A业务时通过控制通道向服务器交互控制信息
小区网络

# ICQ工作原理简介

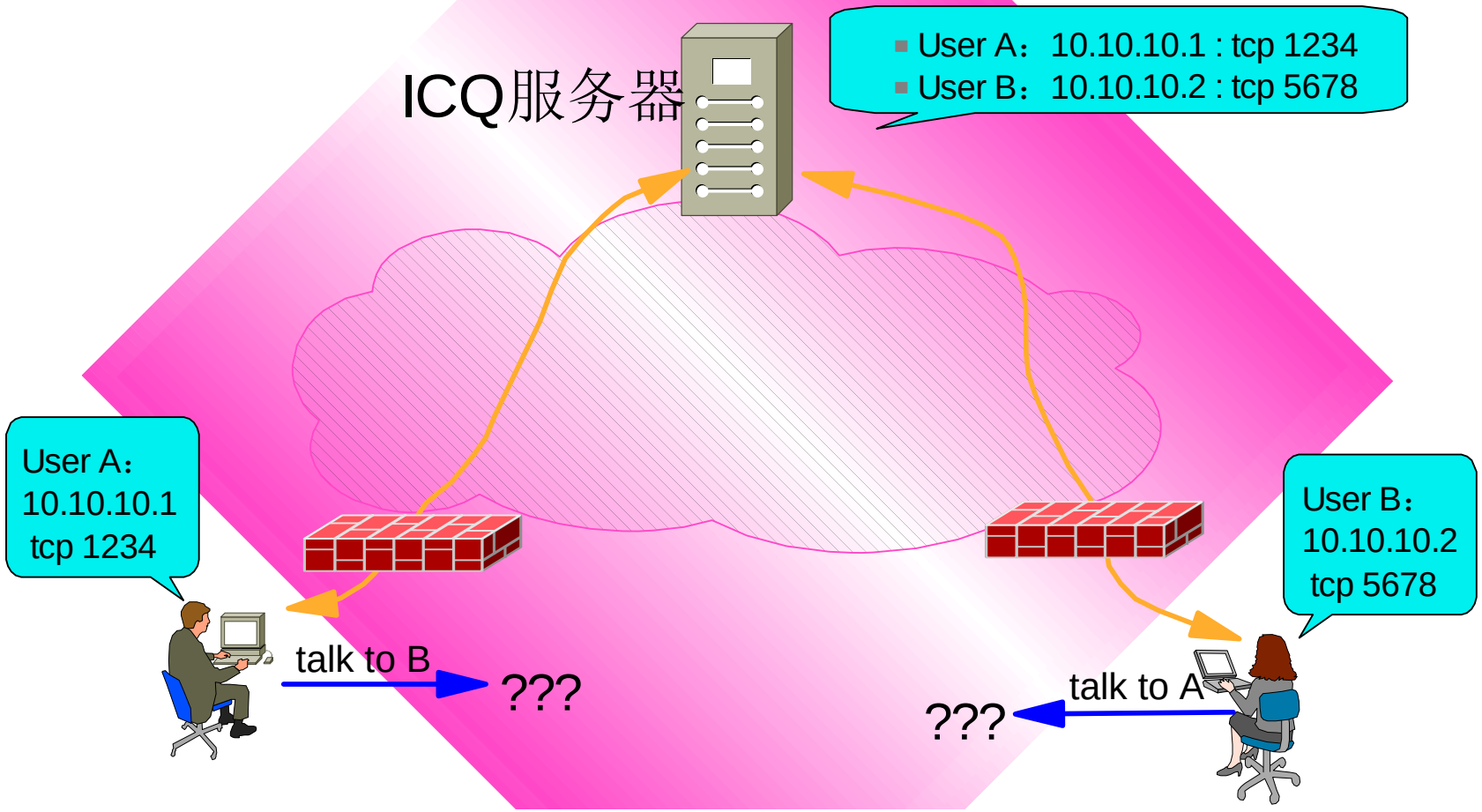

ICQ服务器
UDP控制流
注册、连线检测、传递数据端口参数
用户属性查询和更改，离线消息发送
TCP数据流，负责传送用户通信数据
参数由控制流传递

# ICQ工作原理(续)

- UDP控制报文
  - 报文重传确认间隔为10秒，告警前可重试6次
  - 2次告警即认为离线
- TCP数据联接建立方式
  - 联接可由任何一方发起，只要被动监听者能通过Internet直接访问到
  - TCP监听端口通过UDP控制报文向服务器注册，并通告给其它用户来发起连接

# ICQ穿越NAT的问题

双方在不同的NAT里面时，将会出现的问题：



# DNS

1. 普通DNS解析在应答报文中传递了IP地址，反向DNS解析在请求报文和应答报文中都包含IP地址
2. 对于传统的单向NAT，DNS不需ALG支持，因为外部地址在私有网络中也是唯一的
3. 对于双向NAT、二次NAT的情况都需要DNS-ALG支持

# FTP

1. FTP分为控制连接和数据连接，控制连接是永久的（直到用户关闭FTP），数据连接是临时的，在需要传输文件或ls结果时临时建立。数据连接所使用的端口号由控制连接协商得到。需要FTP-ALG才能解决地址转换问题（除非是数据连接都使用被动方式打开）
2. VRP已经能够提供FTP-ALG，主要是解决线速问题
3. FTP在Internet中的流量很小，且对QoS无要求。在要求不严格的情况下可以用软件实现

# VoIP

H.323、MGCP和H.248都需要在控制连接中协商RTP所使用的端口号，所以NAT需要解析内容，即，需要VoIP-ALG

VoIP是双向会话，所以需要双向NAT。但VoIP不使用DNS协议，只能通过GK和NAT设备的配合来解决

- 对于控制连接，通过在GK和NAT上共同配置端口号来识别被叫网关/话机（位于私有网络中）
- 同时，NAT（VoIP-ALG）解析控制连接的内容，动态建立NAT地址匹配表，以允许入呼叫

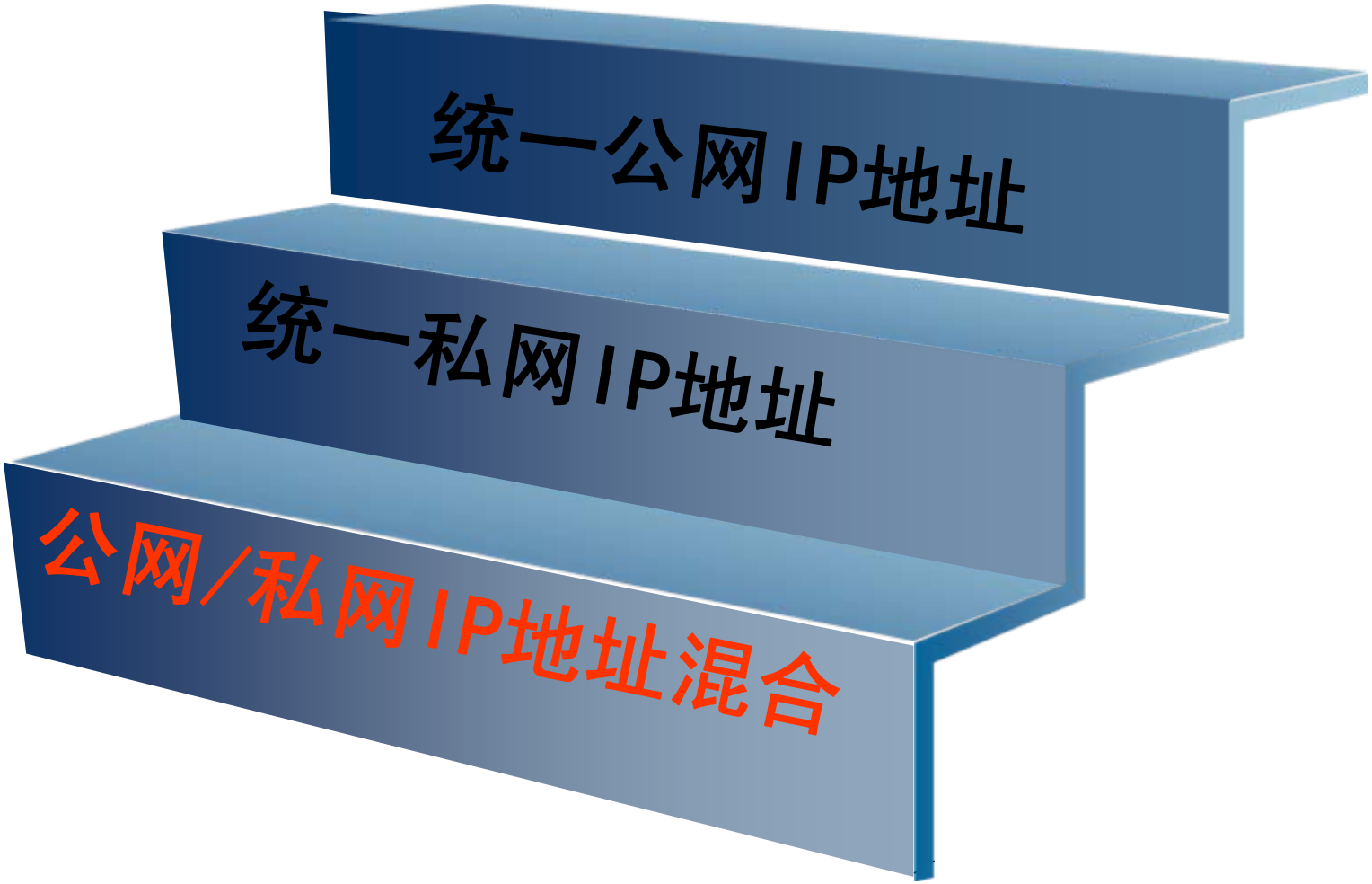
# SNMP

- SNMP报文中也包括IP地址信息，也需要SNMP-ALG或SNMP-Proxy
- 如果长城宽带等希望统一管理分布于各地的本地业务网，就需要对多地址域进行支持；如果省网使用私有地址，同时又希望全国有一个统一的网管中心，则中国电信等大运营商（运营商的运营商）也需要SNMP的多地址域解决方案
- 多地址域的SNMP方案有三种
  - 基本SNMP-ALG
    - 只对报文中类型为IP地址的对象进行转换
    - 优点是ALG无需识别MIB库，实现简单，运算复杂度低
    - 缺点是对很多由IP地址衍生的对象（如IP地址作为索引）无法转换
  - 高级SNMP-ALG
    - 需要编译、加载MIB库，通过识别对象标识（OID）来识别转换对象
    - 优点是可对IP地址衍生的对象进行转换
    - 缺点是需要加载MIB库，会引起报文长度变化，实现难度高，计算复杂度高，会引起表形对象的字典顺序混乱
  - SNMP-Proxy
    - 不对报文内容进行转换
    - 对设备和网管站不透明，设备和网管站需要知道Proxy的存在
    - 网管站需要支持地址冲突
  - 使用SNMPV3时三种方式都需要集中维护安全参数（密钥等），增加了不安全因素

# SOCK5协议

1. SOCK5的基本思想是客户端操纵Proxy，在Proxy上开一个“代理socket”。SOCK5支持connect、bind、UDP associate三种远程socket调用，所以客户端不但可以通过Proxy“说”，还可以通过Proxy“听”
2. SOCK5是一个对等协议，不但要求应用程序知道Proxy的存在（不透明），还要求应用程序识别并使用SOCK5
3. SOCK5全程工作在应用层，不同于NAT ALG的Cut-through方式，效率非常低（虽然不需要对应用数据进行转换），并且对用户不透明，运营商使用时会比较困难，ePhone等终端也很难支持

# 城域网IP地址规划

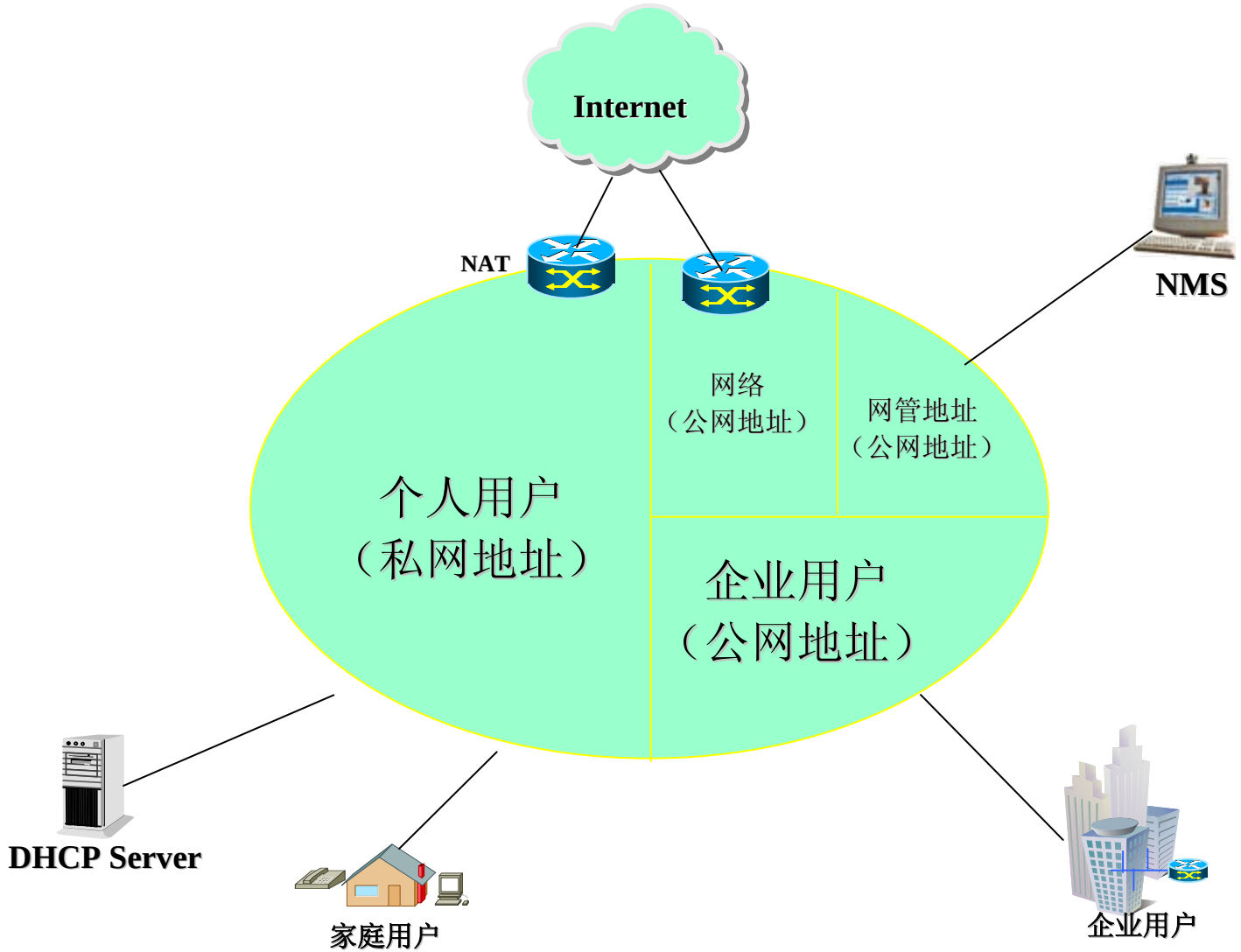


# 公网/私网IP地址规划原则

## 城域网中使用公网IP地址、私网IP地址的原则：

1. 根据数量与流量的关系：
   - 数量小但数据量大——采用公网IP地址极大减少NAT的工作量：骨干网络、内容网络、企业用户等
   - 数量大但数据量小——采用私网IP地址充分利用公网IP地址资源：散户、小区用户等
2. 根据方便规划的程度：
   - 容易规划——散户、小区用户本身无地址规划，可由运营商统一规划
   - 难于规划——企业/学校用户大部分已经使用私有网络地址规划，使用公有地址解决企业上网问题既可以避免用户重新规划地址
3. 根据流量灵活部署NAT，网关的位置越高，公网IP地址的利用率就越高，但同时对网关的容量和速率要求就越高

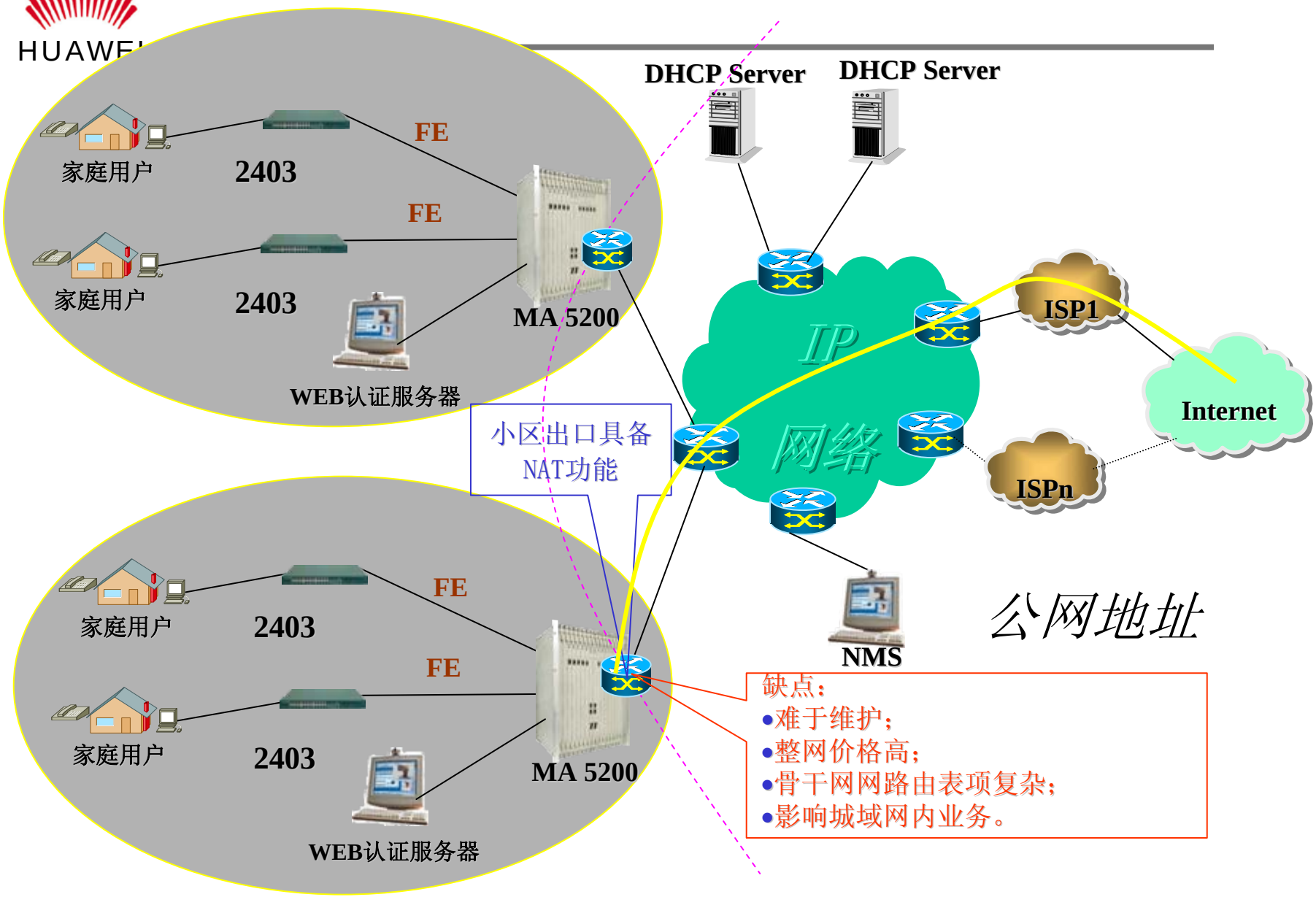
# 公网/私网IP地址混合示意图



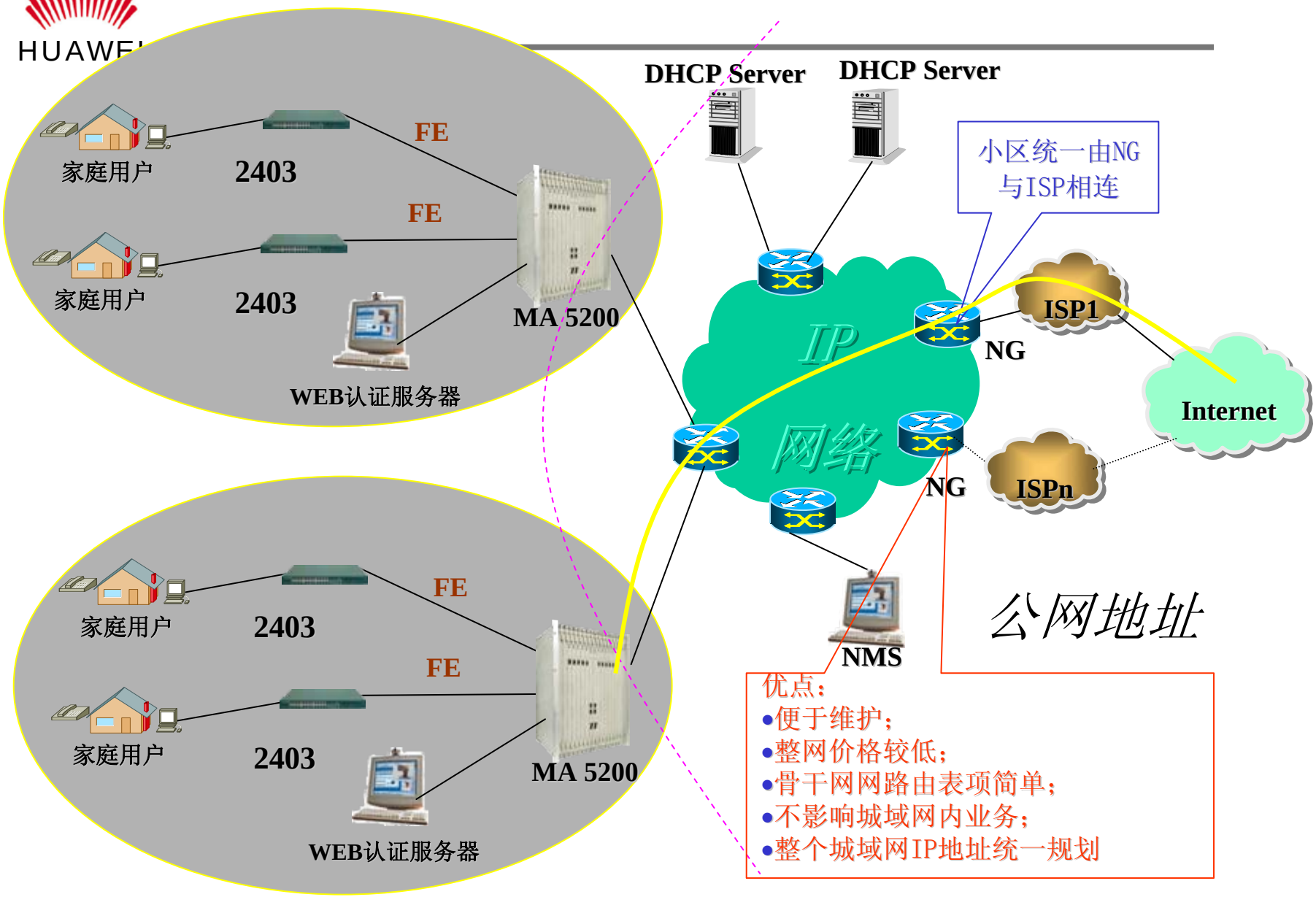
# 公网/私网IP地址类型

1. **私网IP地址类型：**
   - 用户IP地址：驻地网中有效的、分配给本地主机的IP地址
2. **公网网IP地址类型：**
   - 用户IP地址：驻地网转换的公网IP地址、PPPOE分配的公网IP地址、企业用公网IP地址
   - 网络IP地址
   - 管理IP地址

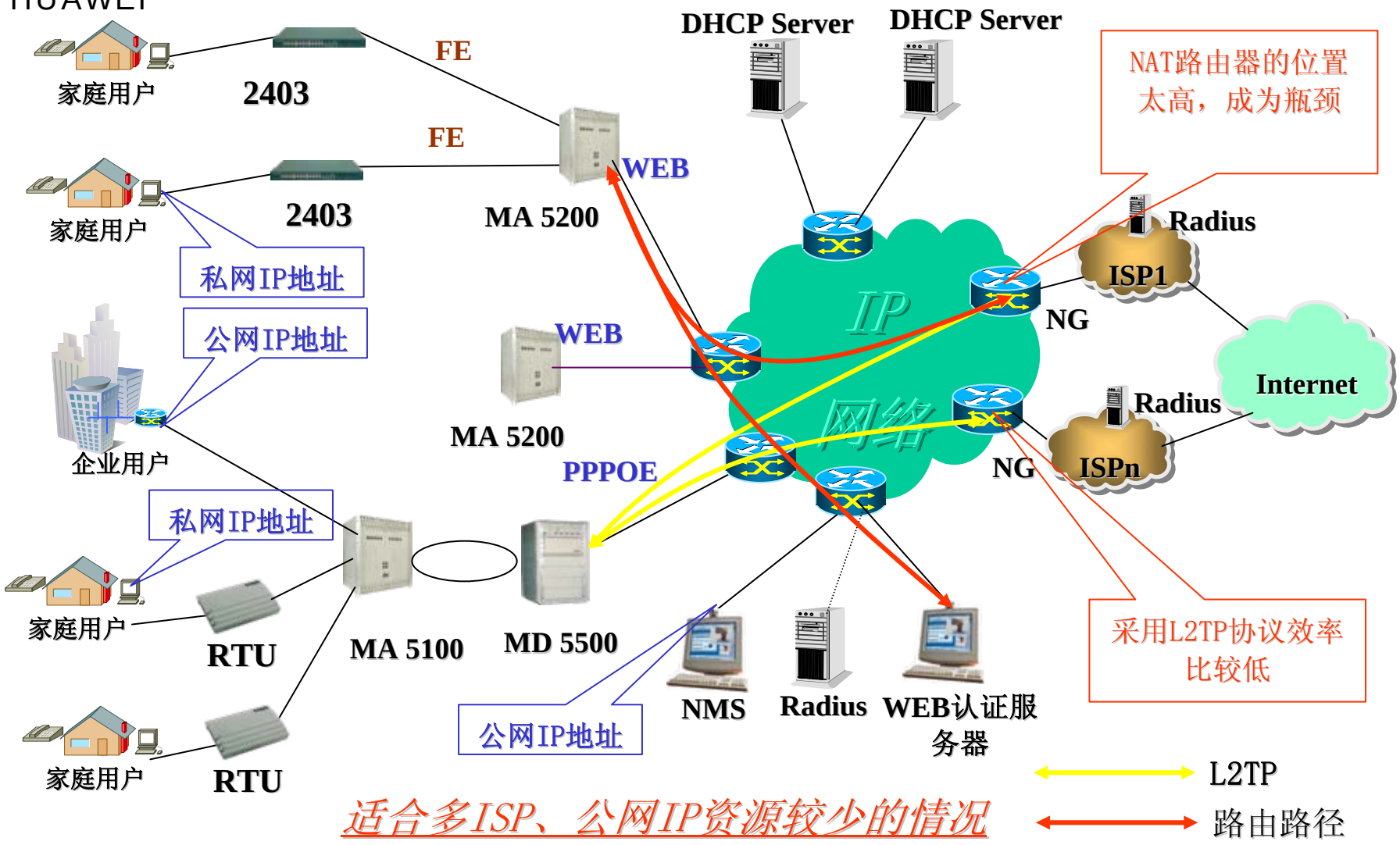
# 公网/私网IP地址混合（小区）



# 公网/私网IP地址混合（小区）



# 公网/私网IP地址混合（PPPOE/WEB）



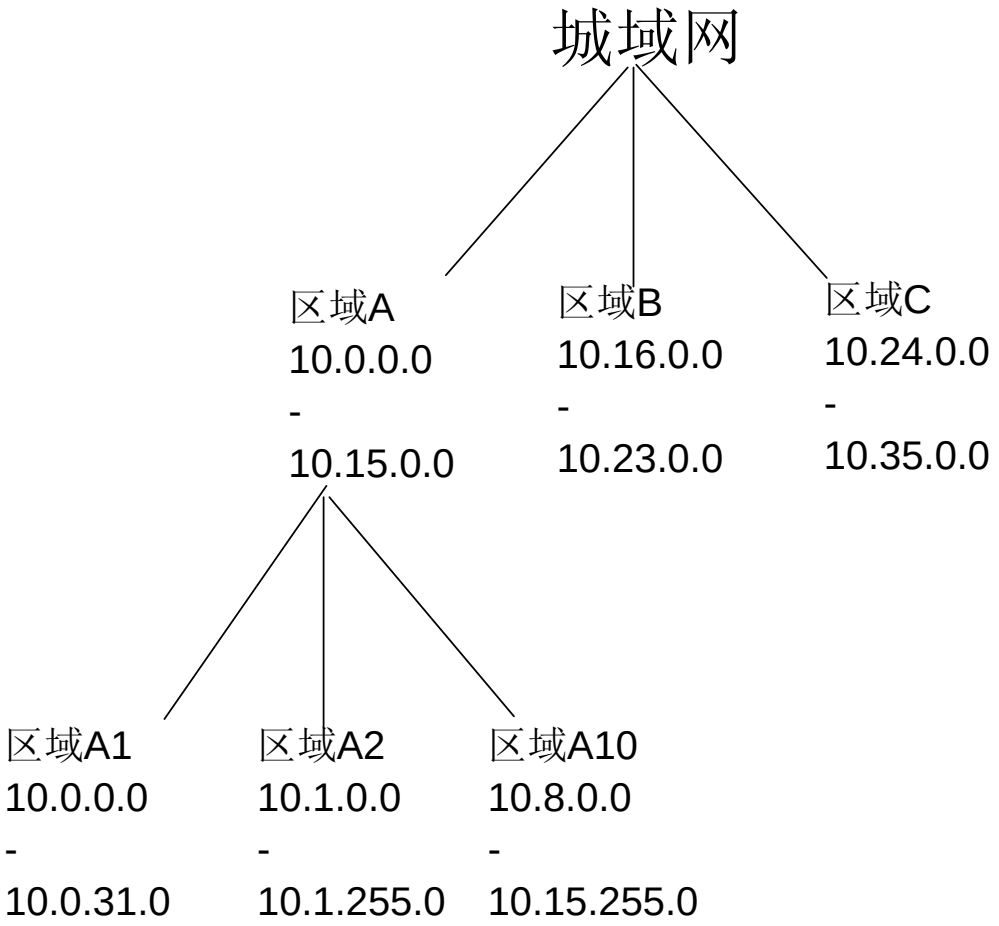
# 公网/私网IP地址混合优势

1. 采用灵活的NAT层次，可解决NG瓶颈问题；
2. 公网/私网地址灵活分配，可充分利用公网IP地址资源
3. 运营商设备都使用公网地址（适用于运营商既做骨干又做接入的情况），无须采用SNMP应用层解析；
4. 企业网/校园网采用公网地址大量减少了NG的工作量。

# 公网/私网IP地址混合弱势

1. 私有地址地址与公有地址混合，则增加了设备路由表复杂化；
2. NG会屏蔽一些已有业务（公网），需要进行会话层解析，但会导致NG性能下降
3. 除了对私网地址做规划外，还必须对公网地址做规划，增加了网络的维护复杂度。

# 城域网地址分布举例




**自顶向下规划地址**

聚合后分别是：
10.0/12
10.16/14
10.24/14

聚合后分别是：
10.0.0/28
10.1/16
10.8/14

# 关于NAT

- NAT只是一个补丁方案，对各种应用的解决更是补丁落补丁
- 需要特殊NAT应用很多
- 每种应用的NAT/ALG程序都不相同，实现NAT/ALG的难度与防火墙类似
- 但是NAT+ALG目前仍然是解决地址问题唯一的现实的方案

HUAWEI

# 总　　结

建议采用私有地址地址与公有地址混合的方式：

- 小区接入等便于规划管理、流量较小的接入方式采用私网地址及WEB认证方式；
- 企业网/校园网等难于规划管理、流量较大的接入方式采用公网地址；
- ADSL用户采用PPPOE方式认证及返回私网地址的方式。