第 6 部分 IP 协议

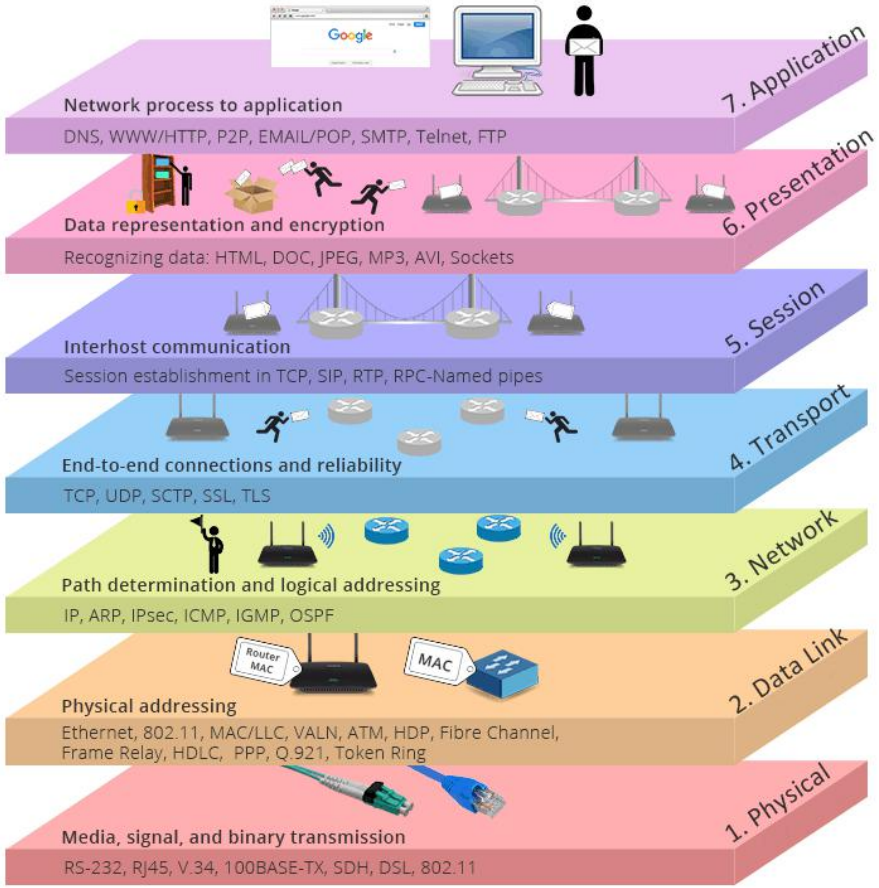
扫码试看/订阅极客时间

《Web协议详解与抓包实战》视频课程

第 1 课 网络层与链路层的功能

网络层功能

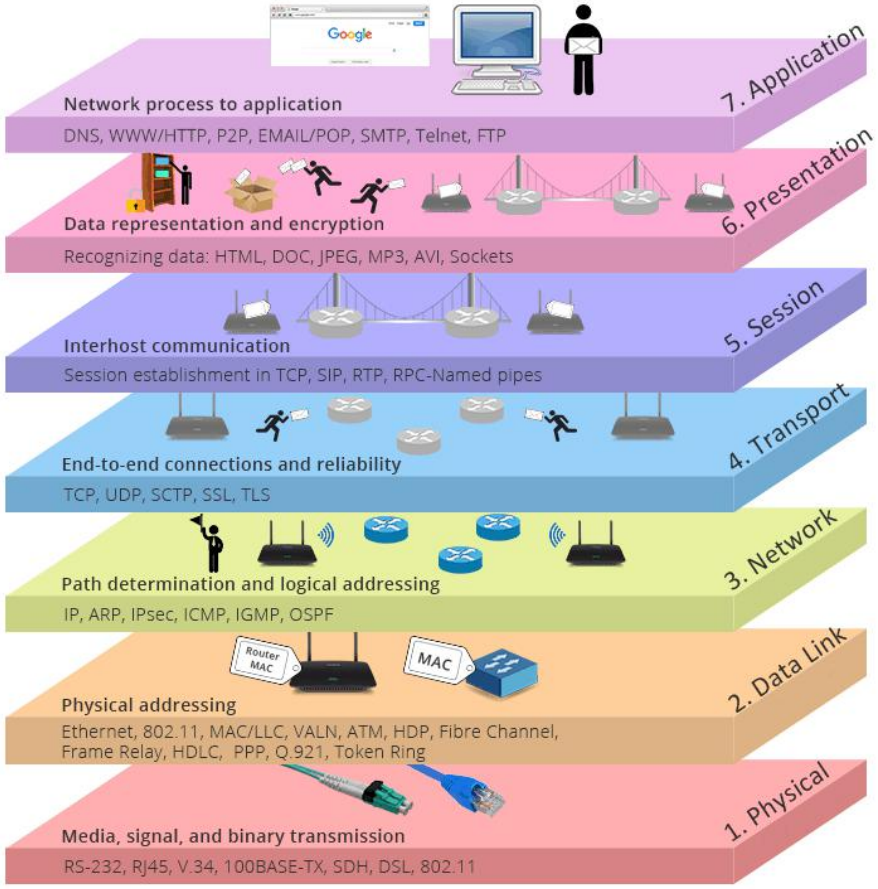
- IP 寻址
- 选路
- 封装打包
- 分片



- 应用层
- 表示层
- 会话层
- 传输层
- **三层/网络层**
- 二层/数据链路层
- 物理层

数据链路层功能

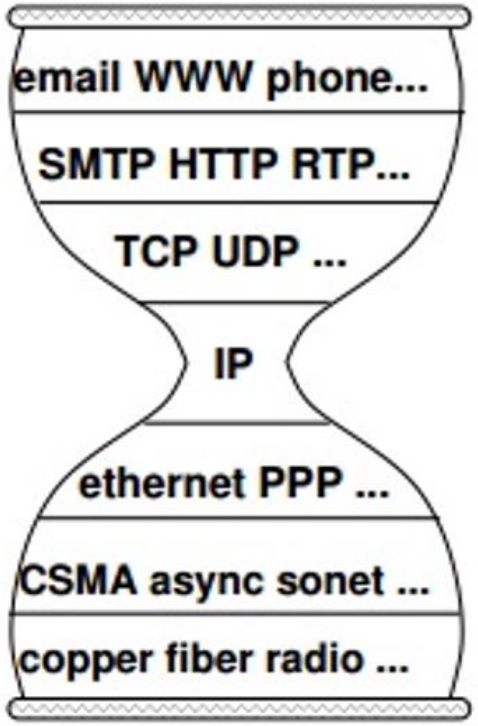
- 逻辑链路控制
- 媒体访问控制
- 封装链路层帧
- MAC 寻址
- 差错检测与处理
- 定义物理层标准



- 应用层
- 表示层
- 会话层
- 传输层
- 三层/网络层
- **二层/数据链路层**
- 物理层

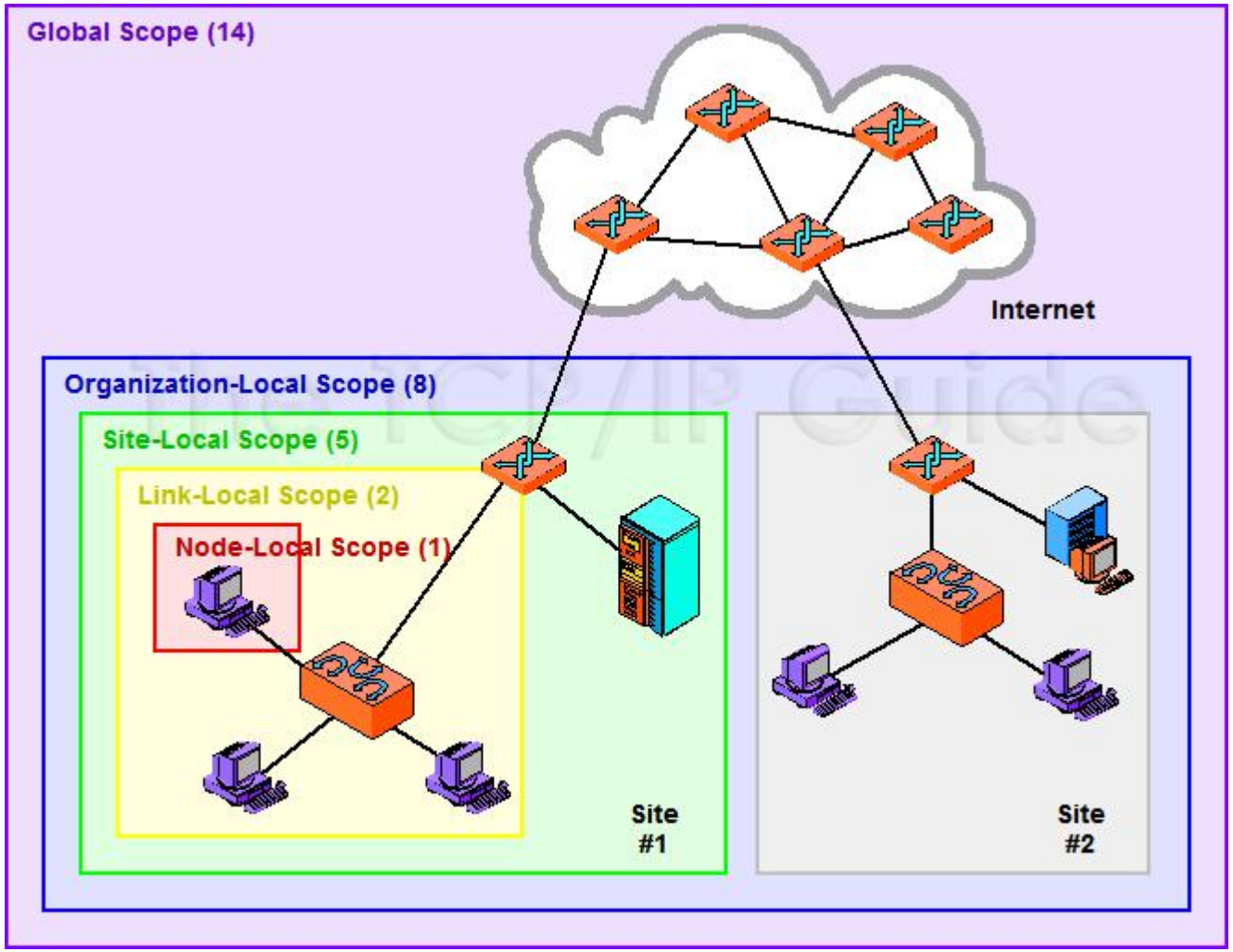
细腰结构：IP 网络层的核心地位

- 性能至上的 IP 层
  - 无连接
  - 非可靠
  - 无确认



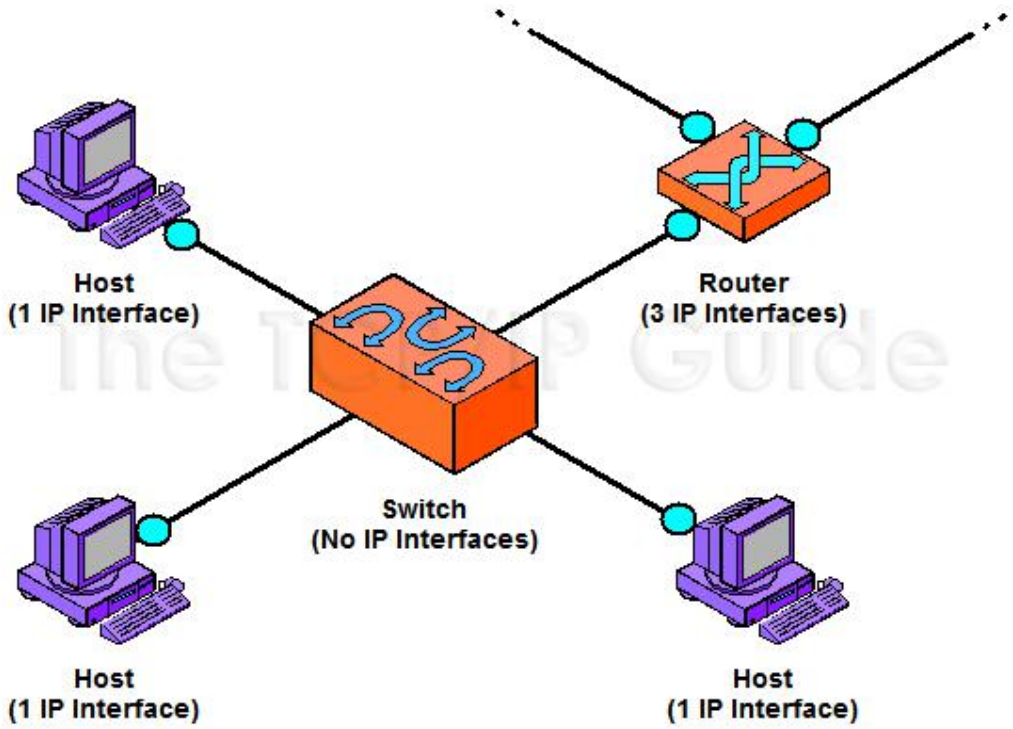
多播：广播与组播

- 全球作用域
- 组织内
- 场点内
- 本地链路层
- 本机作用域

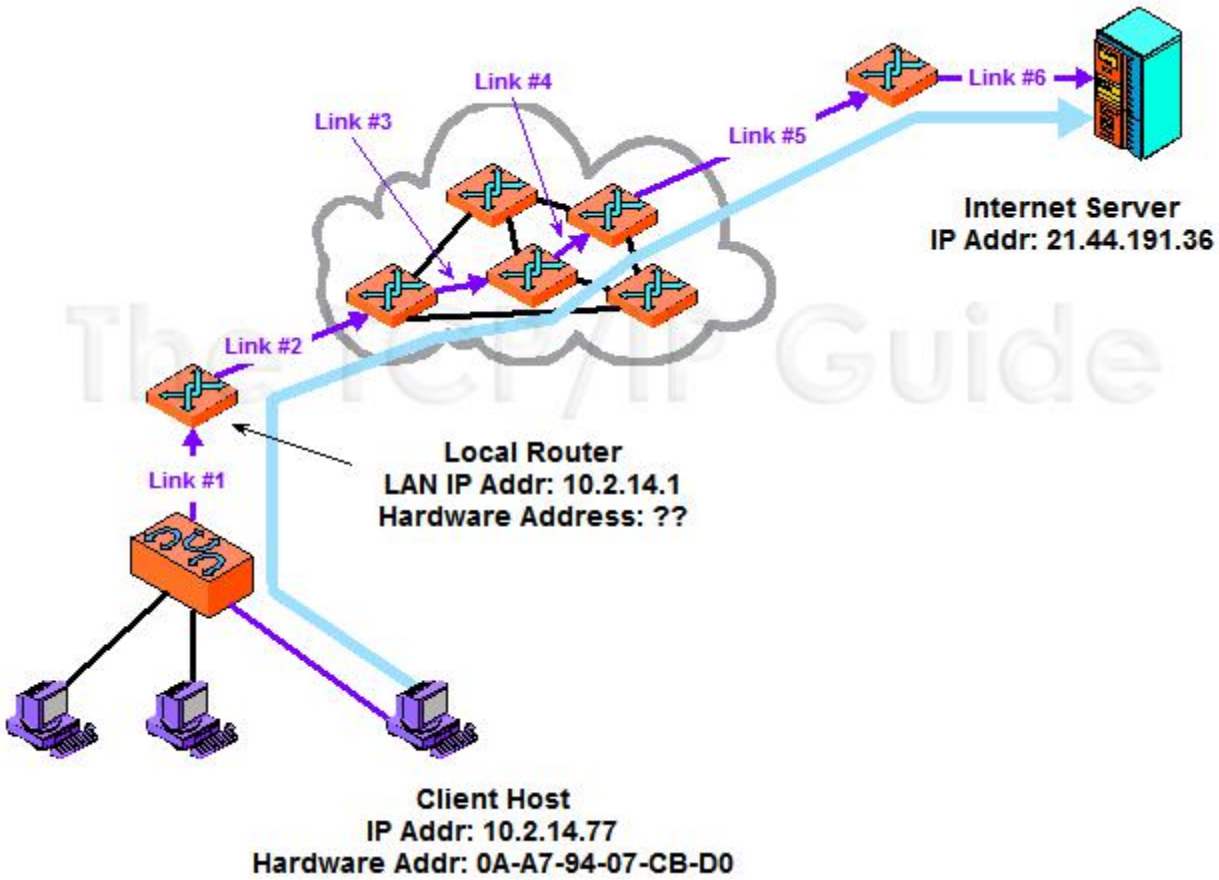


路由器与交换机

- 工作在网络层的路由器
  - 连接不同网络的设备
- 工作在数据链路层的交换机
  - 同一个网络下连接不同主机的设备



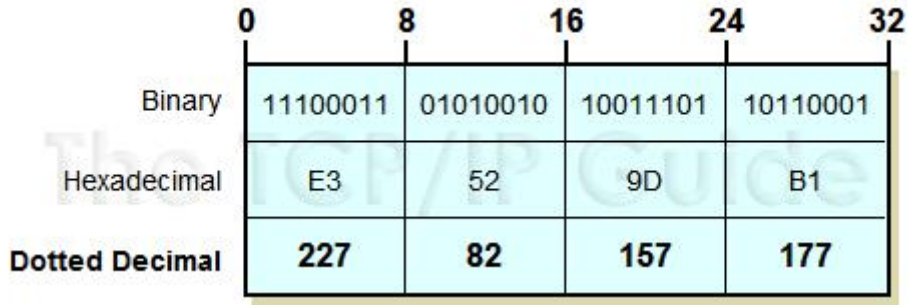
网络传输示例


Link #1
Link #2
Link #3
Link #4
Link #5
Link #6
Internet Server
IP Addr: 21.44.191.36
Local Router
LAN IP Addr: 10.2.14.1
Hardware Address: ??
Client Host
IP Addr: 10.2.14.77
Hardware Addr: 0A-A7-94-07-CB-D0

第 2 课 IPv4 分类地址

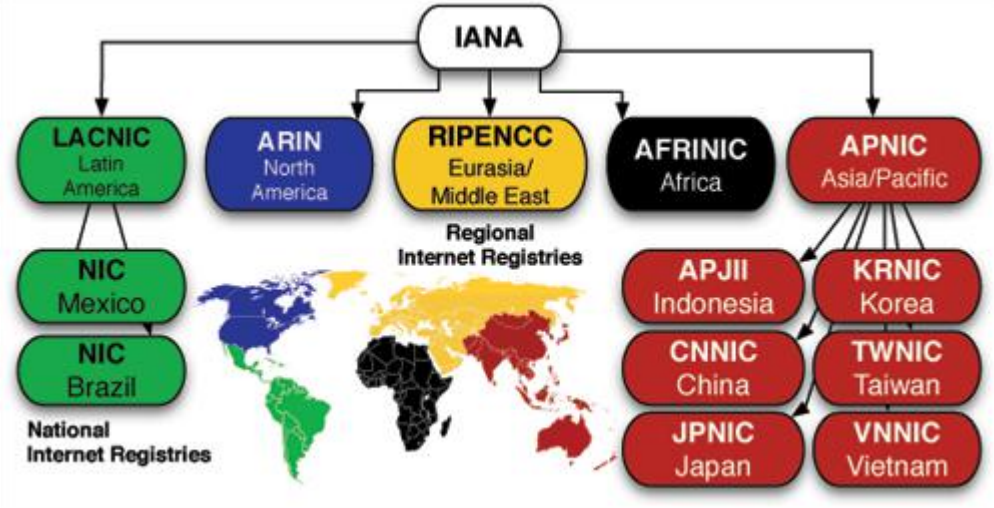
易用性：IPv4 地址的点分十进制表示

- 32 位二进制数
- IP 地址空间：2^{32} 个



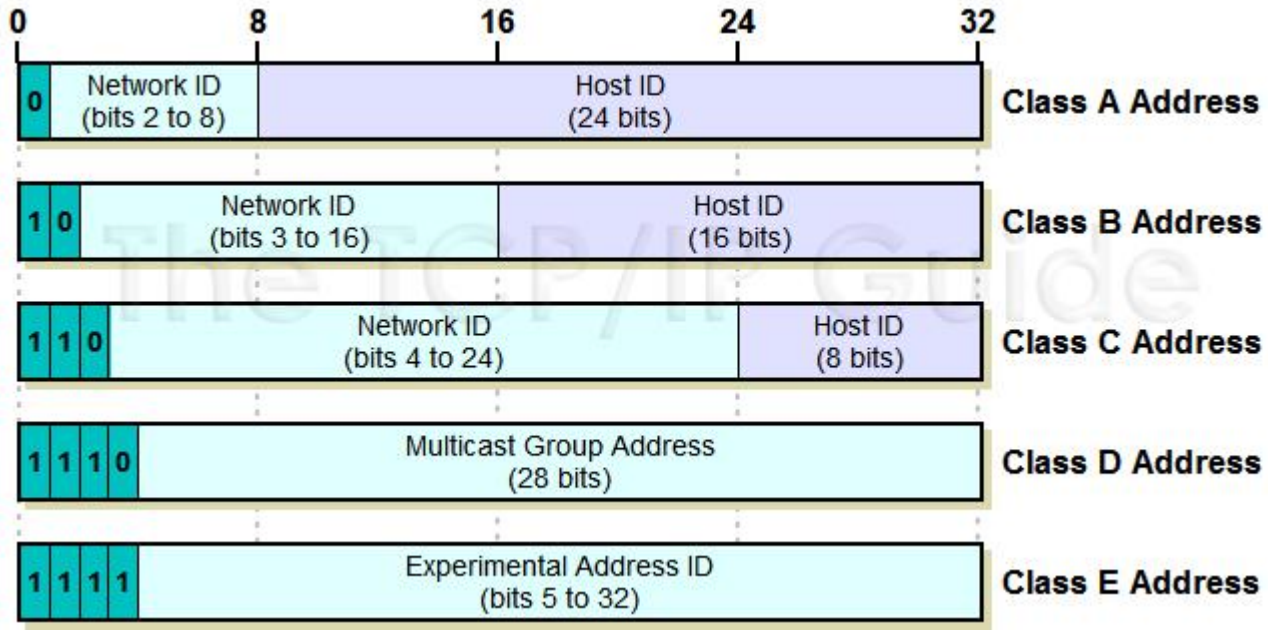
IP 地址的分配机构

- 层层分配的 IP 地址



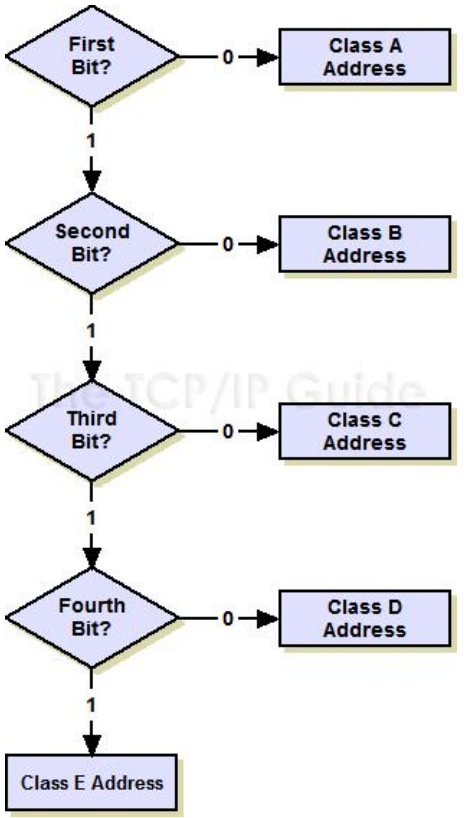
当互联网规律很小时，类别信息被编码进 IP 地址

IP 地址类别	首字节	网络号 Bit 数	主机号 Bit 数	理论地址范围	预期用途
A 类地址	0xxx xxxx	8	24	1.0.0.0 -126.255.255.255	特大网络的单播传输
B 类地址	10xx xxxx	16	16	128.0.0.0 -191.255.255.255	数千台中大型网络的单播传输
C 类地址	110x xxxx	24	8	192.0.0.0 -223.255.255.255	250 台主机以下小型网络的单播传输
D 类地址	1110 xxxx	n/a	n/a	224.0.0.0 -239.255.255.255	IP 多播
E 类地址	1111 xxxx	n/a	n/a	240.0.0.0 - 255.255.255.255	预留实验用



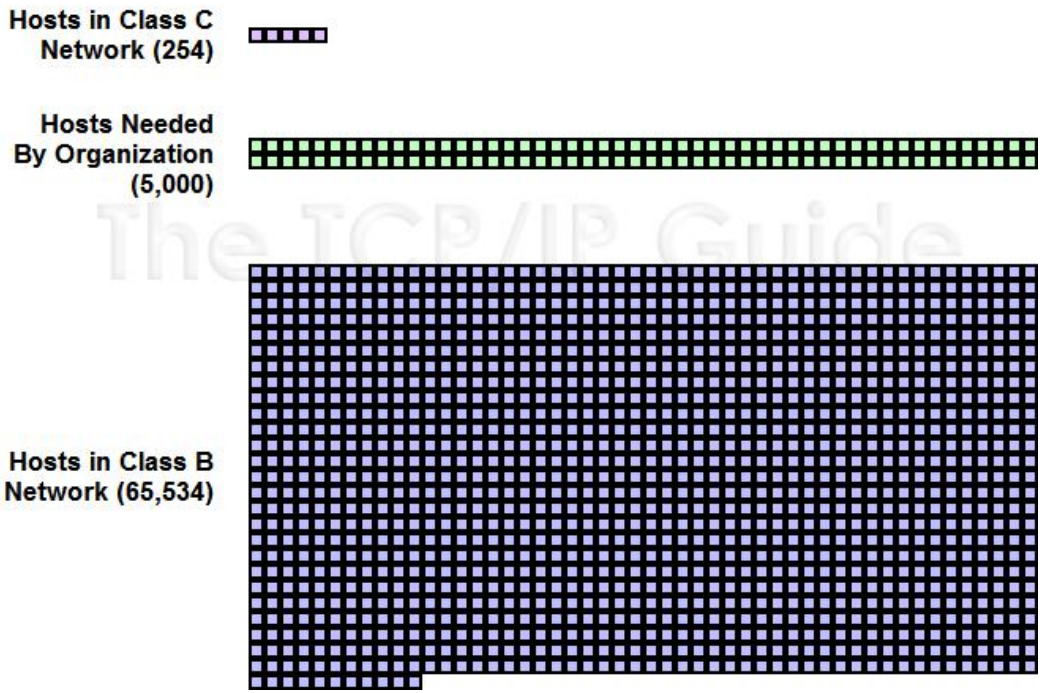
分类 IP 地址的优点

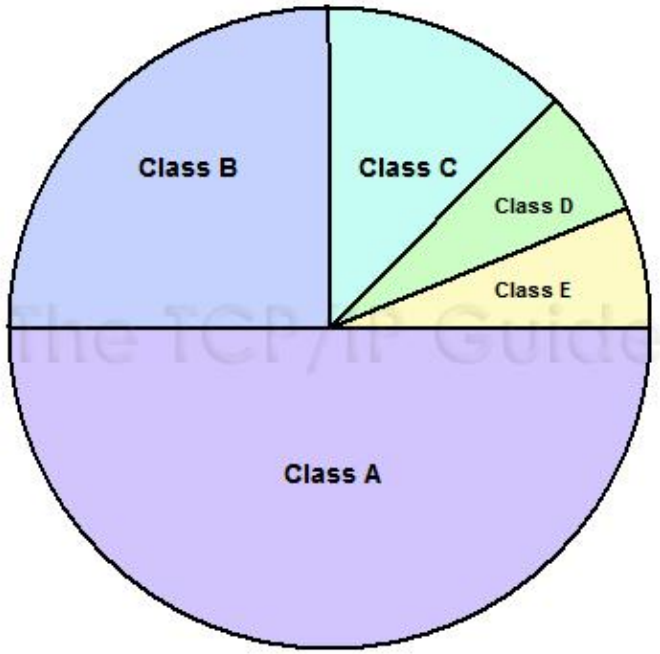
- 简单明了
- 具有 3 个级别的灵活性
- 选路（基于网络地址）简单



分类 IP 寻址的问题

- 缺少私有网络下的地址灵活性：同一个网络下没有地址层次
- 3 类地址块太少，无法与现实网络很好的匹配

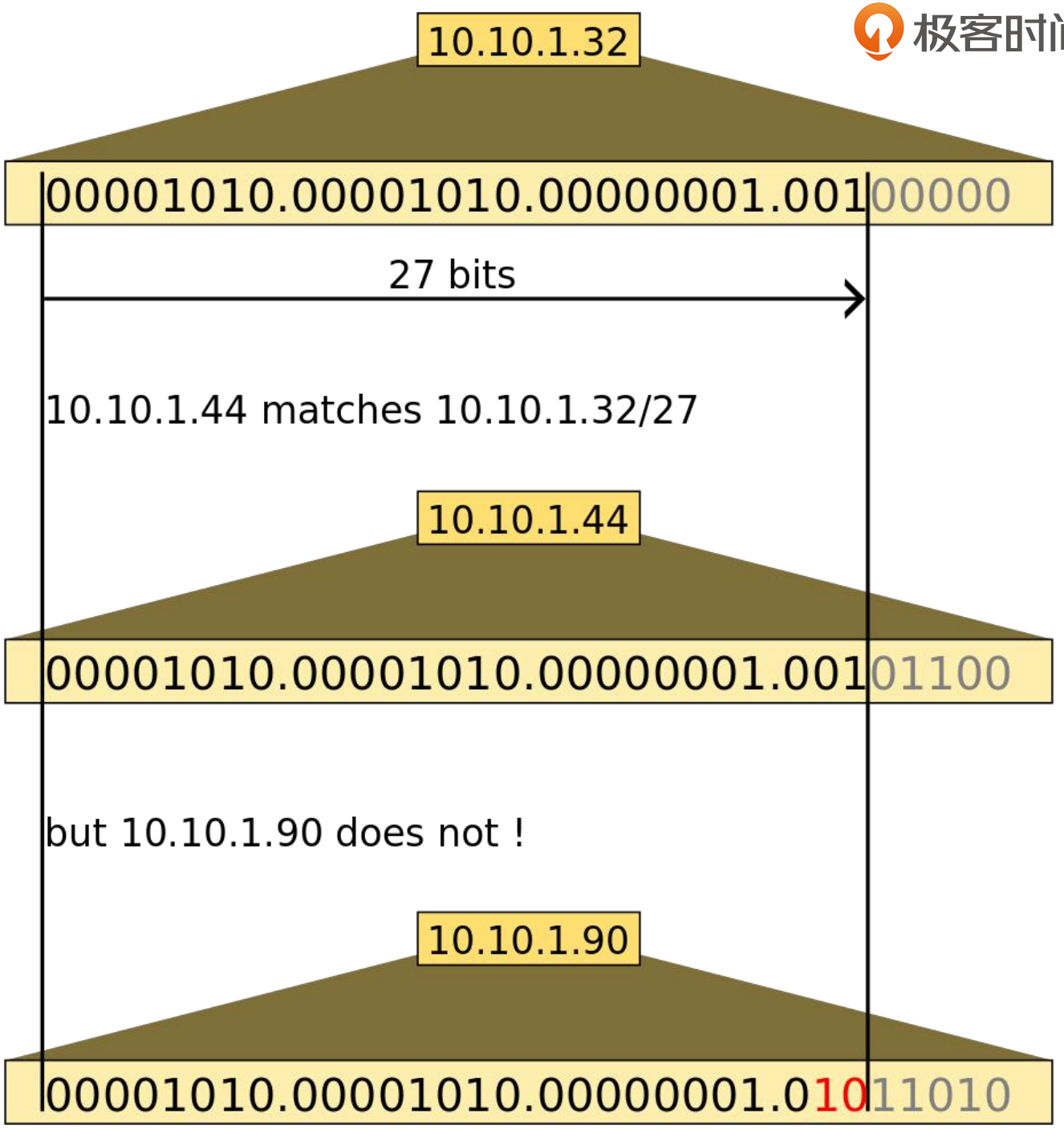




第 3 课 CIDR无分类地址

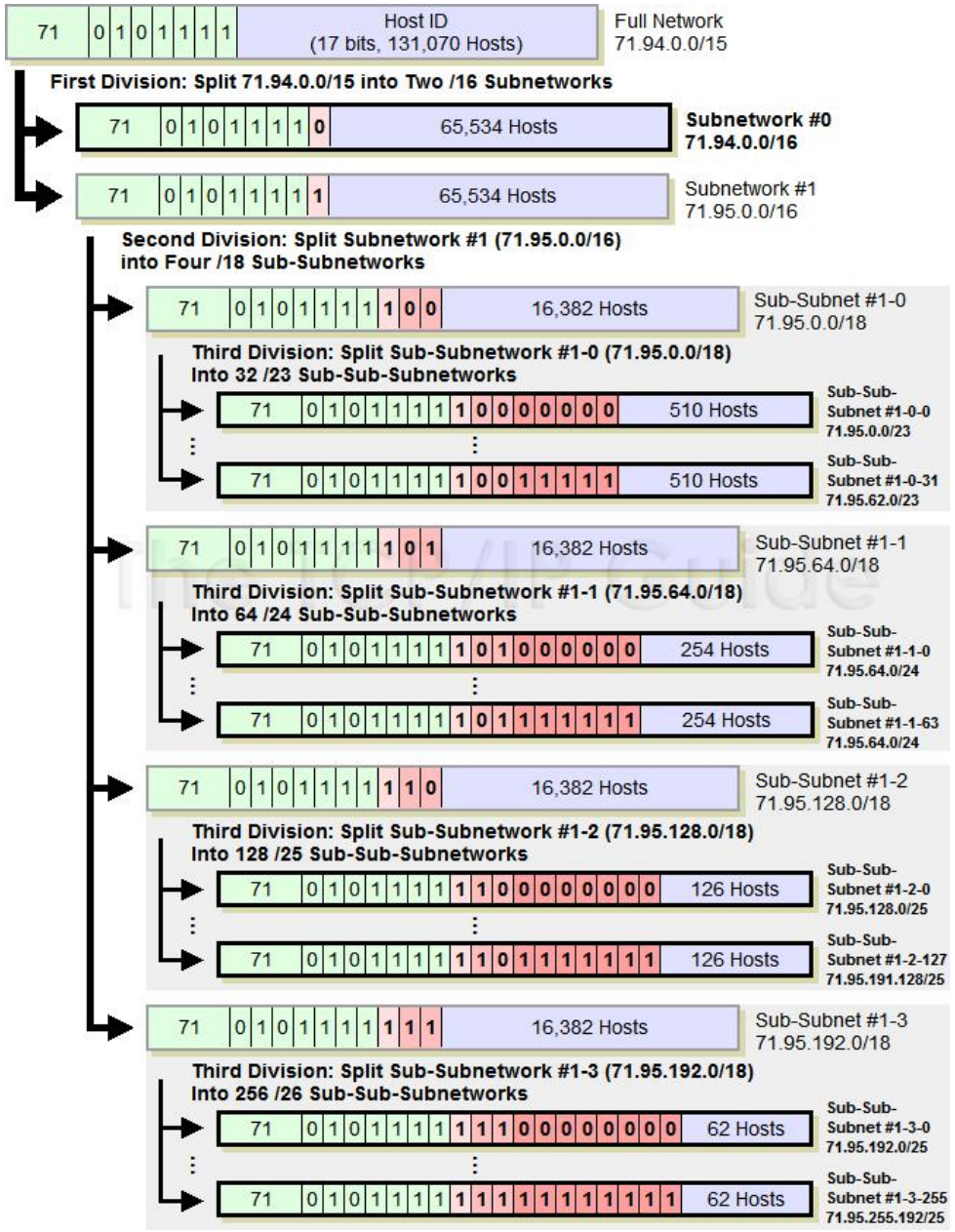
CIDR 子网掩码

- CIDR
  - Classless Inter-Domain Routing
- 表示方法
  - A.B.C.D/N，N 范围[0, 32]



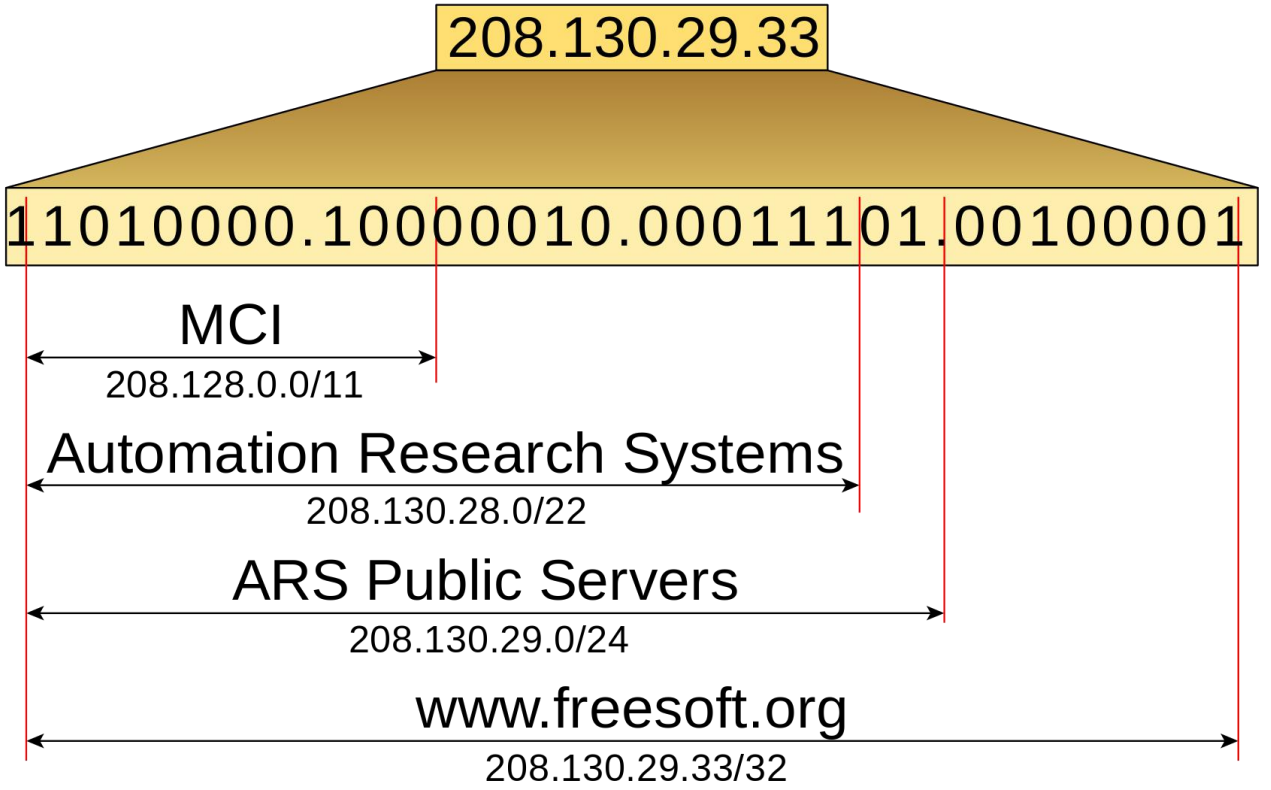
CIDR 子网划分示例

- 71.94.0.0/15
  - 多级子网划分



208.130.29.33 的寻址历程

- MCI 分配到了 208.128.0.0/11
- MCI 将 208.130.28.0/22 分配给 ARS
- ARS 将 208.130.29.0/22 分配给 Public Servers 使用
- www.freesoft.org 使用了 208.130.29.33 地址



全 0 或者全 1 的特殊含义

网络号	主机号	A 类示例	B 类示例	C 类示例	含义
网络号	主机号	77.91.215.5	154.3.99.6	227.82.157.160	指定某个主机
网络号	全 0	77.0.0.0	154.3.0.0	227.82.157.0	指定某个网络
全 0	主机号	0.91.215.5	0.0.99.6	0.0.0.160	指定当前所属网络下的某个主机
全 0	全 0		0.0.0.0		指定自己的默认 IP 地址
网络号	全 1	77.255.255.255	154.3.255.255	227.82.157.255	指定某个网络下的所有主机，用于广播
全 1	全 1		255.255.255.255		所有主机

预留 IP 地址（RFC1918）

起始地址	结束地址	等价分类地址	等价无类别地址	描述
0.0.0.0	0.255.255.255	A 类网络0.x.x.x	0/8	保留
10.0.0.0	10.255.255.255	A 类网络10.x.x.x	10/8	A 类私有地址
127.0.0.0	127.255.255.255	A 类网络127.x.x.x	127/8	环回地址
128.0.0.0	128.0.255.255	B 类网络128.0.x.x	128.0/16	保留
169.254.0.0	169.254.255.255	B 类网络169.254.x.x	169.254/16	B 类私有地址（APIPA）
172.16.0.0	172.31.255.255	从 172.16.x.x 至 172.31.x.x 共 16 个 B 类网络	172.16/12	B 类私有地址
191.255.0.0	191.255.255.255	B 类网络191.255.x.x	191.255/16	保留
192.0.0.0	192.0.0.255	C 类网络192.0.0.x	192.0.0/24	保留
192.168.0.0	192.168.255.255	从 192.168.0.x 至 192.168.255.x 共256个C类网络	192.168/16	C 类私有地址
223.255.255.0	223.255.255.255	C 类网络 223.255.255.x	223.255.255/24	保留

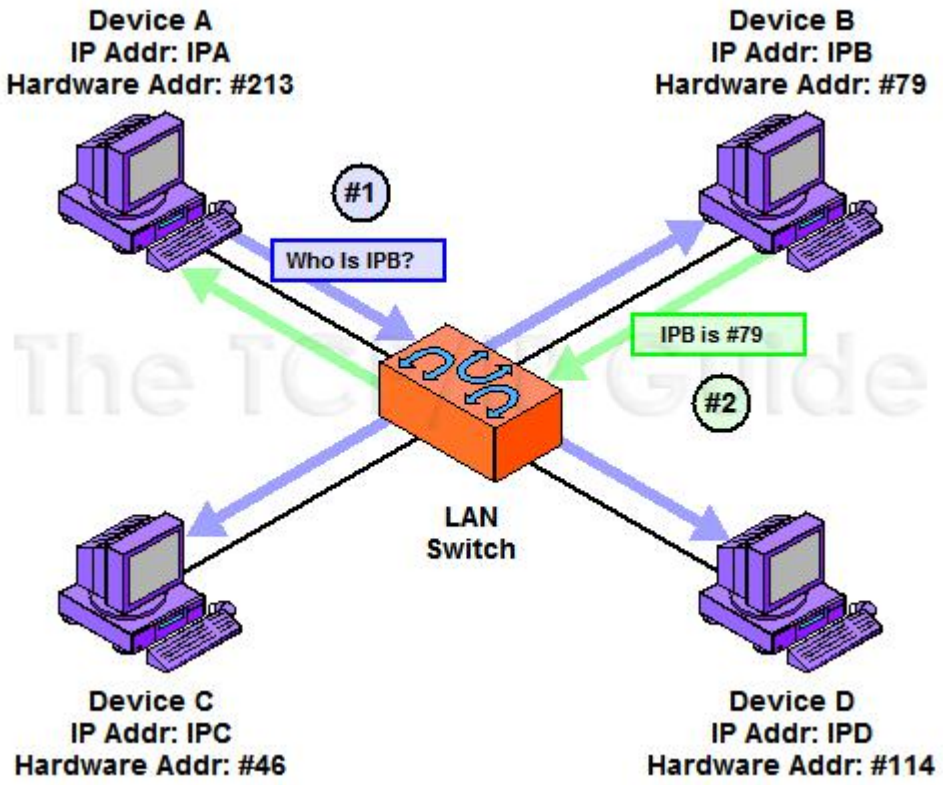
第 4 课 IP 地址与链路地址的转换：ARP 与 RARP 协议

链路层 MAC 地址

- 链路层地址 MAC（Media Access Control Address）
  - 实现本地网络设备间的直接传输
- 网络层地址 IP（Internet Protocol address）
  - 实现大型网络间的传输，
- 查看 MAC 地址
  - Windows: ipconfig /all
  - Linux：ifconfig

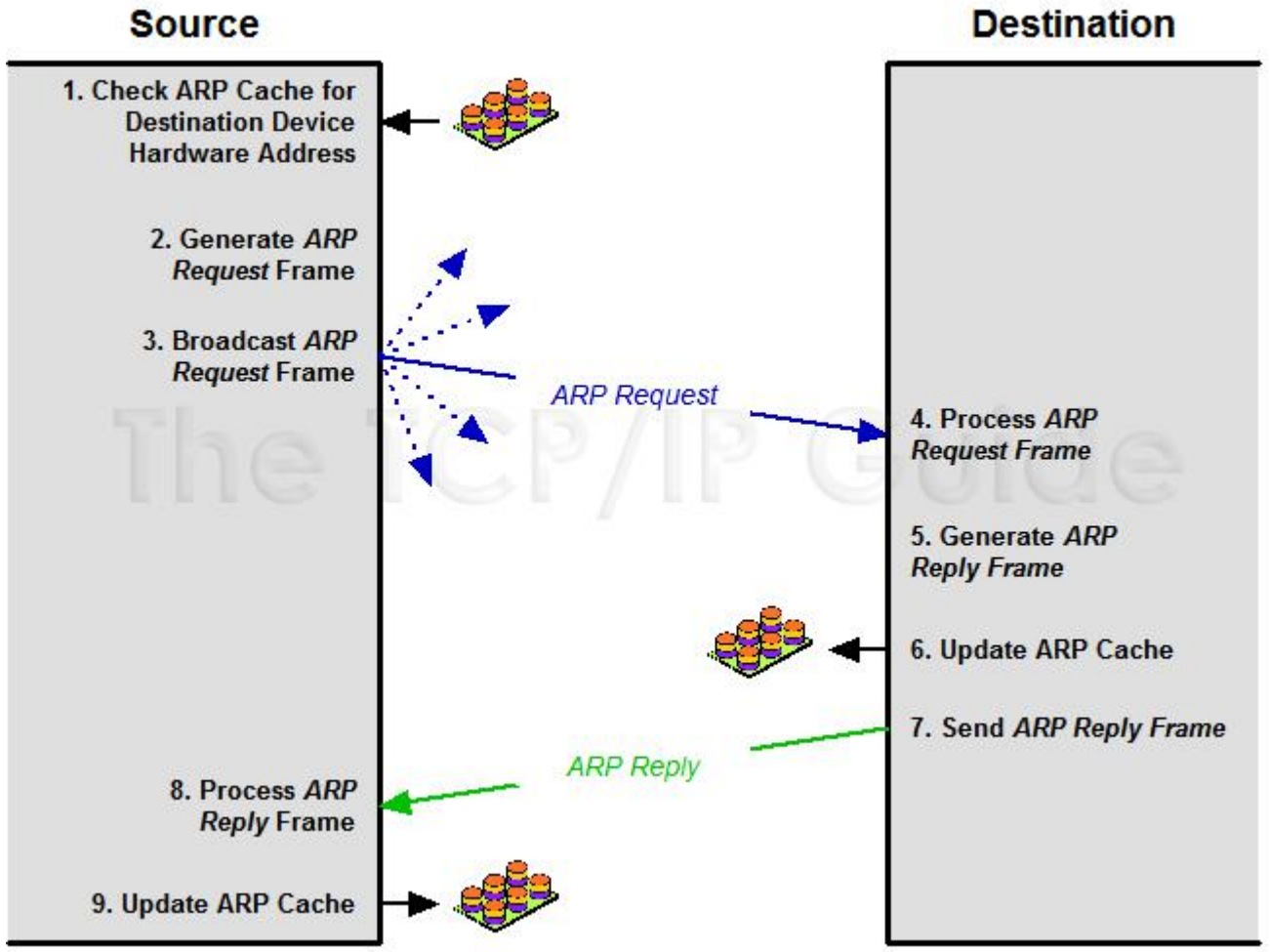
2.5 层协议 ARP：从 IP 地址寻找 MAC 地址

- 动态地址解析协议 ARP（RFC826）
  - Address Resolution Protocol
- 动态地址解析：广播



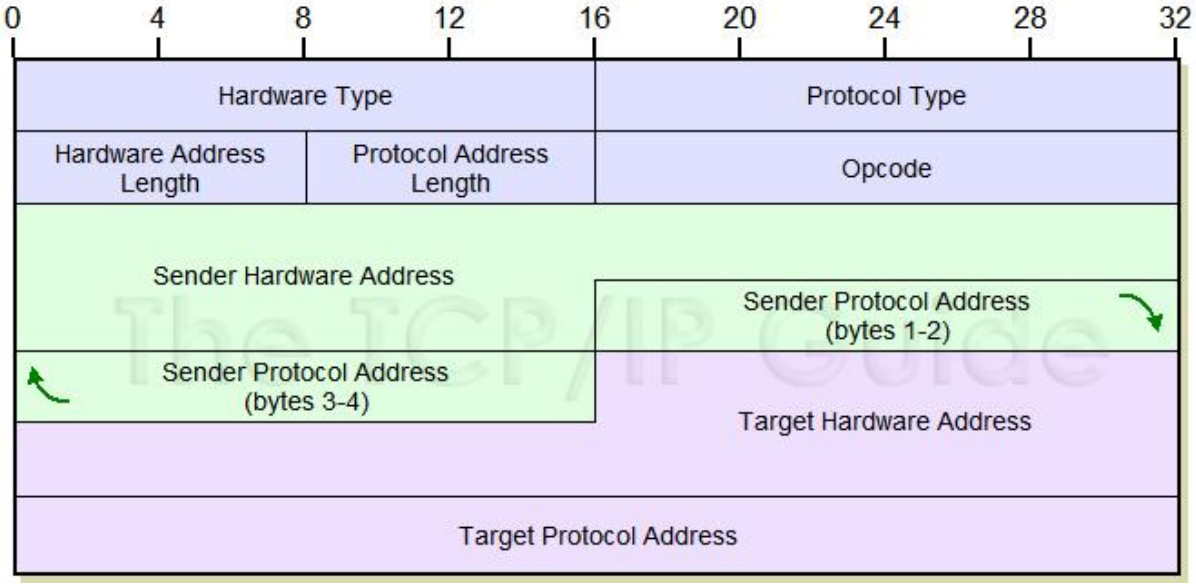
2.5 层协议：ARP

1. 检查本地缓存
   - Windows: arp –a
   - Linux: arp –nv
   - Mac: arp -nla
2. 广播形式的请求
3. 单播形式的应答



ARP 报文格式：FrameType=0x0806

- 硬件类型，如 1 表示以太网
- 协议类型，如 0x0800 表示 IPv4
- 硬件地址长度，如 6
- 协议地址长度，如 4 表示 IPv4
- 操作码，如 1 表示请求，2 表示应答
- 发送方硬件地址
- 发送方协议地址
- 目标硬件地址
- 目标协议地址



硬件类型与操作码

- 硬件类型取值

Hardware Type: This field specifies the type of hardware used for the local network transmitting the ARP message; thus, it also identifies the type of addressing used. Some of the most common values for this field:

HRD Value	Hardware Type
1	Ethernet (10 Mb)
6	IEEE 802 Networks
7	ARCNET
15	Frame Relay
16	Asynchronous Transfer Mode (ATM)
17	HDLC
18	Fibre Channel
19	Asynchronous Transfer Mode (ATM)
20	Serial Line

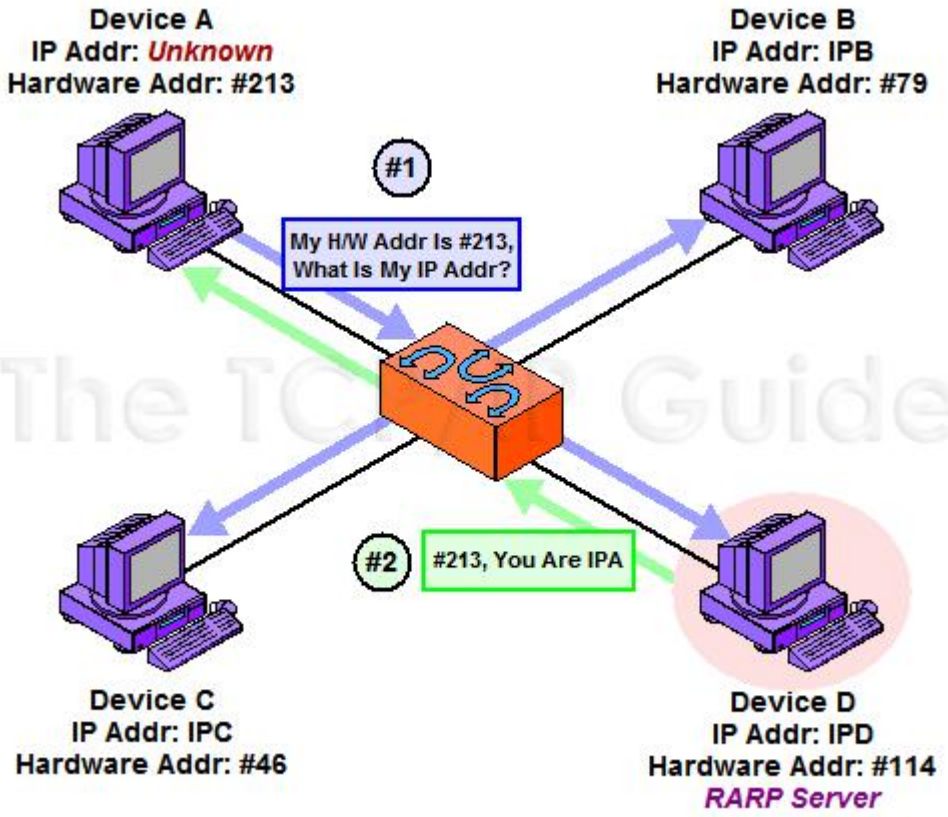
- 操作码取值

Opcode: This field specifies the nature of the ARP message being sent. The first two values (1 and 2) are used for regular ARP. Numerous other values are also defined to support other protocols that use the ARP frame format, such as RARP, some of which are more widely used than others:

Opcode	ARP Message Type
1	ARP Request
2	ARP Reply
3	RARP Request
4	RARP Reply
5	DRARP Request
6	DRARP Reply
7	DRARP Error
8	InARP Request
9	InARP Reply

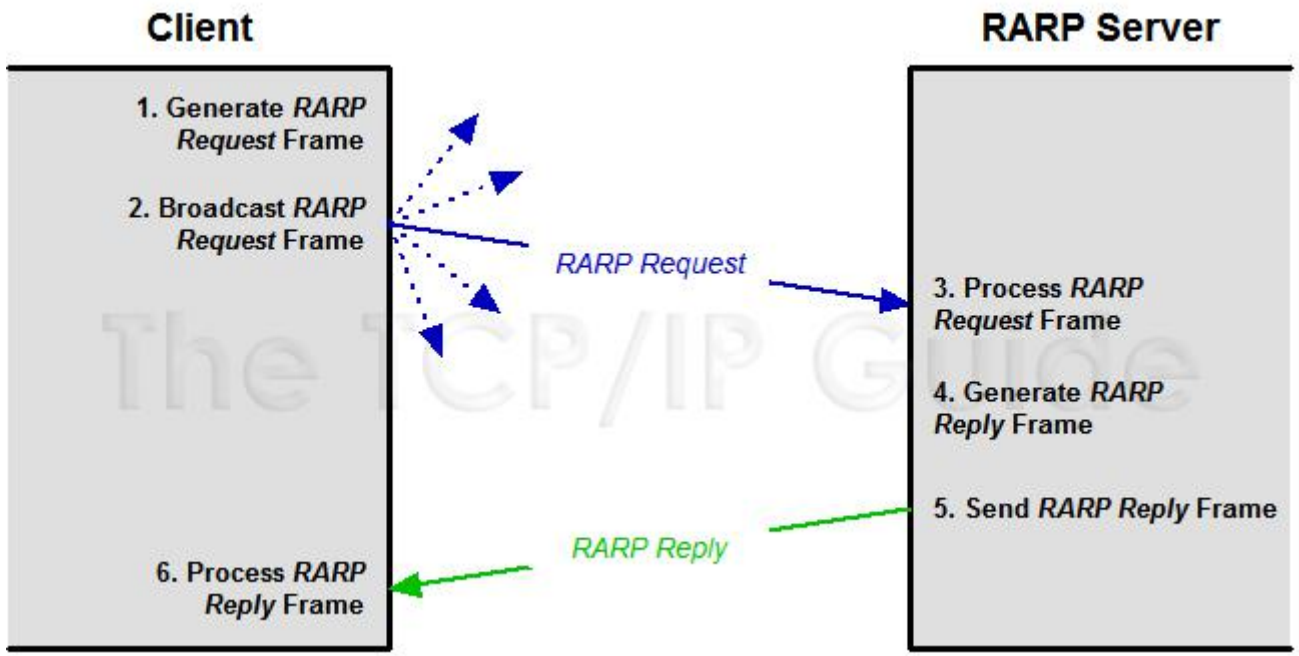
2.5 层协议 RARP：从 MAC 地址中寻找 IP 地址

- 动态地址解析协议 RARP（RFC903）
  - Reverse Address Resolution Protocol



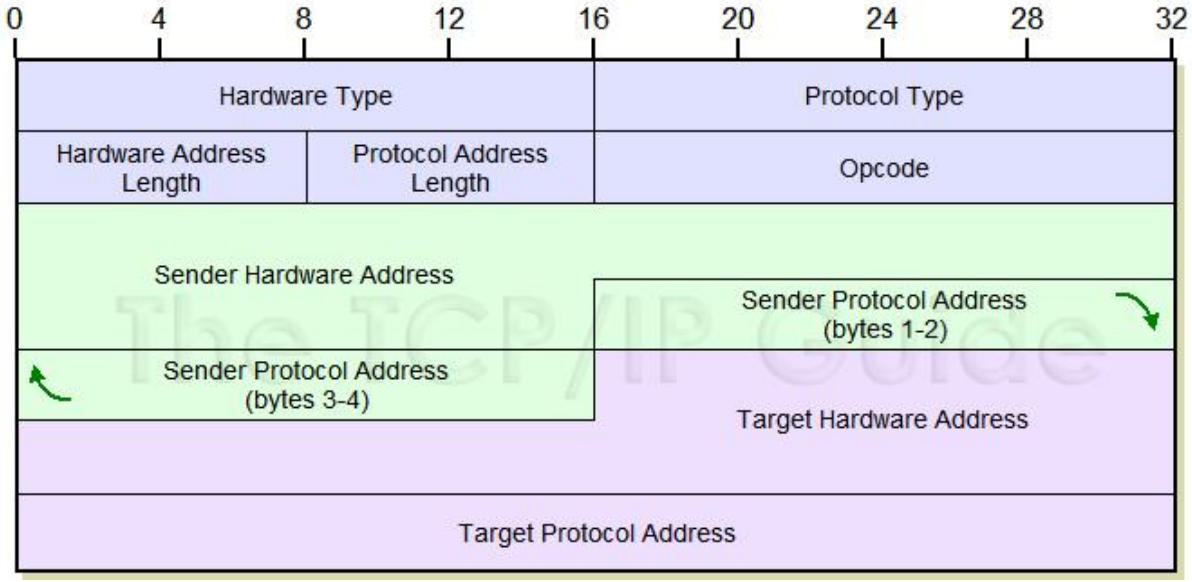
RARP 的工作流程

1. 广播形式的请求
2. 单播形式的应答

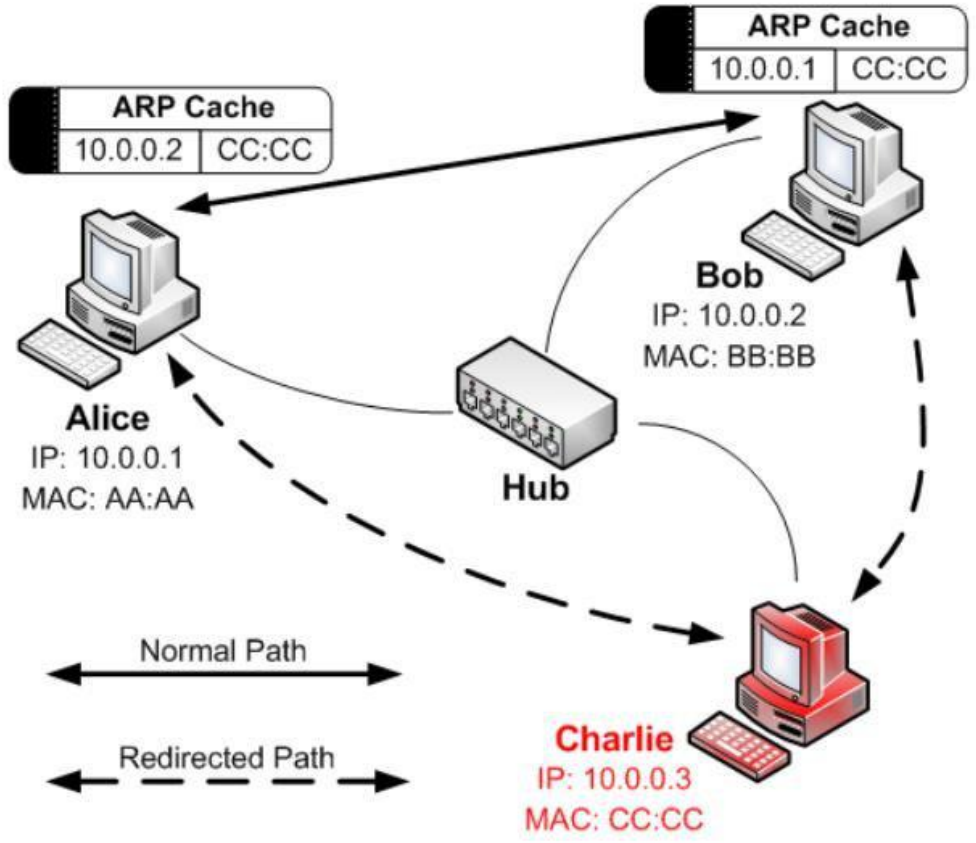


RARP 报文格式：FrameType=0x8035

- 硬件类型，如 1 表示以太网
- 协议类型，如 0x0800 表示 IPv4
- 硬件地址长度，如 6
- 协议地址长度，如 4 表示 IPv4
- 操作码，如 3 表示请求，4 表示应答
- 发送方硬件地址
- 发送方协议地址
- 目标硬件地址
- 目标协议地址

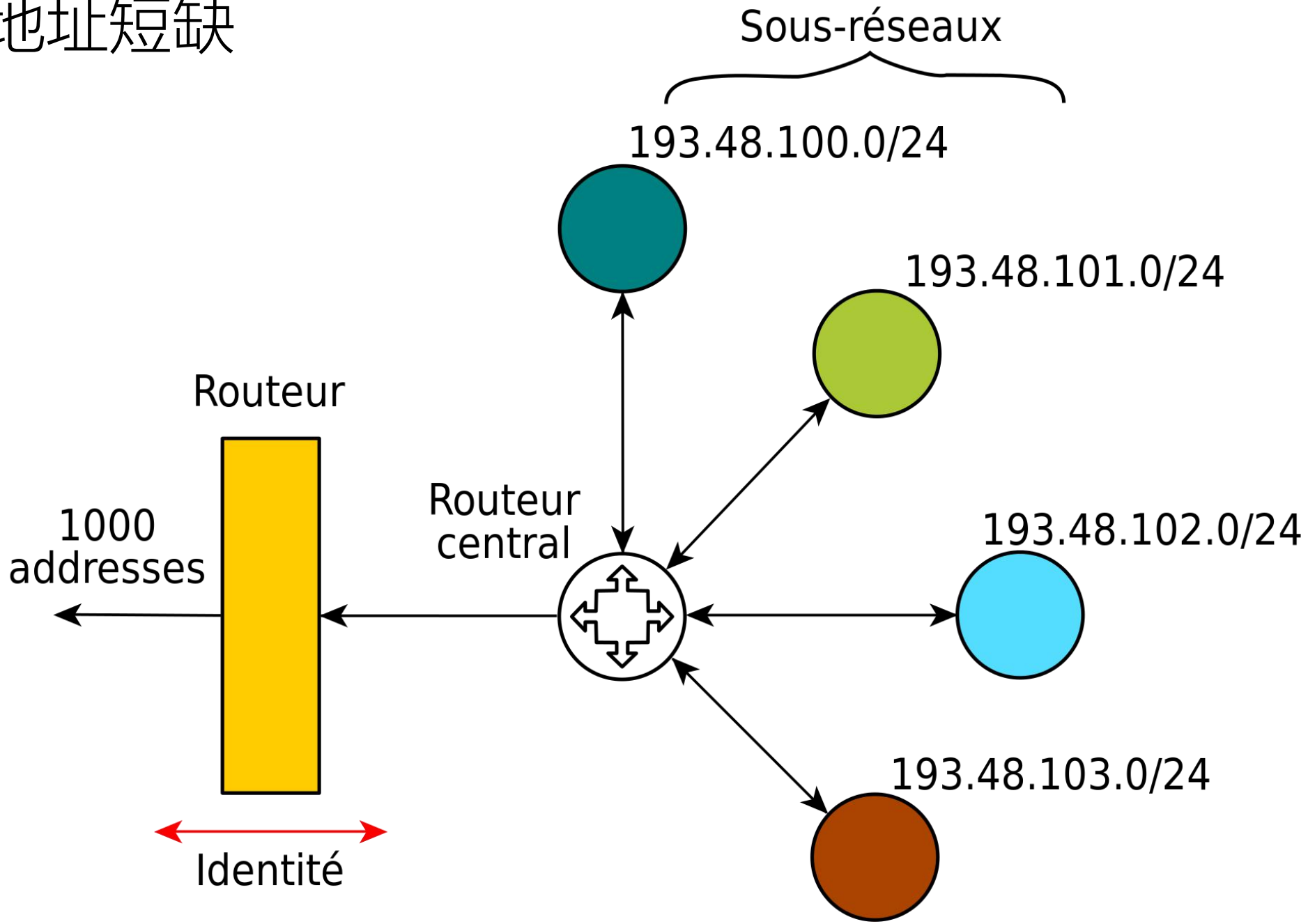


ARP 欺骗（ARP spoofing/poisoning）

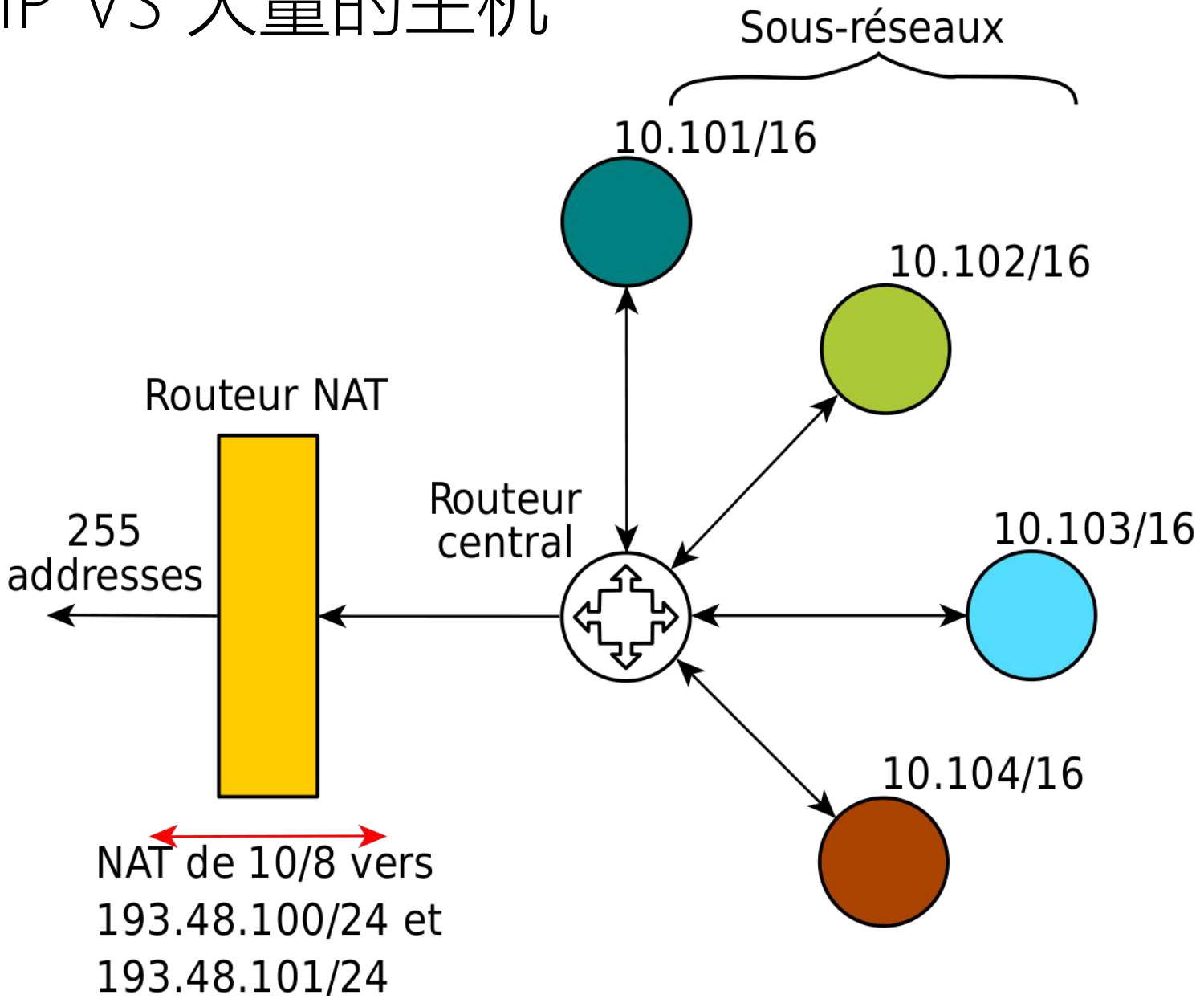


第 5 课 NAT 地址转换与 LVS 负载均衡

IPv4 地址短缺


Sous-réseaux
193.48.100.0/24
193.48.101.0/24
Routeur
1000
addresses
Routeur
central
193.48.102.0/24
193.48.103.0/24
Identité

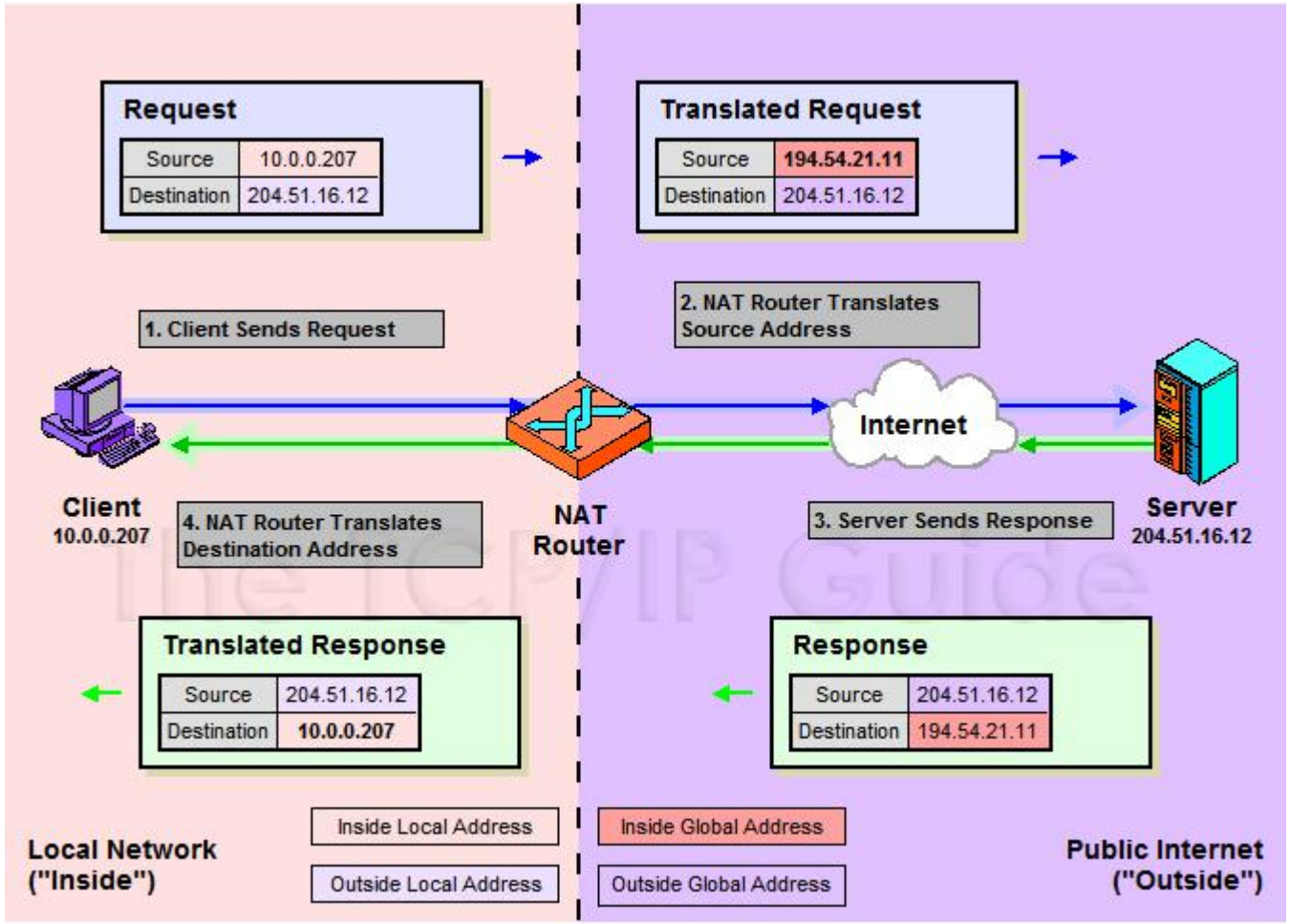
少量的公网 IP VS 大量的主机



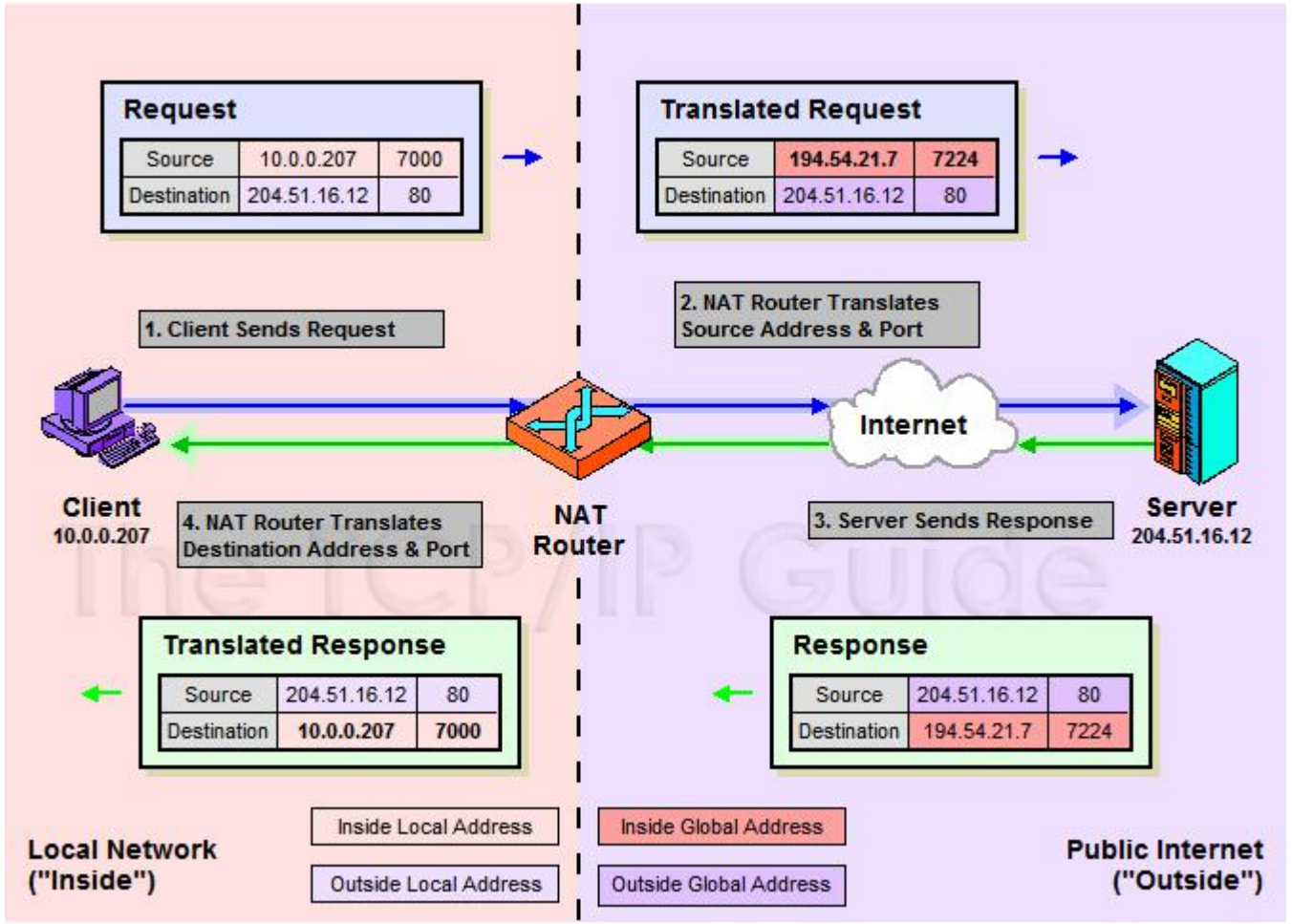
NAT（IP Network Address Translator）应用的前提

- 内网中主要用于客户端访问互联网
- 同一时间仅少量主机访问互联网
- 内网中存在一个路由器负责访问外网

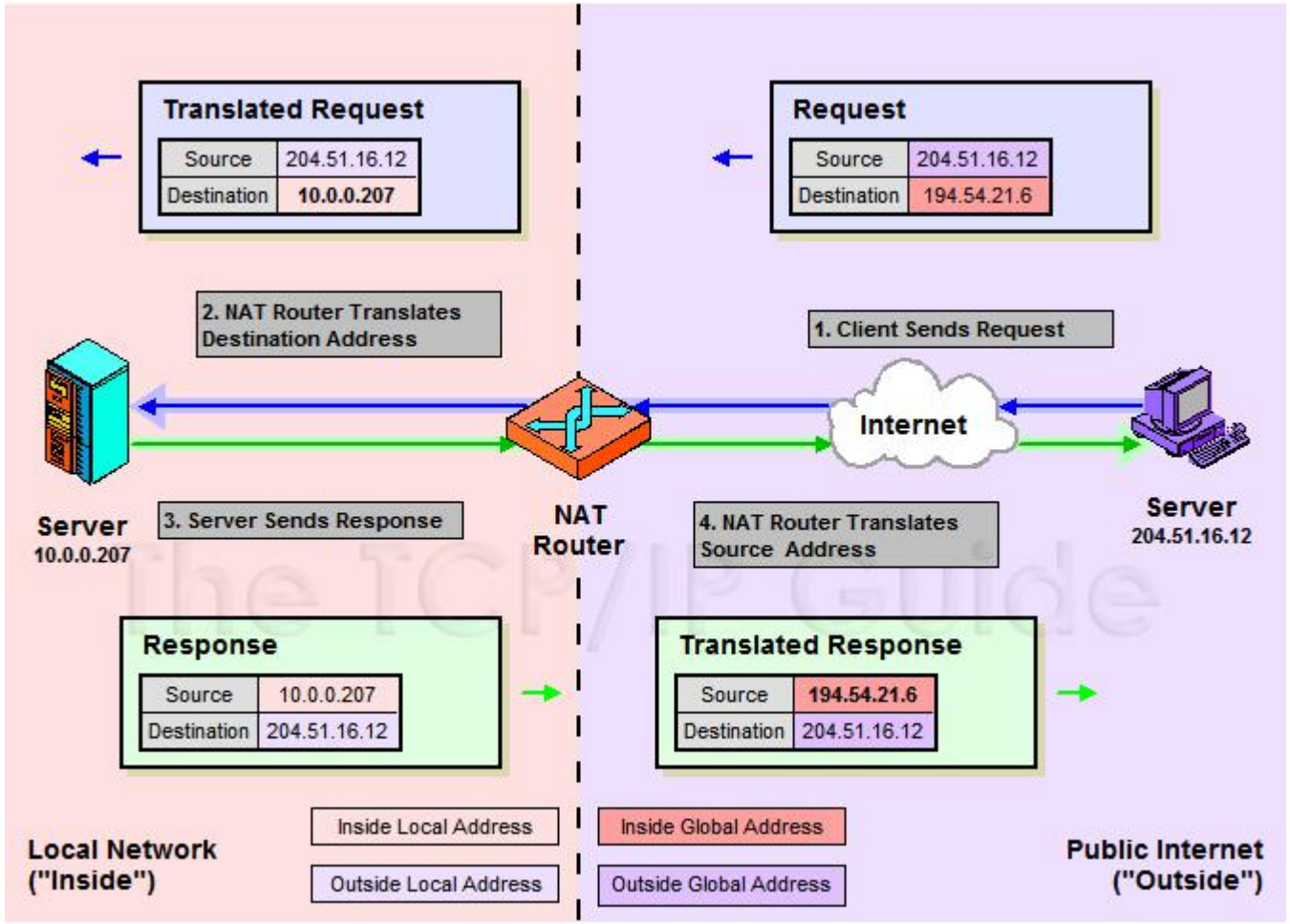
单向（向外）转换 NAT：动态映射



NAPT 端口映射：Network Address Port Translation

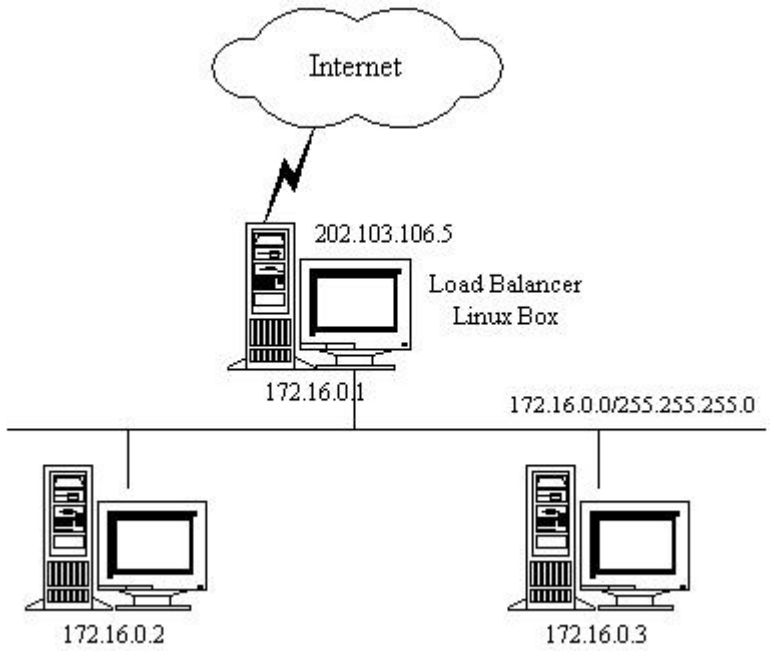


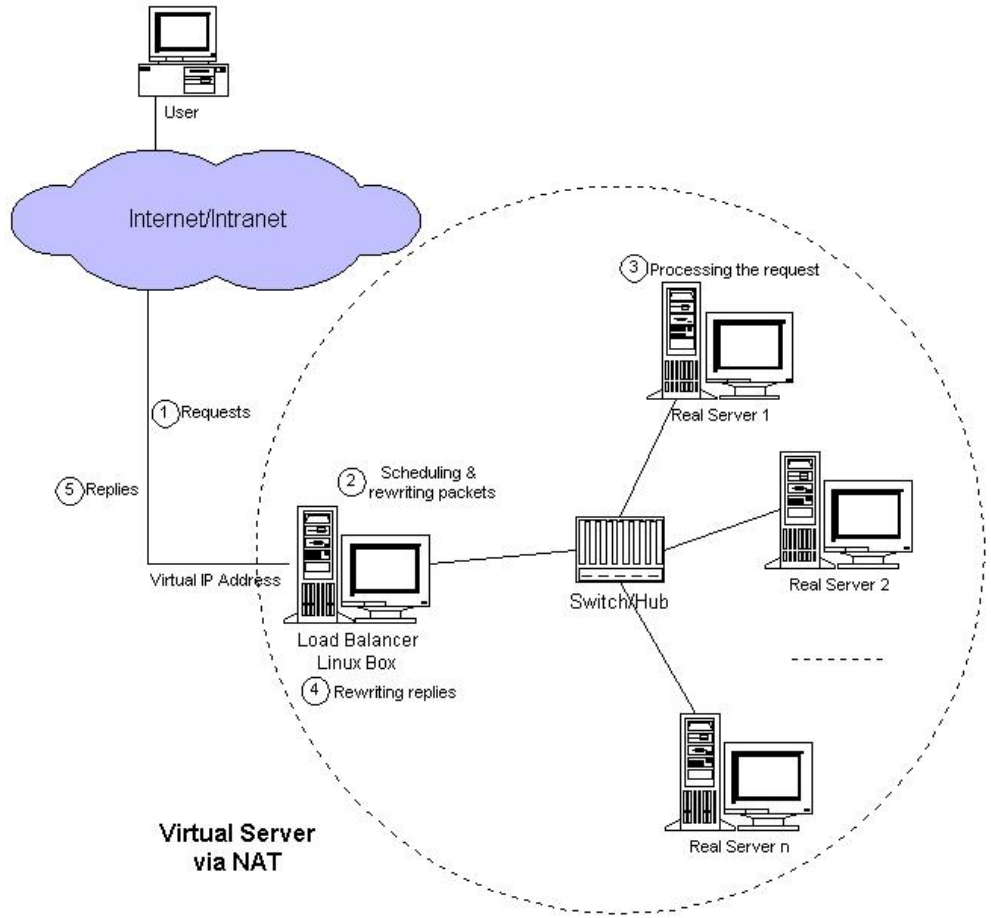
双向（向内）NAT：IP 地址静态映射



LVS（Linux Virtual Server）/NAT 工作模式

- 三层负载均衡





NAT 优点

优点

- 共享公共 IP 地址，节约开支
- 扩展主机时不涉及公共地址
- 更换 ISP 服务商（更换公网 IP 地址），不对主机地址产生影响
- 更好的安全性，外部服务无法主动访问内网服务
- 更好的隔离性

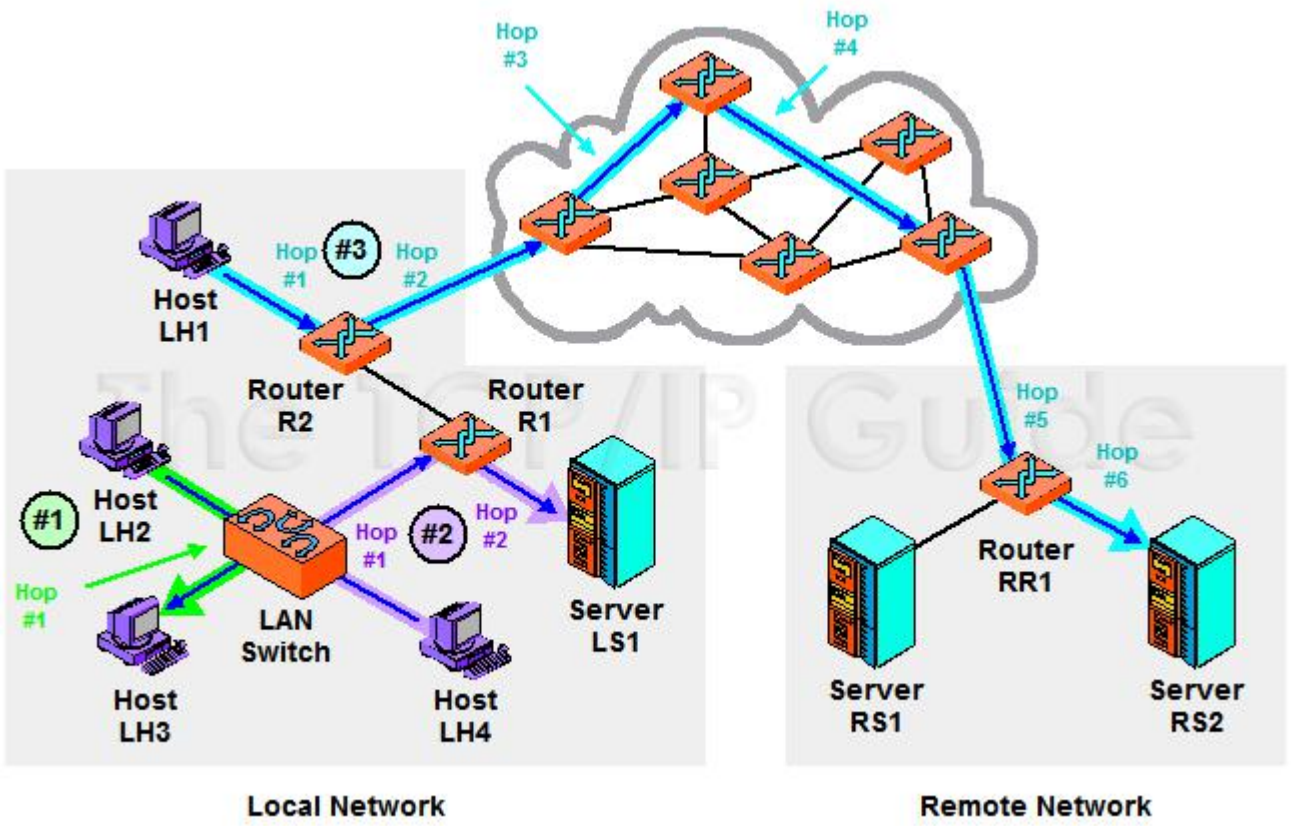
缺点

- 网络管理复杂
- 性能下降
- 重新修改校验和
- 客户端缺乏公网 IP 导致功能缺失
- 某些应用层协议由于传递网络层信息而功能受限

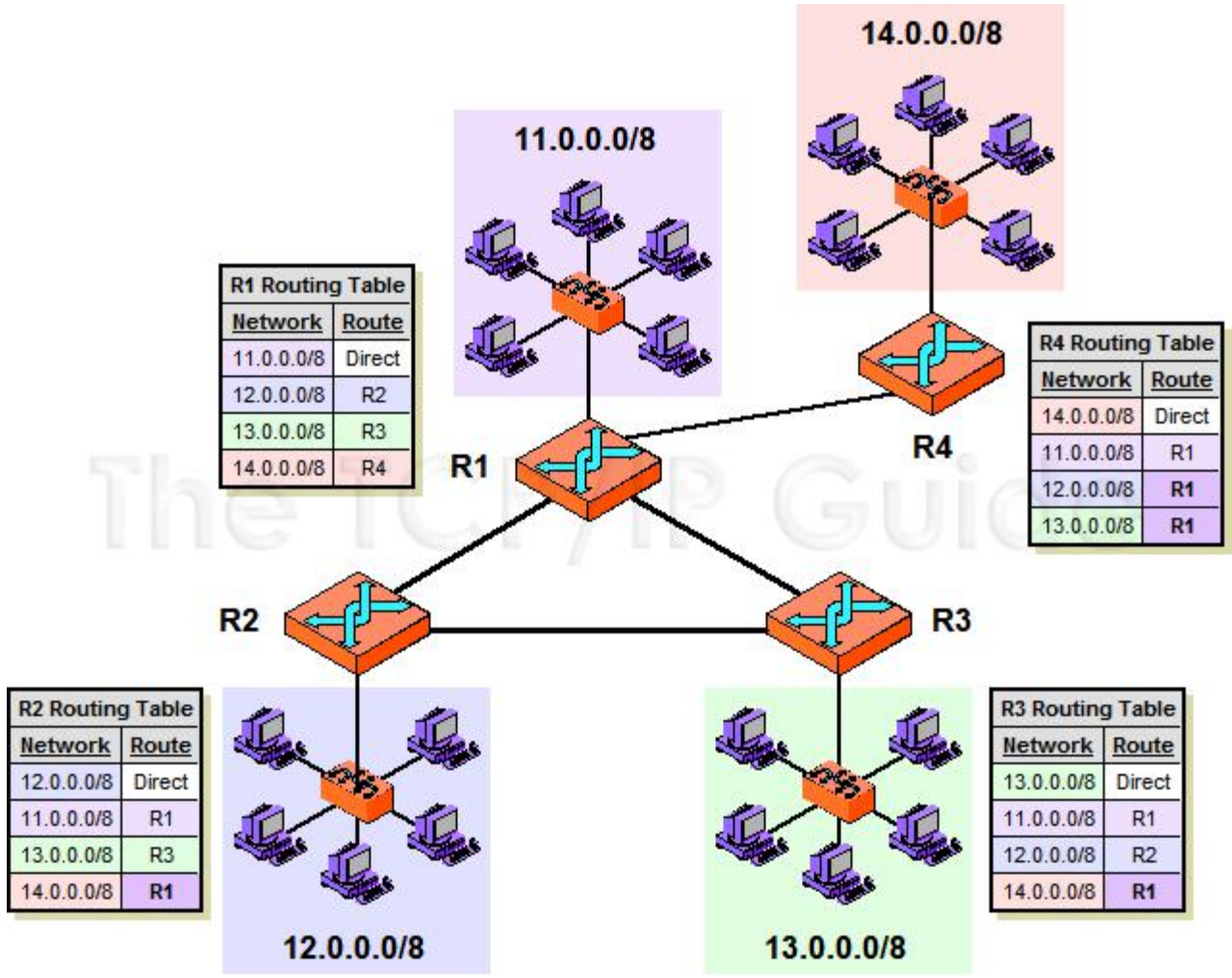
第 6 课 IP 选路协议

如何传输 IP 报文?

- 直接传输
- 本地网络间接传输
  - 内部选路协议
    - RIP
    - OSPF
- 公网间接传输
  - 外部选路协议
    - BGP

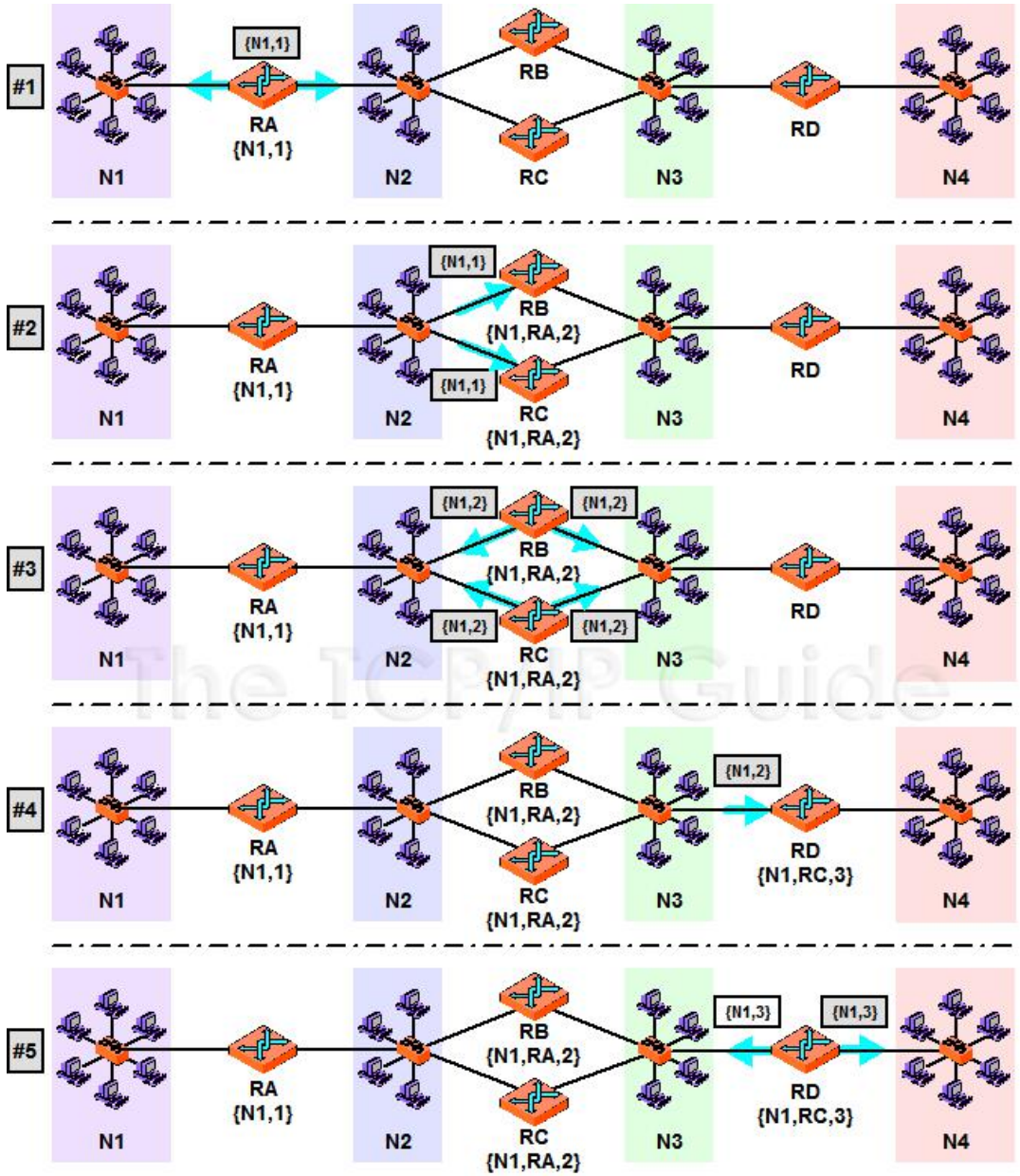


路由表 routing table



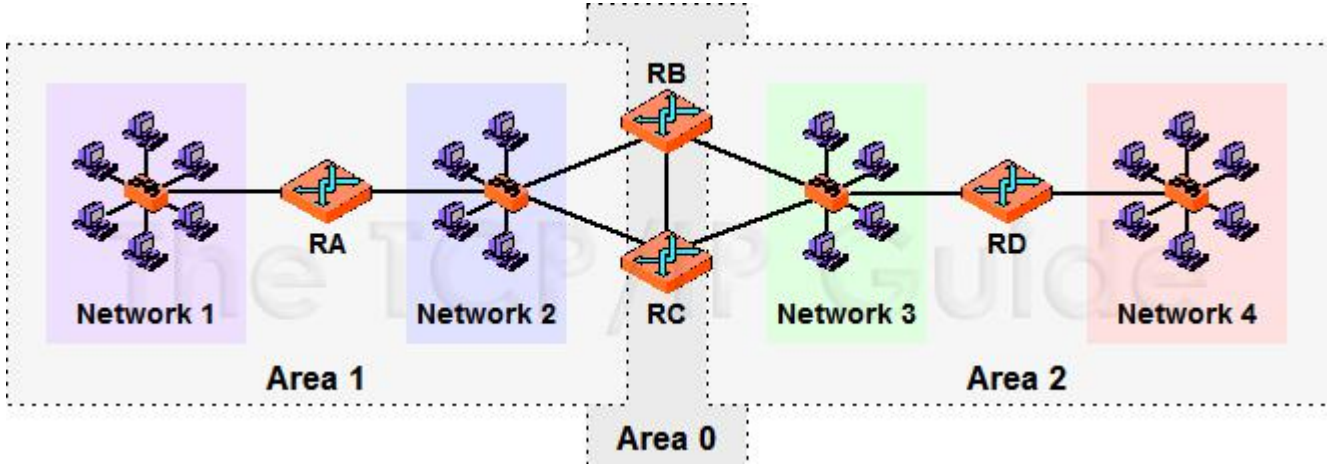
RIP 内部选路协议

- Routing Information Protocol
- 特点
  - 基于跳数确定路由
  - UDP 协议向相邻路由器通知路由表
- 问题
  - 跳数度量
  - 慢收敛
  - 选路环路



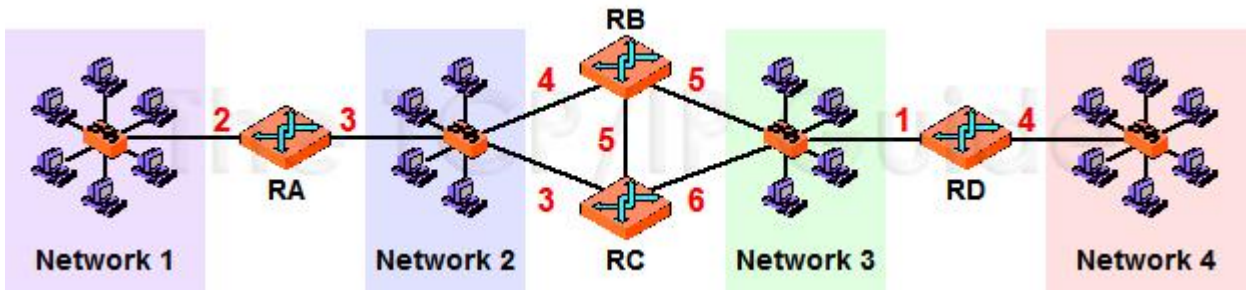
OSPF 内部选路协议

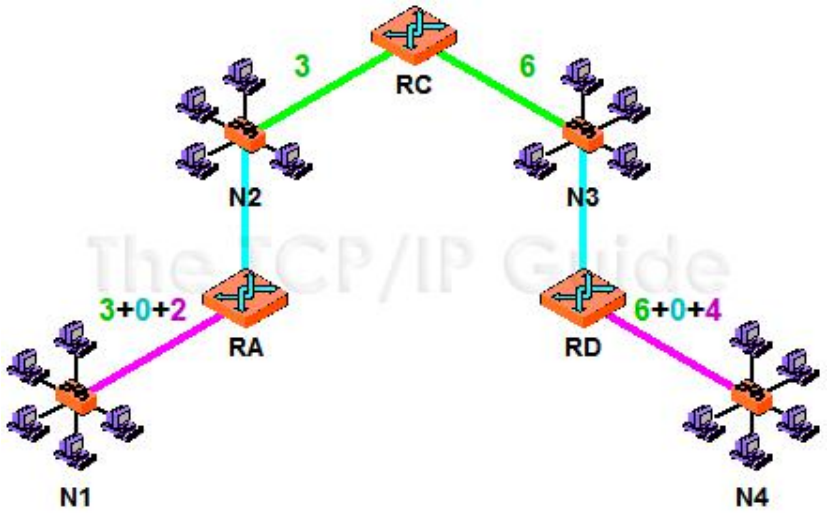
- Open Shortest Path First
- 多级拓扑结构：同级拓扑中的每台路由器都具有最终相同的数据信息（LSDB）
  - 直接使用 IP 协议（协议号 0x06 为 TCP，0x11 为 UDP，而 0x59 为 OSPF）传递路由信息



OSPF 最短路径树

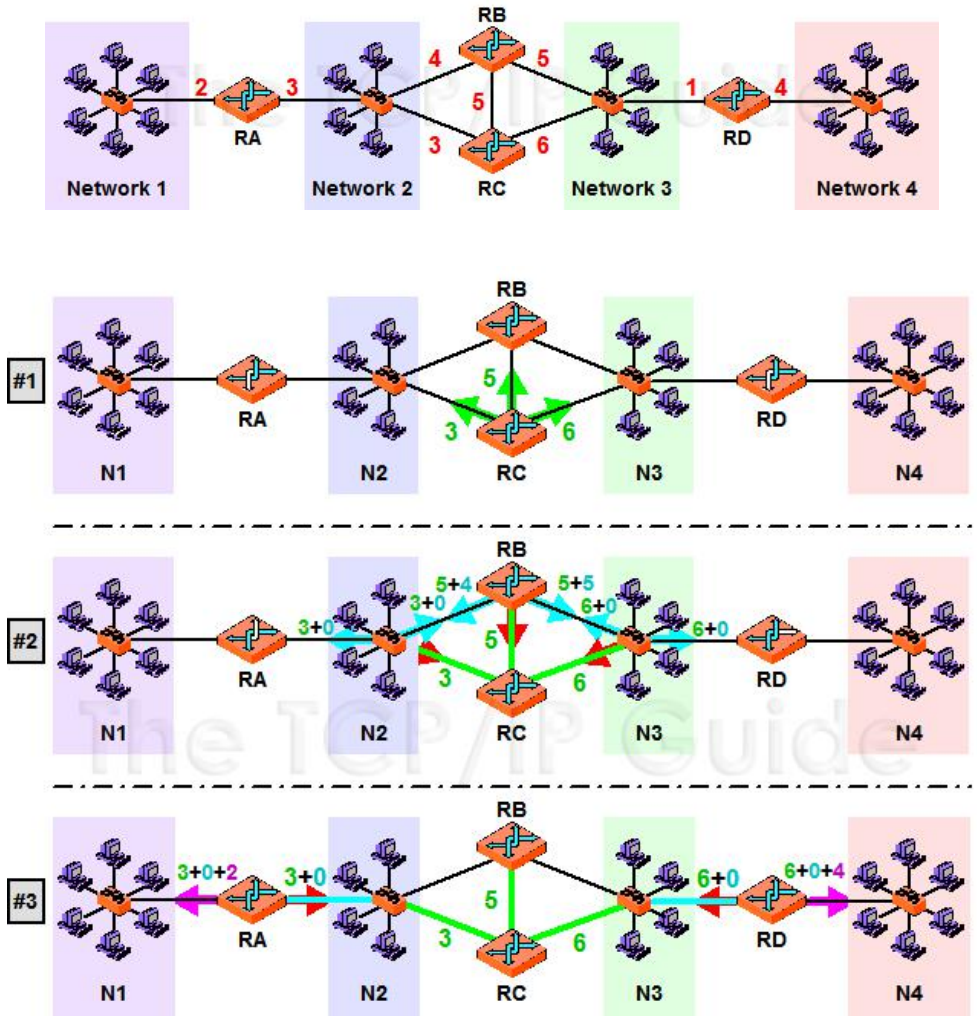
- 只有路由器到达网络有开销
  - 网络到达路由器没有开销
- RC 的最短路径树





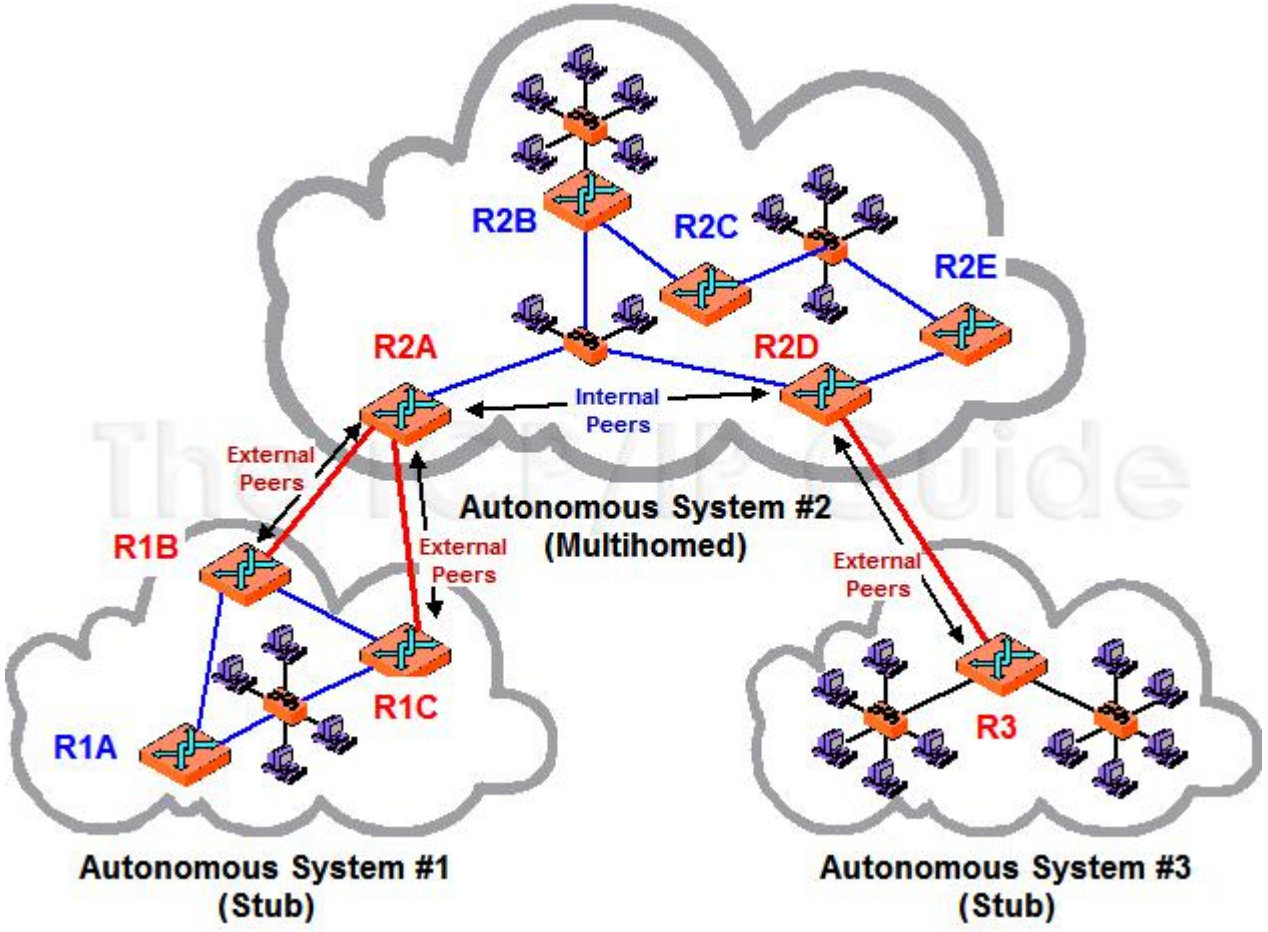
RC 构造最短路径树

1. 第一级：RC 直达设备
   - N2：3
   - N3：6
   - RB：5
2. 第二级：间隔 1 跳设备
   - 经过 N2 到 RA：3
   - 经过 N3 到 RD：6
3. 第三级：间隔 2 跳设备
   - 经过 N2、RA 到 N1：5
   - 经过 N3、RD 到 N4：10



BGP：Border Gateway Protocol

- 网络间的选路协议
- 存放网络间信息 RIB
  - Routing Information Base
  - TCP 协议传输 RIB 信息
- E(External)BGP
  - 外部对等方传输使用
- I(Internal)BGP
  - 内部对等方传输使用



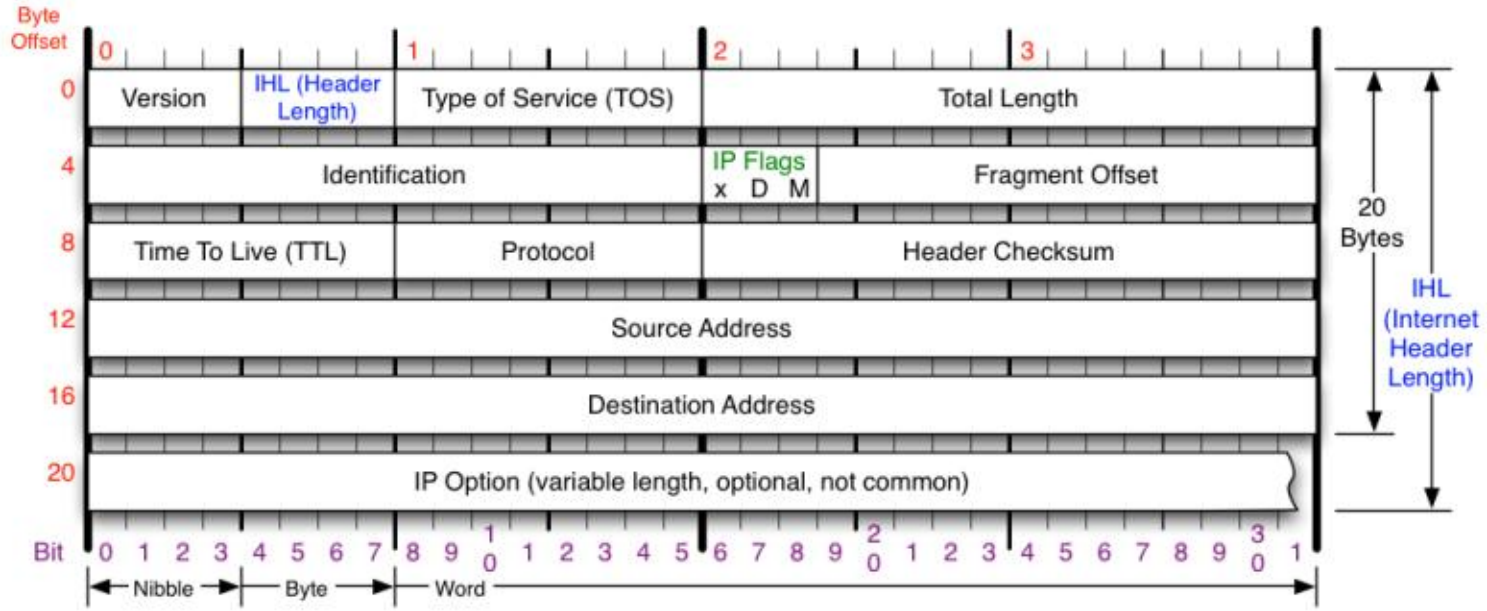
路由跟踪工具

- Windows: tracert
- Linux/Mac: traceroute

第 7 课 MTU 与 IP 报文分片

IP 报文格式

- IHL：头部长度，单位字
- TL：总长度，单位字节
- Id：分片标识
- Flags：分片控制
  - DF 为1：不能分片
  - MF 为1：中间分片
- FO：分片内偏移，单位 8 字节
- TTL：路由器跳数生存期
- Protocol：承载协议
- HC：校验和



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

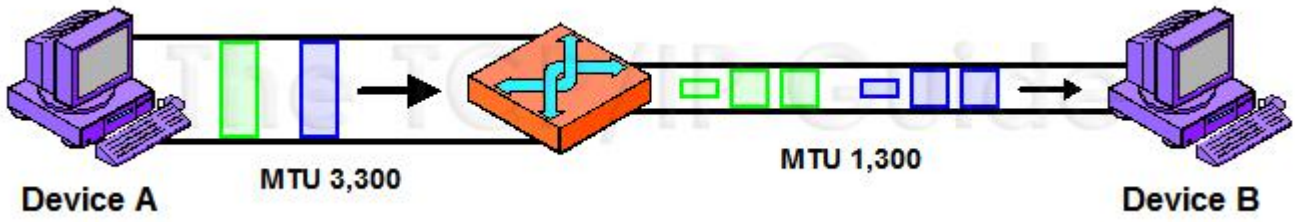
x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

MTU（Maximum Transmission Unit）分片

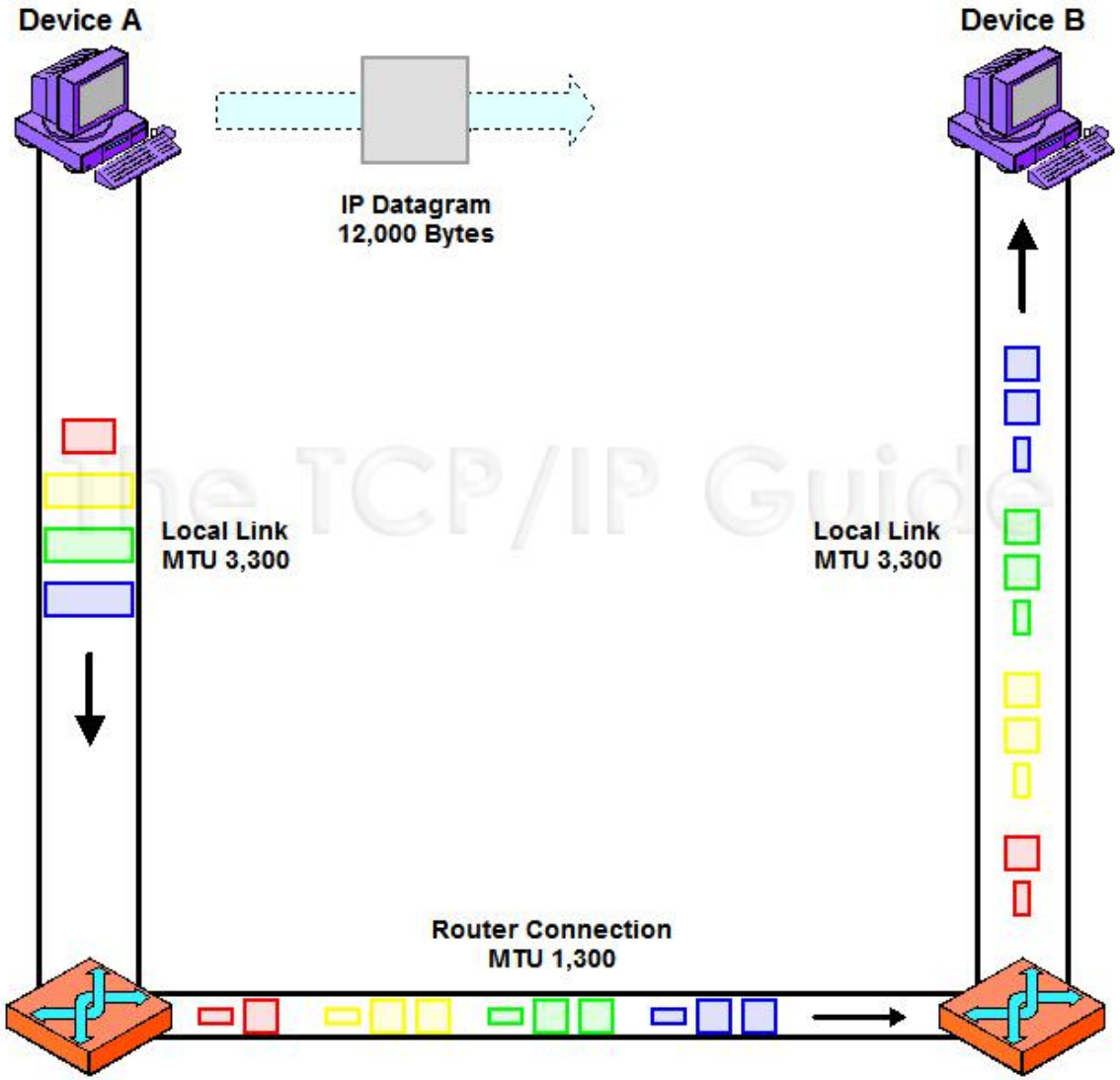
- MTU 最大传输单元（ RFC791 ： >=576 字节）
- ping 命令
  - -f：设置 DF 标志位为 1
  - -l：指定负载中的数据长度



常见网络 MTU

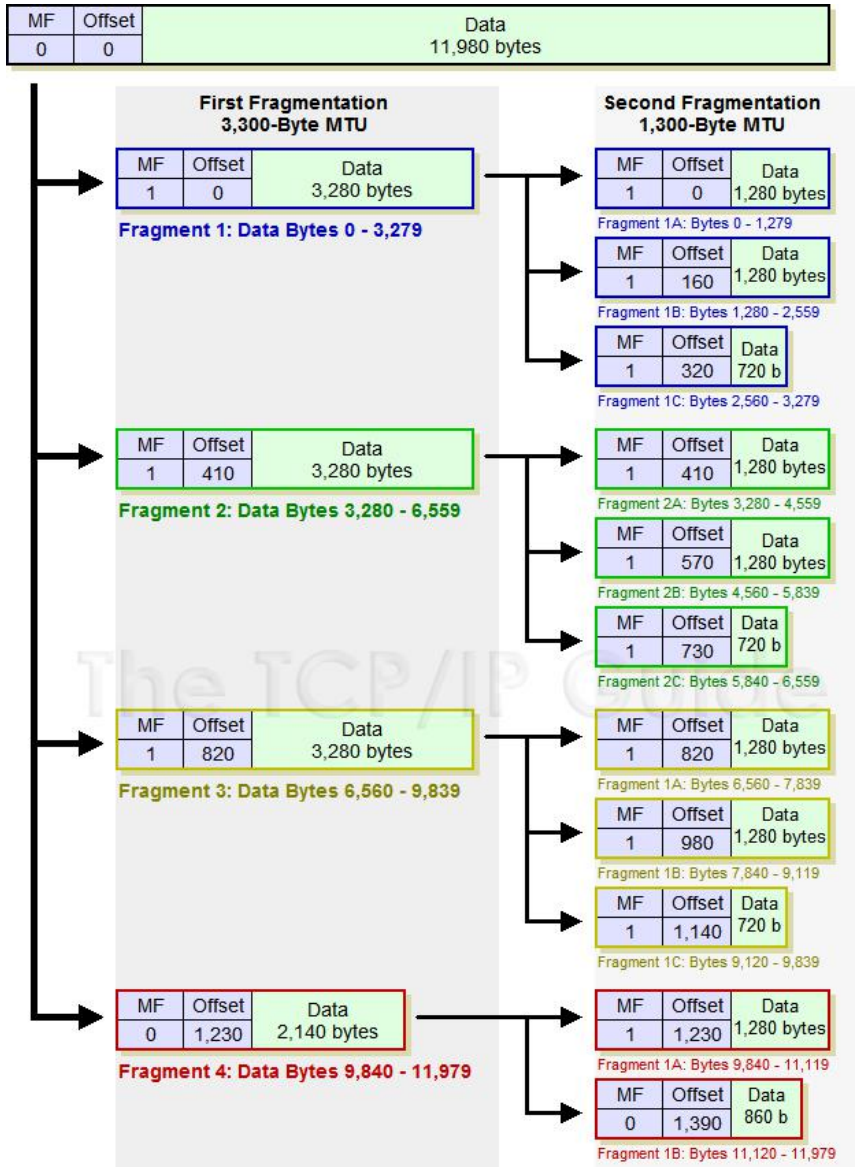
网络	MTU(Byte)
超通道	65535
16Mb/s 令牌环	17914
4Mb/s 令牌环	4464
FDDI	4352
以太网	1500
IEEE 802.3/802.2	1492
X.25	576
点对点（低时延）	296

可能出现多次分片


Device A
Device B
IP Datagram
12,000 Bytes
Local Link
MTU 3,300
Local Link
MTU 3,300
Router Connection
MTU 1,300

IP 分片示例

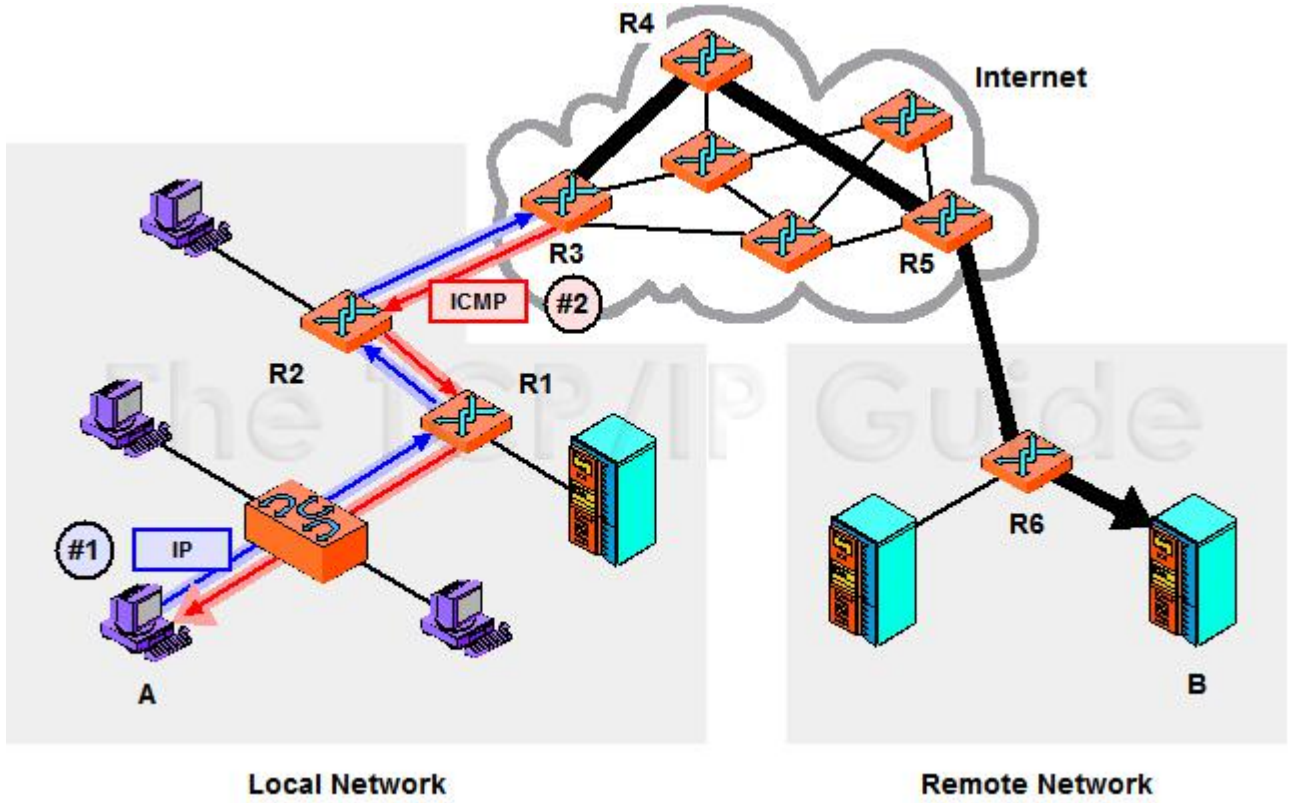
- 分片主体
  - 源主机
  - 路由器
- 重组主体
  - 目的主机



第 8 课 IP 协议的助手：ICMP 协议

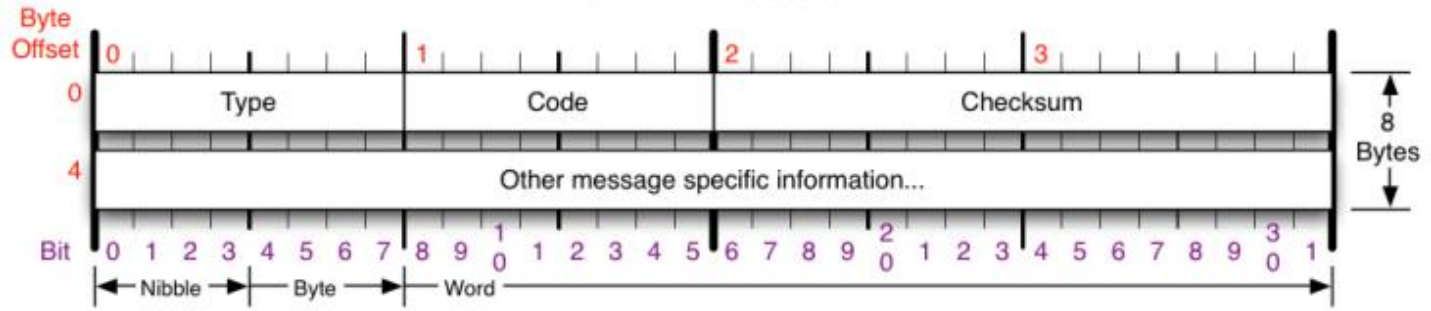
ICMP： Internet Control Message Protocol

- RFC792
- IP 助手
  - 告知错误
  - 传递信息



ICMP协议格式

- 承载在 IP 之上
- 组成字段
  - 类型
  - 子类型
  - 校验和



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

Checksum of ICMP header

RFC 792

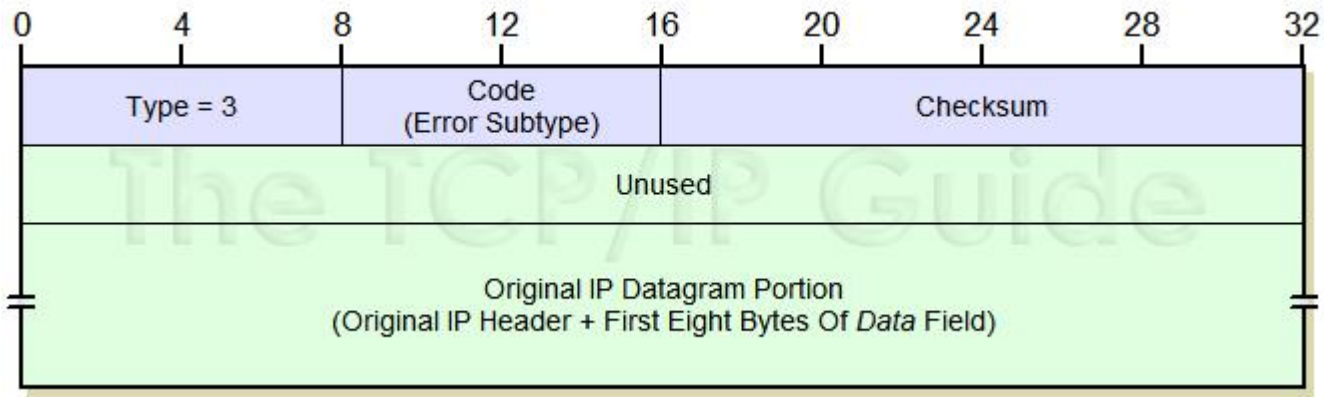
Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

ICMPv4 报文类型

- 错误报文
  - 3：目的地不可达
  - 4：发生拥塞，要求发送方降低速率
  - 5：告诉主机更好的网络路径
  - 11：路径超出 TTL 限制
  - 12：其他问题
- 信息报文
  - 0：连通性测试中的响应
  - 8：连通性测试中的请求
  - 9：路由器通告其能力
  - 10：路由器通知请求
  - 13：时间戳请求
  - 14：时间戳应答
  - 17：掩码请求
  - 18：掩码应答
  - 30：Traceroute

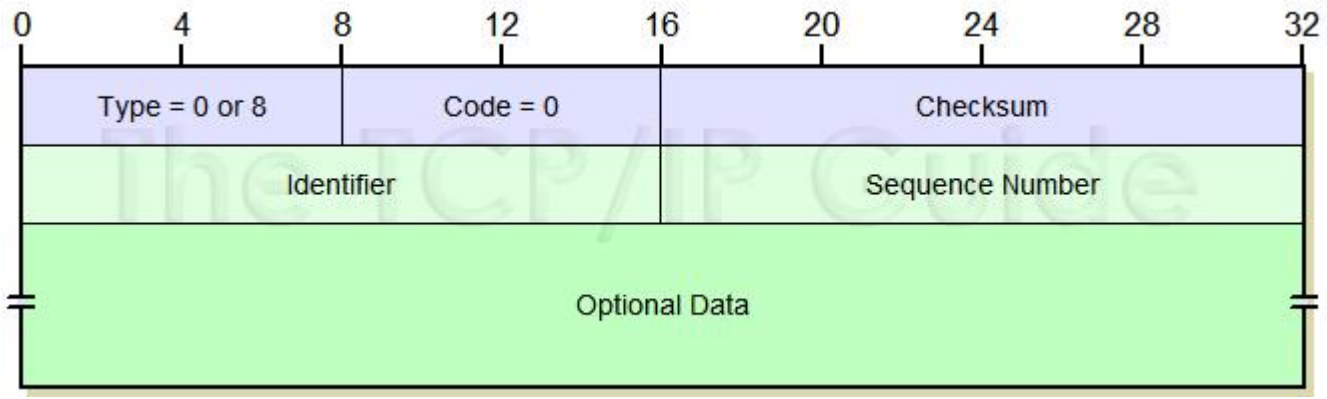
目的地不可达报文：Type=3

- 常用子类型 Code
  - 0：网络不可达
  - 1：主机不可达
  - 2：协议不可达
  - 3：端口不可达
  - 4：要分片但 DF 为1
  - 10：不允许向特定主机通信
  - 13：管理受禁



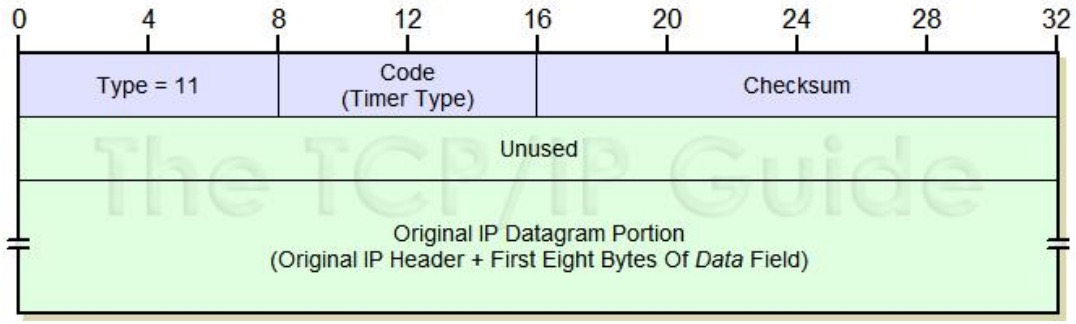
Echo 与 Echo Reply 报文

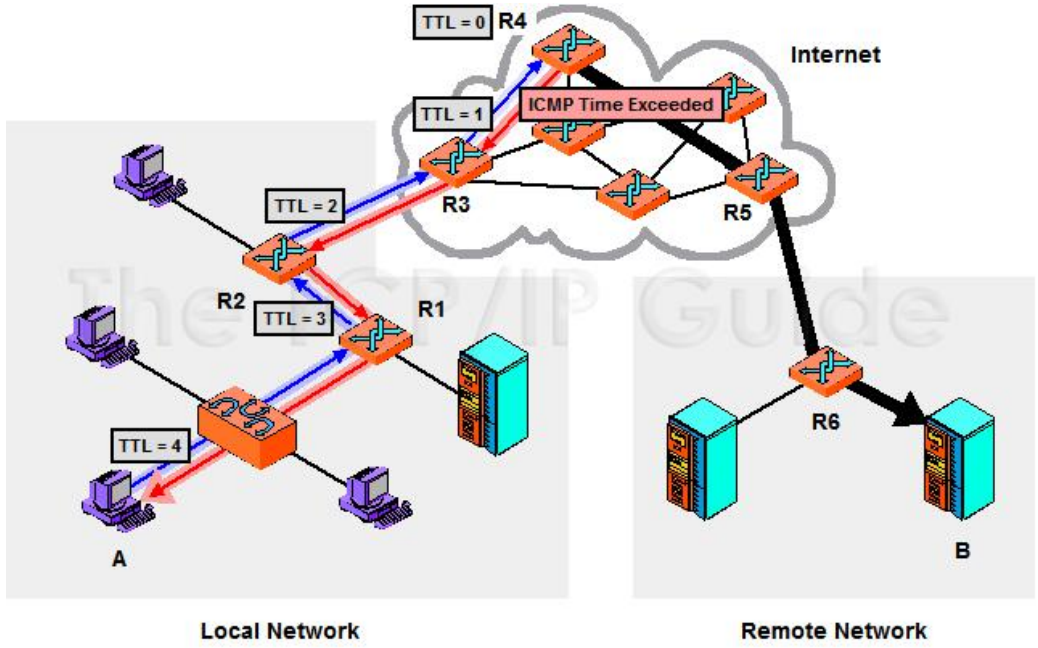
- ping 联通性测试



TTL 超限：Type=11

- traceroute/tracert

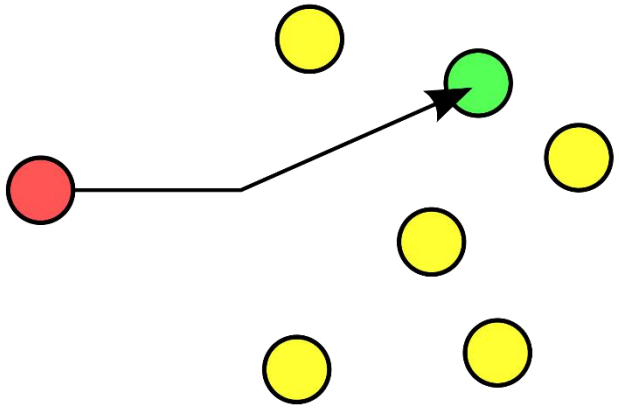




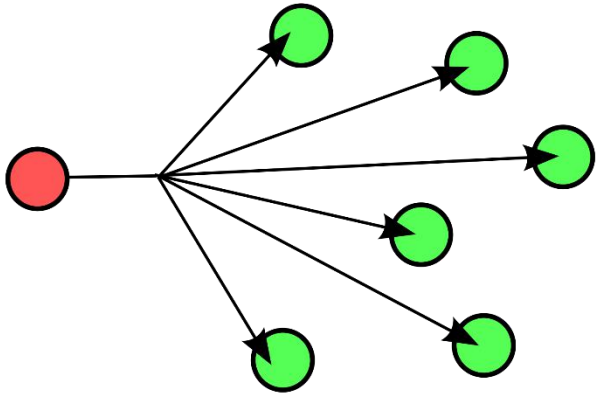
第 9 课 多播与 IGMP 协议

广播与组播

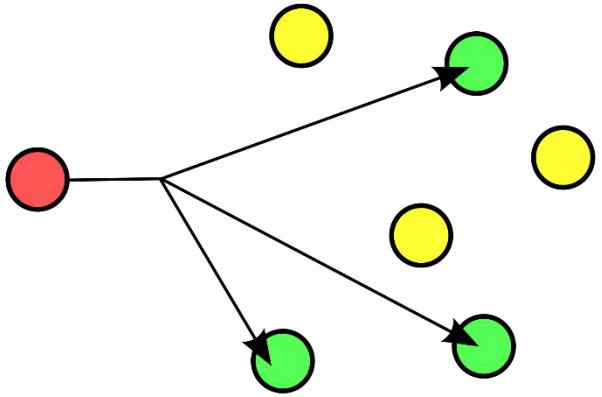
- 单播



- 广播



- 组播



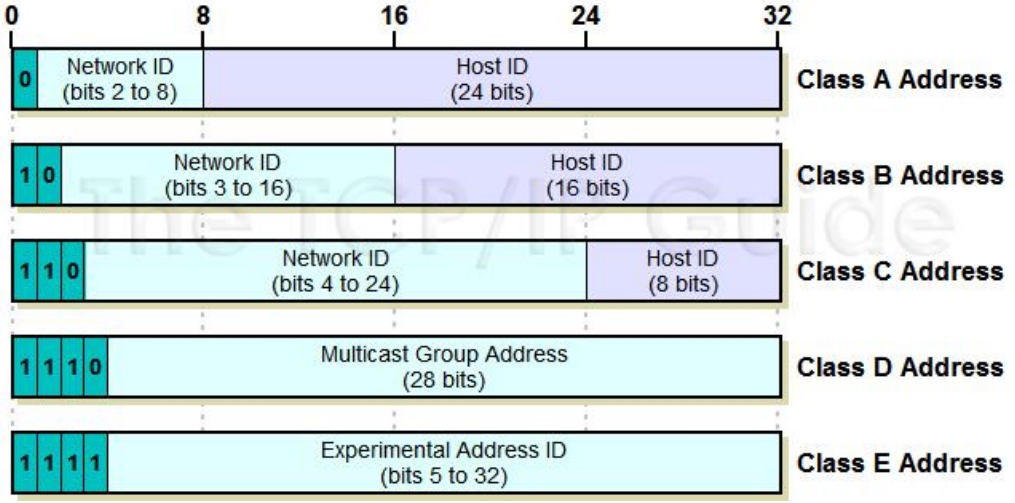
广播地址

- 以太网地址：ff:ff:ff:ff:ff:ff
- IP 地址

网络号	主机号	A 类示例	B 类示例	C 类示例	含义
网络号	主机号	77.91.215.5	154.3.99.6	227.82.157.160	指定某个主机
网络号	全 0	77.0.0.0	154.3.0.0	227.82.157.0	指定某个网络
全 0	主机号	0.91.215.5	0.0.99.6	0.0.0.160	指定当前所属网络下的某个主机
全 0	全 0		0.0.0.0		指定自己的默认 IP 地址
网络号	全 1	77.255.255.255	154.3.255.255	227.82.157.255	指定某个网络下的所有主机，用于广播
全 1	全 1		255.255.255.255		所有主机

组播IP地址

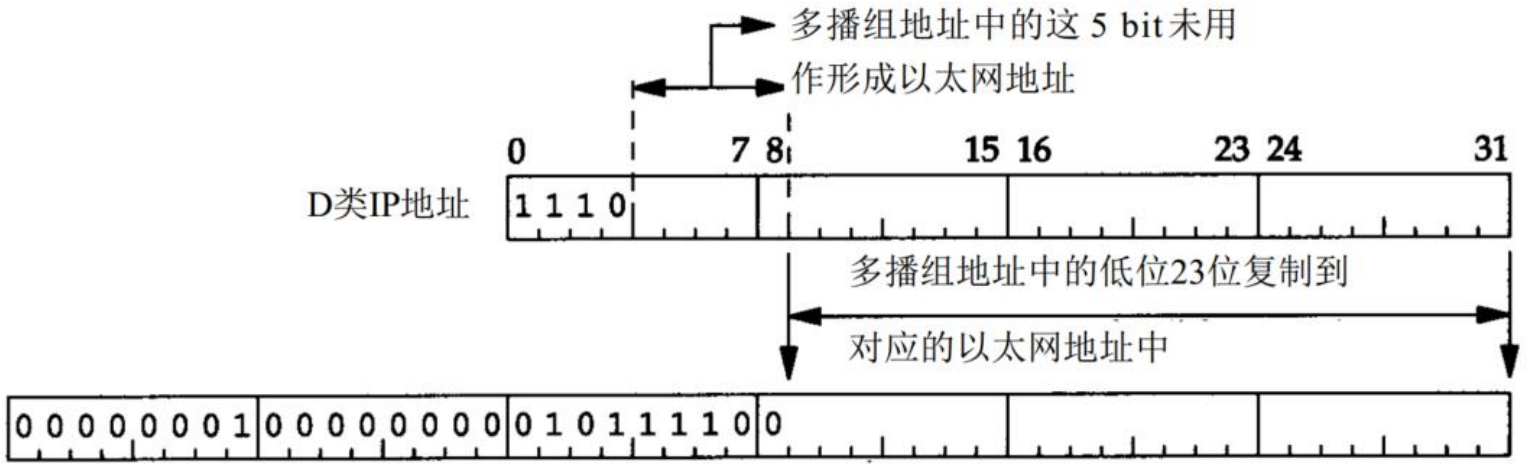
- 预留组播地址
  - 224.0.0.1：子网内的所有系统组
  - 224.0.0.2：子网内的所有路由器组
  - 224.0.1.1：用于 NTP 同步系统时钟
  - 224.0.0.9：用于 RIP-2 协议



IP 地址类别	首字节	网络号 Bit 数	主机号 Bit 数	理论地址范围	预期用途
A 类地址	0xxx xxxx	8	24	1.0.0.0 -126.255.255.255	特大网络的单播传输
B 类地址	10xx xxxx	16	16	128.0.0.0 -191.255.255.255	数千台中大型网络的单播传输
C 类地址	110x xxxx	24	8	192.0.0.0 -223.255.255.255	250 台主机以下小型网络的单播传输
D 类地址	1110 xxxx	n/a	n/a	224.0.0.0 -239.255.255.255	IP 组播
E 类地址	1111 xxxx	n/a	n/a	240.0.0.0 - 255.255.255.255	预留实验用

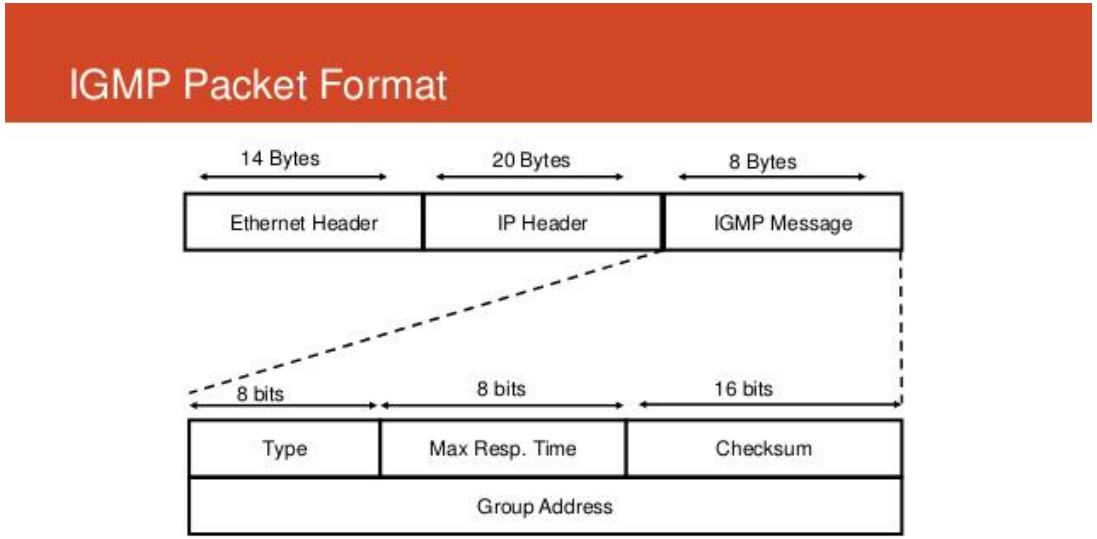
组播以太网地址

- 以太网地址：01:00:5e:00:00:00 到 01:00:5e:7f:ff:ff
- 低 23 位：映射 IP 组播地址至以太网地址
  - 224.0.0.22: 11100000 00000000 00000000 00010110
  - 01:00:5e:00:00:16: 0000001 00000000 01011110 00000000 00000000 00010110

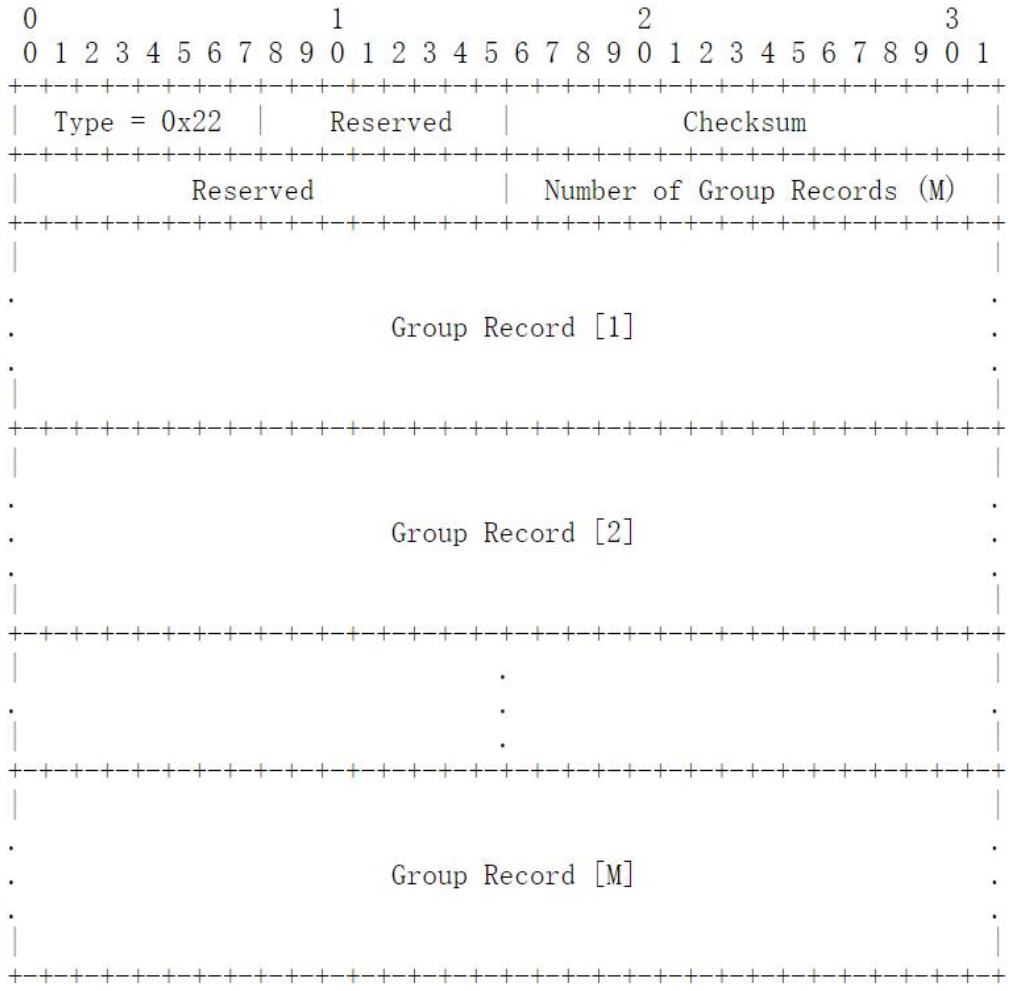


IGMP（Internet Group Management Protocol）协议

- Type 类型
  - 0x11 Membership Query [RFC3376]
  - 0x22 Version 3 Membership Report [RFC3376]
  - 0x12 Version 1 Membership Report [RFC-1112]
  - 0x16 Version 2 Membership Report [RFC-2236]
  - 0x17 Version 2 Leave Group [RFC-2236]

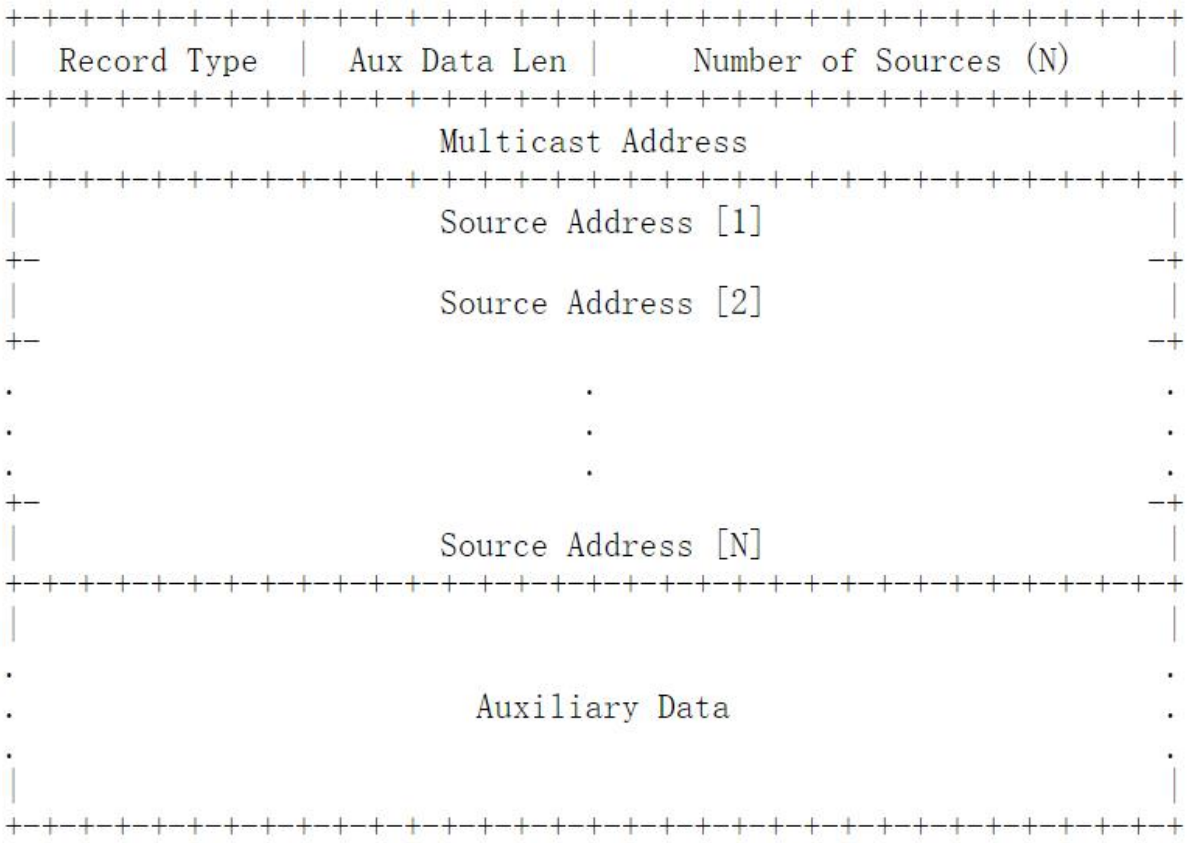


0x22 Membership Report：状态变更通知



Group Record 格式

- Record Type 类型
  - 当前状态
    - 1: MODE_IS_INCLUDE
    - 2: MODE_IS_EXCLUDE
  - 过滤模式变更（如从 INCLUDE 变为 EXCLUDE）
    - 3: CHANGE_TO_INCLUDE
    - 4: CHANGE_TO_EXCLUDE
  - 源地址列表变更（过滤模式同时决定状态）
    - 5: ALLOW_NEW_SOURCES
    - 6: BLOCK_OLD_SOURCES



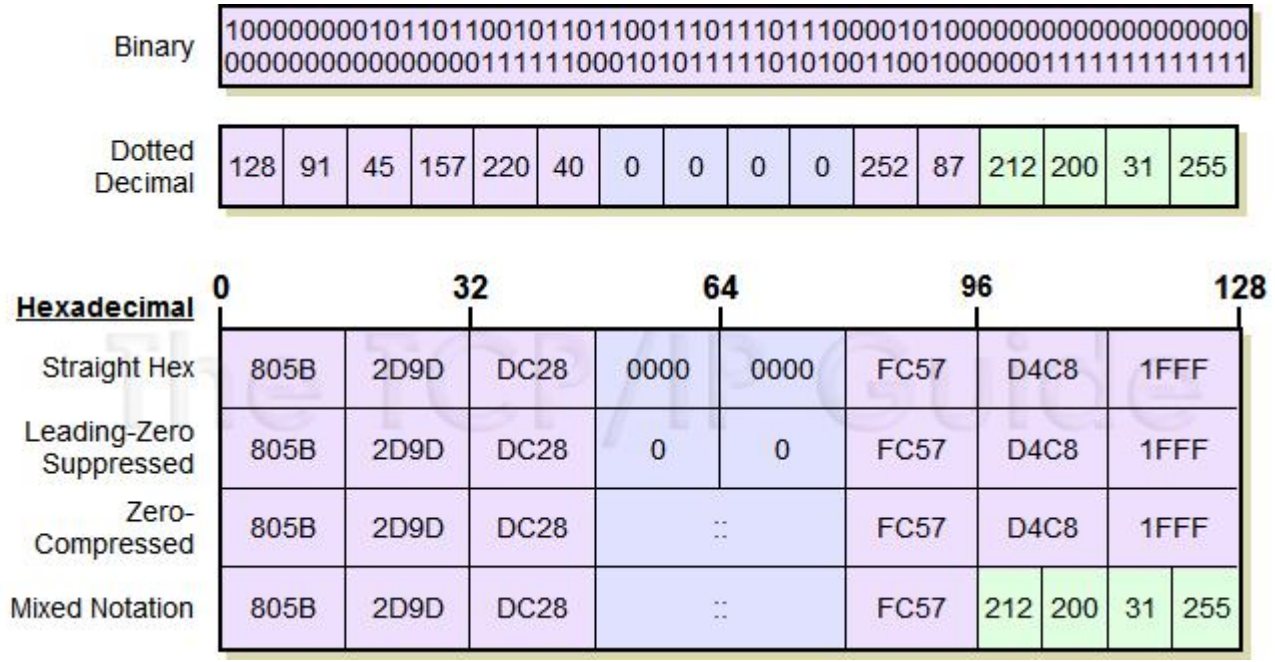
第 10 课 支持万物互联的 IPv6 地址

IPv6 目的

- 更大的地址空间：128 位长度
- 更好的地址空间管理
- 消除了 NAT 等寻址技术
- 更简易的 IP 配置管理
- 优秀的选路设计
- 更好的多播支持
- 安全性
- 移动性

IPv6 地址的冒分十六进制表示法

- 首零去除
- 零压缩
  - FF00:4501:0:0:0:0:0:32
    - FF00:4501::32
  - 805B:2D9D:DC28:0:0:FC57:0:0
    - 805B:2D9D:DC28::FC57:0:0
    - 805B:2D9D:DC28:0:0:FC57::
  - 环回地址0:0:0:0:0:0:0:1
    - ::1

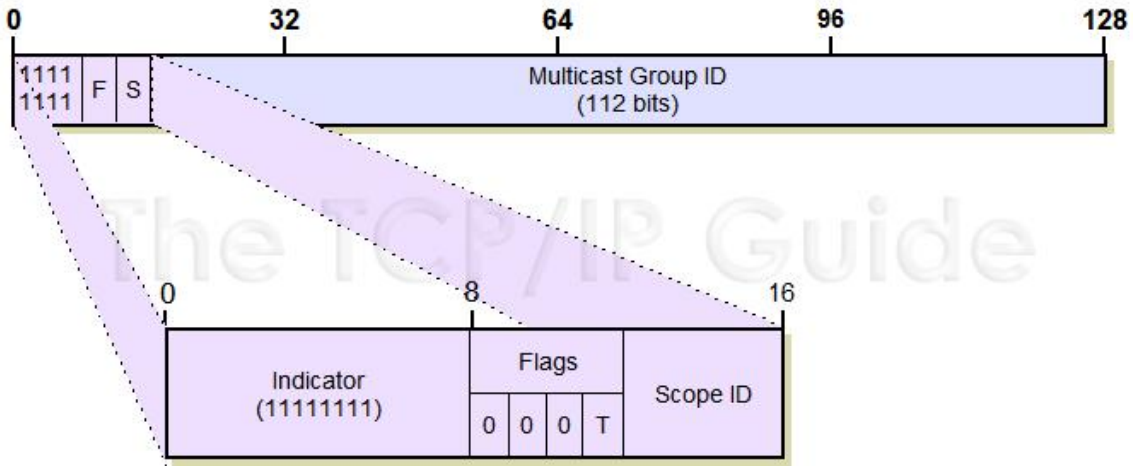


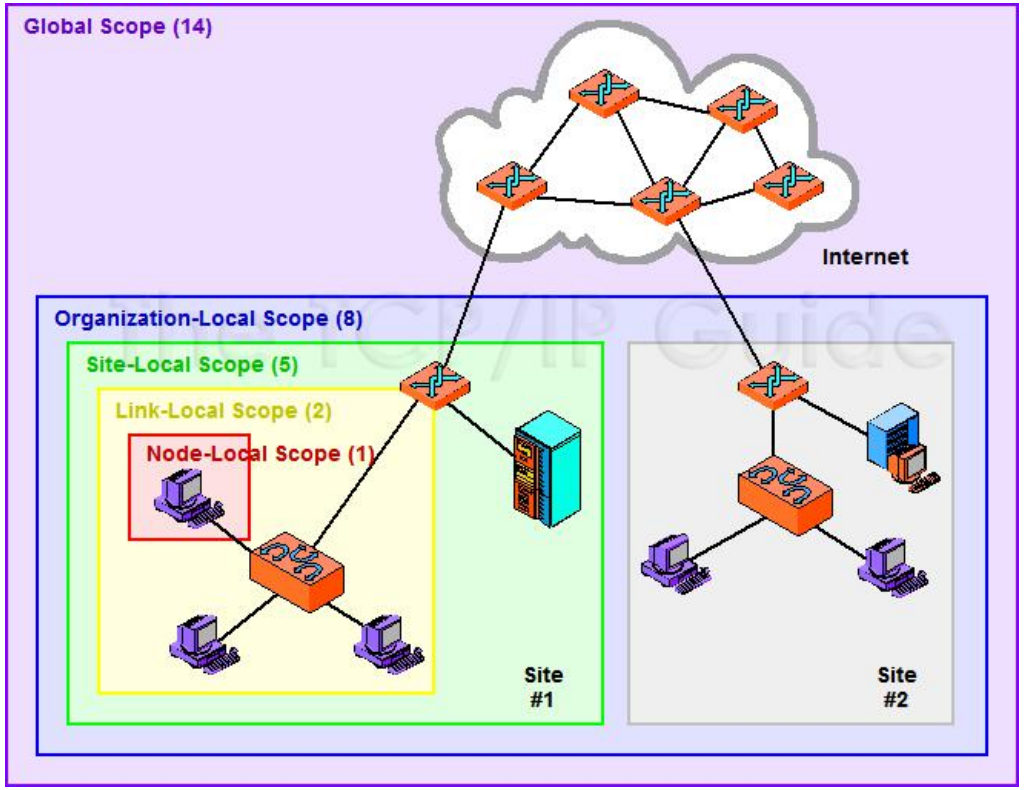
IPv6 地址分布

起始比特	占所有 IPv6 地址的比重	分配情况
0000 0000	1/256	未分配 (含特殊地址)
0000 0001	1/256	未分配
0000 001	1/128	为 NSAP 地址保留
0000 01	1/64	未分配
0000 1	1/32	未分配
0001	1/16	未分配
001	1/8	全局单播地址
010	1/8	未分配
011	1/8	未分配
100	1/8	未分配
101	1/8	未分配
110	1/8	未分配
1110	1/16	未分配
1111 0	1/32	未分配
1111 10	1/64	未分配
1111 110	1/128	未分配
1111 1110 0	1/512	未分配
1111 1110 10	1/1024	链路本地单播地址
1111 1110 11	1/1024	场点本地单播地址
1111 1111	1/256	多播地址

不同作用域下的多播

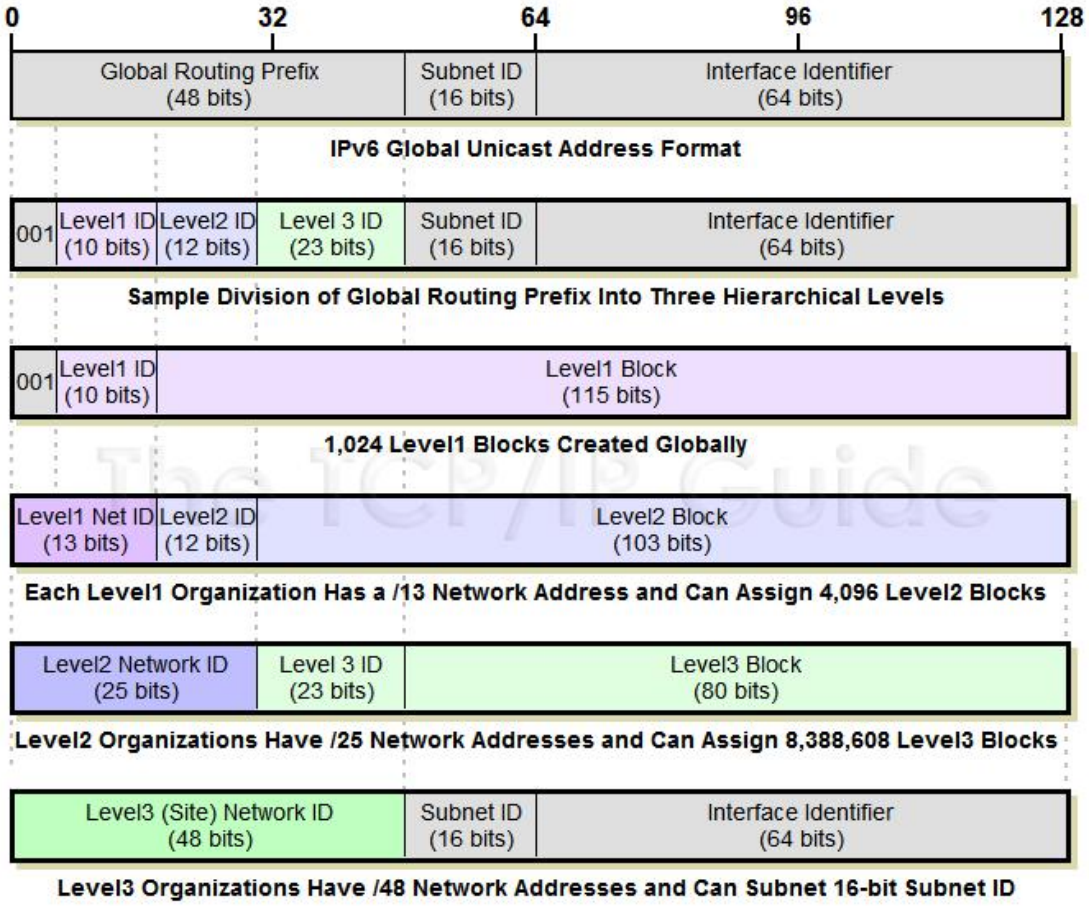
- Scope ID
  - 14：全局作用域
  - 8：组织作用域
  - 5：场点作用域
  - 2：本地链路作用域
  - 1：本机作用域





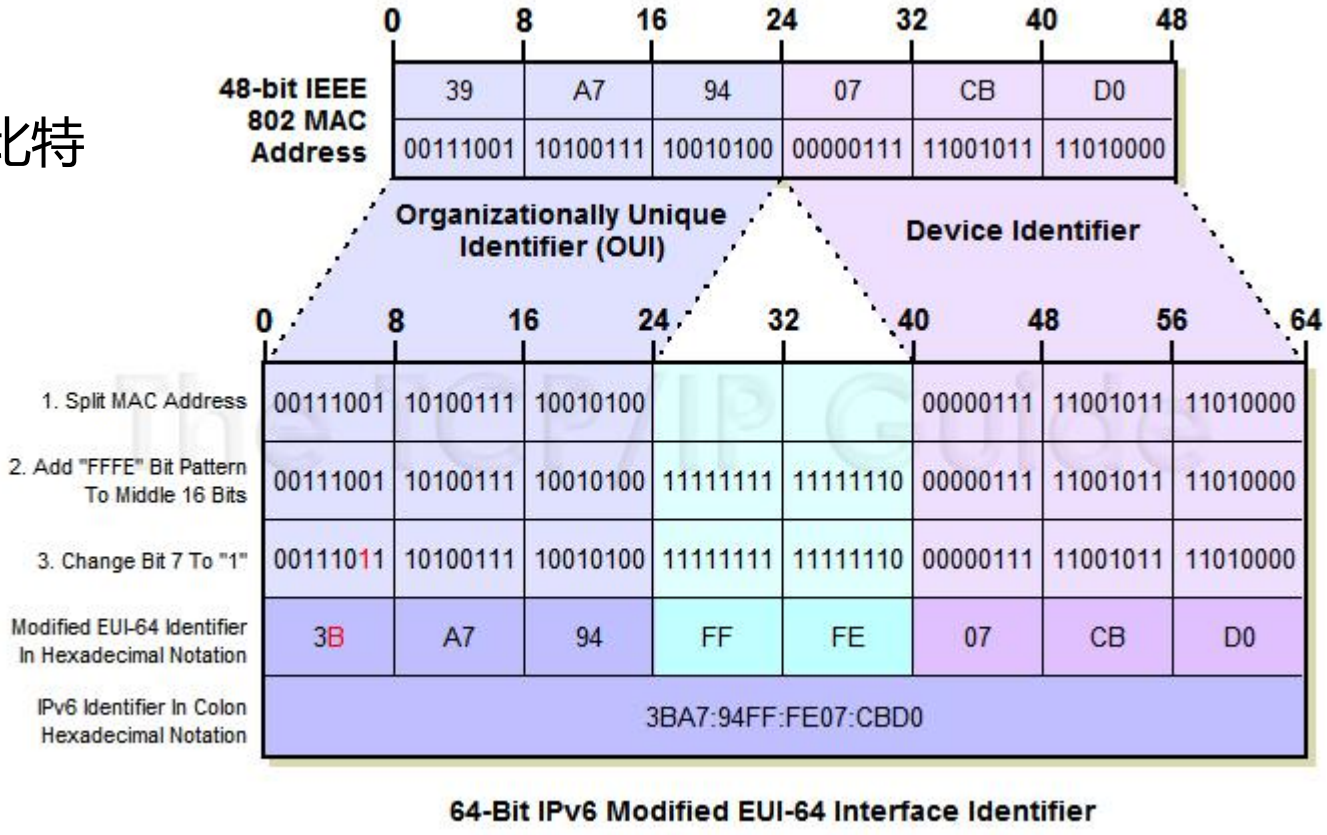
网络地址与主机地址

- 全局路由前缀：48
  - 可任意划分为多级
- 子网ID：16
  - 可任意划分为多级
- 接口ID：64
  - 直接映射 MAC 地址



IEEE802 48 位 MAC 地址映射主机地址（EUI-64）

- 取 OUI(组织唯一标识)放左 24 比特
- 中间 16 比特置为 FFFE
- 置 OUI 第 7 位为 1 表示全局

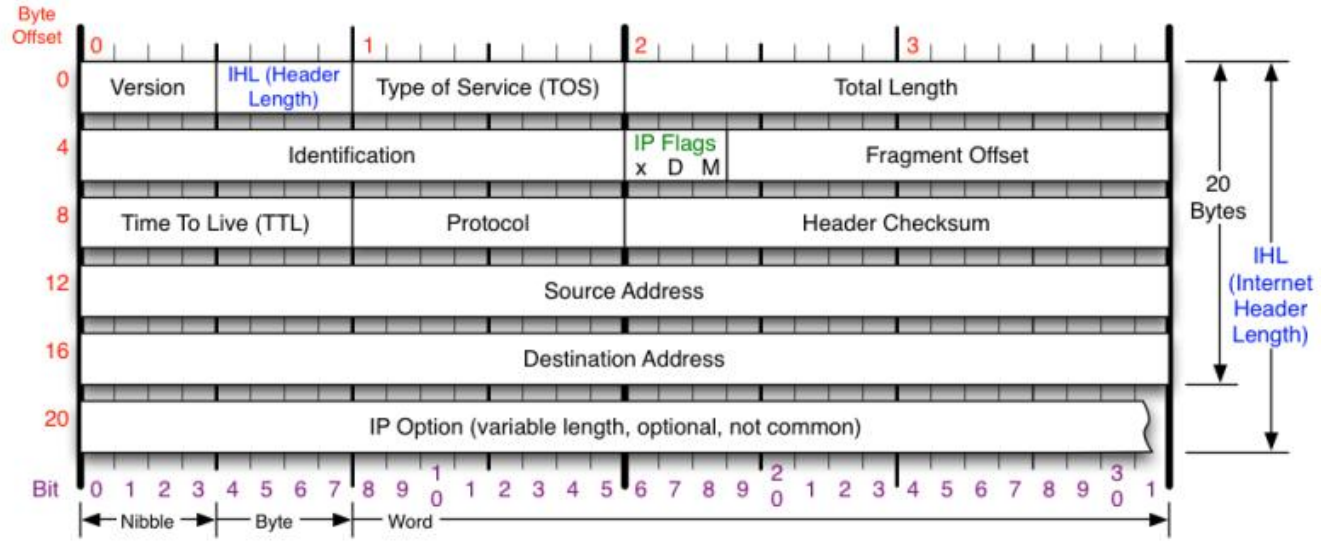


64-Bit IPv6 Modified EUI-64 Interface Identifier

第 11 课 IPv6 报文及分片

IP 头部

- Version：版本号
- ~~IHL：头部长度，单位字~~
- TL：总头部，单位字节
- ~~Id：分片标识~~
- ~~Flags：分片控制~~
  - ~~DF为1：不能分片~~
  - ~~MF为1：中间分片~~
- ~~FO：分片内偏移，单位 8 字节~~
- TTL：路由器跳数生存期
- Protocol：承载协议
- ~~HC：校验和~~



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

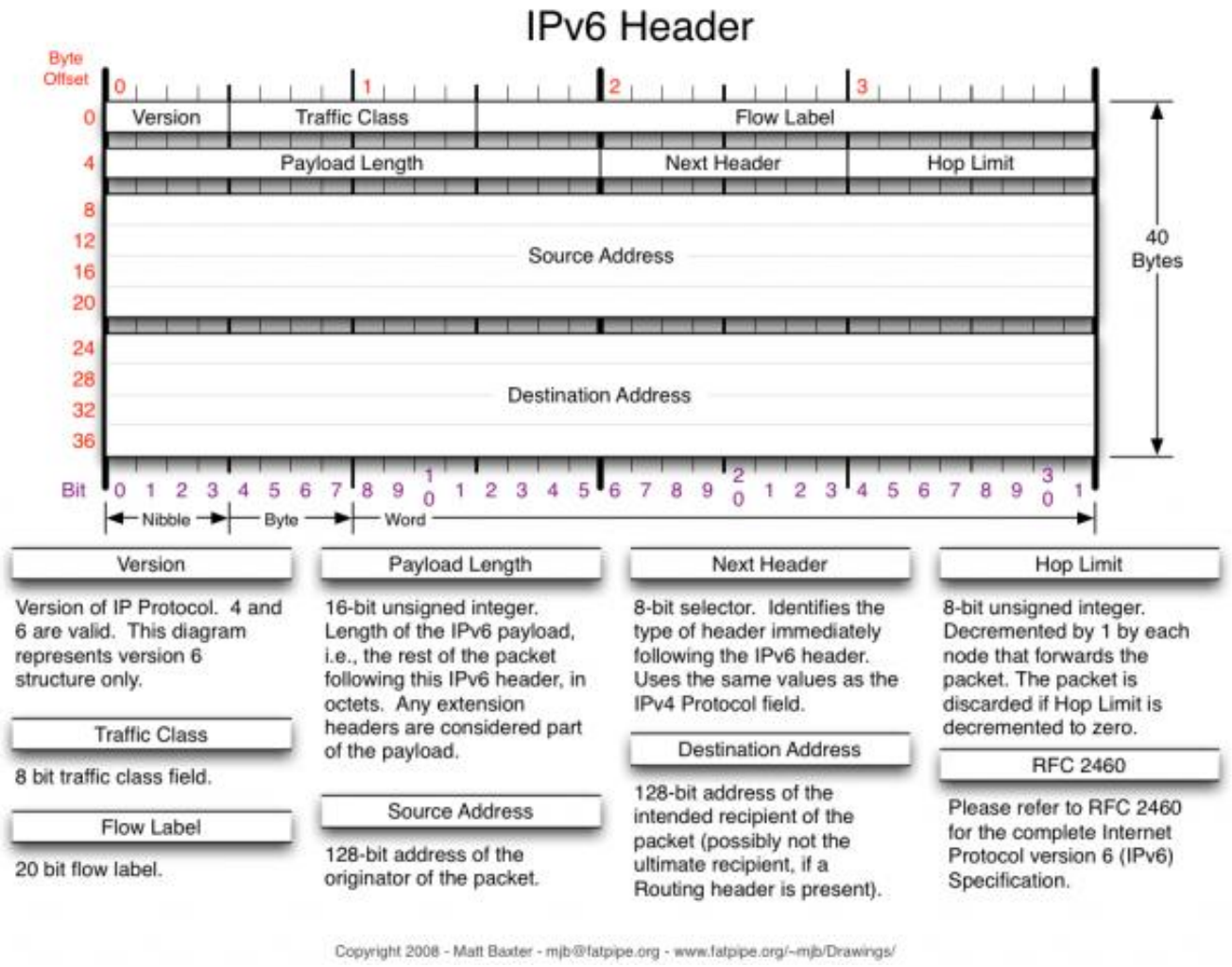
x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

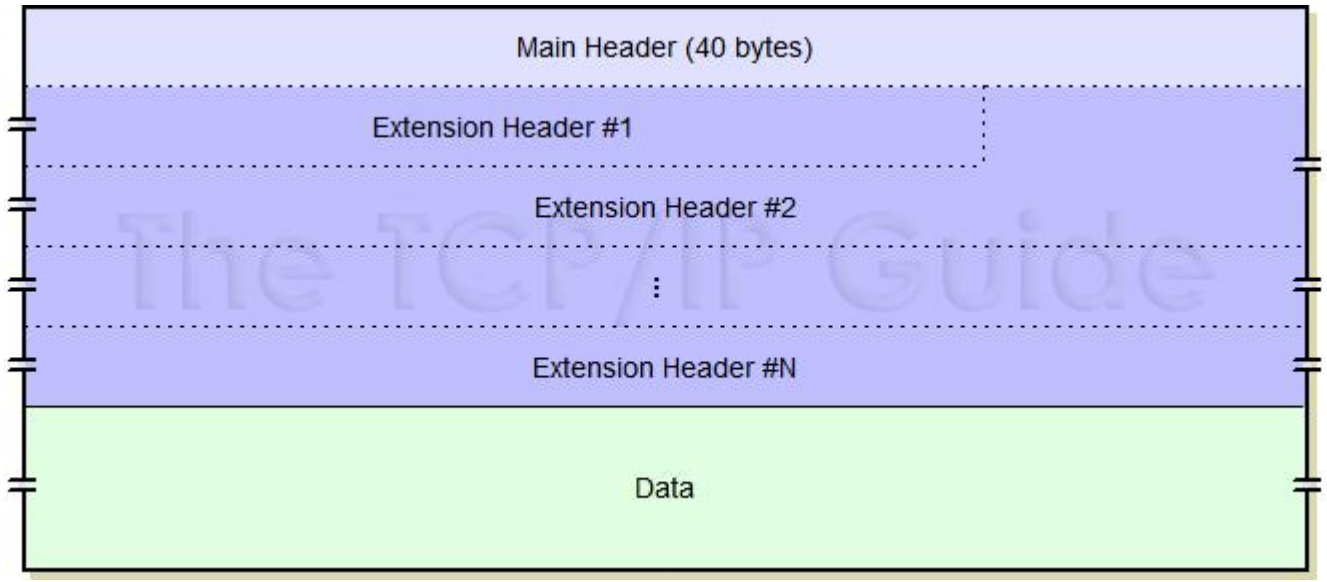
IPv6 主首部格式

- Version
- Traffic Class
  - TOS
- Flow Label：QOS 控制
- **Payload** Length
  - Total Length
- Next Header
- HopLimit
  - TTL
- 删除字段
  - IHL
  - Identification, Flags, Fragment Offset
  - Header Checksum



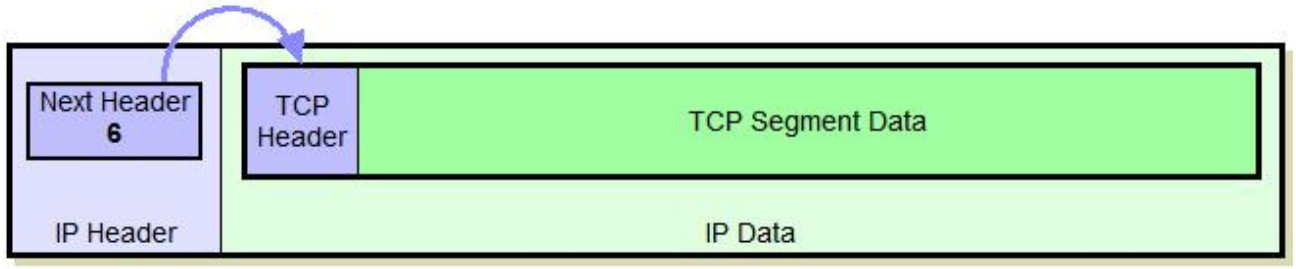
IPv6 报文格式

- 40 字节主首部
- 可选的扩展首部
- 数据

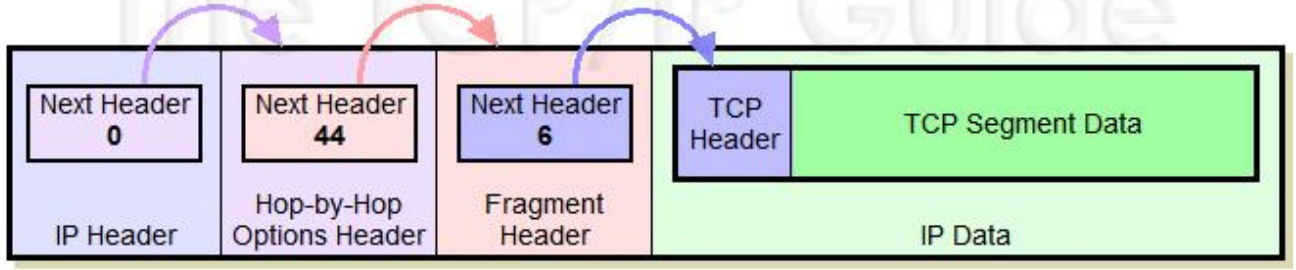


IPv6 首部链

Next Header	扩展首部名称	长度	RFC
0	逐跳选项	可变	2460
43	选 路	可变	2460
44	分片	8	2460
50	ESP	可变	2406
51	验证首部	可变	2402
60	目的地选项	可变	2460



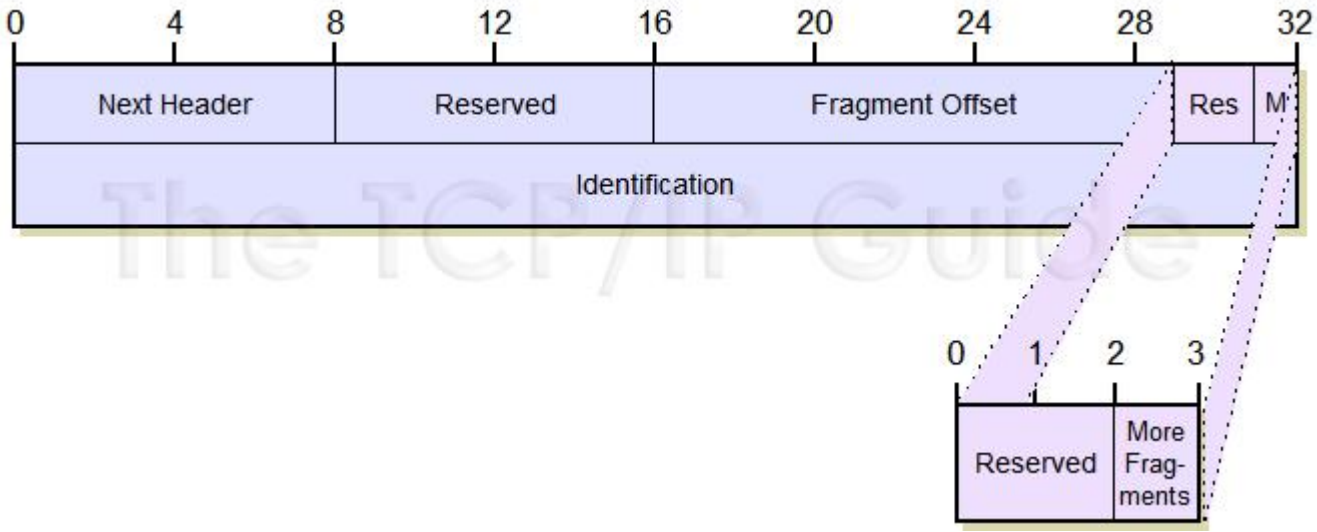
IPv6 Datagram With No Extension Headers Carrying TCP Segment



IPv6 Datagram With Two Extension Headers Carrying TCP Segment

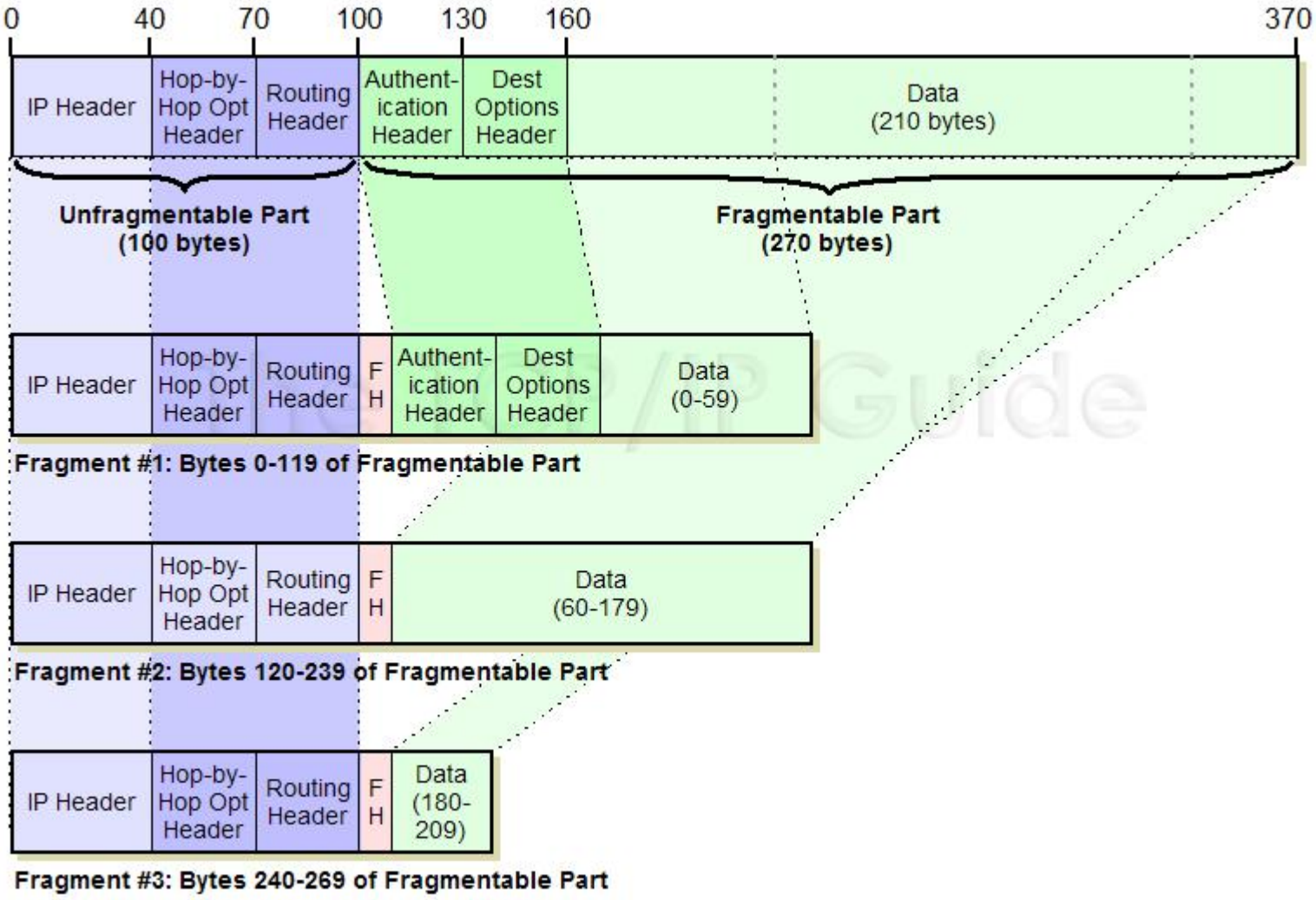
分片扩展首部

- Fragment Offset
  - 单位 8 字节
- MoreFragments
  - 0 表示最后分片
  - 1 表示非最后分片
- identification
  - 扩展 IPv4 相同头部至 4 字节



IPv6 的分片

- 不可分片部分
  - 主首部
  - 部分扩展首部
- 可分片部分
  - 数据
  - 部分扩展首部



第 12 课 从 wireshark 报文统计中找规律

报文统计

- 搭配“显示过滤器”使用
- 统计方式
  - 报文总体分布：捕获文件属性与数据包长度分布
  - 端点统计与会话统计
  - 协议分级统计
  - HTTP/HTTP2 等应用层协议统计
  - TCP 协议连接统计
  - IO 流统计与数据流统计

报文总体分布

- **捕获文件属性**
  - when：何时抓包
  - where：哪个 IP 接口在抓包
  - how：捕获过滤器是什么？
  - how much：多少报文？多少字节？多快速率？
- **报文长度分布：信息传输效率**
  - 各种长度报文的分布

协议分级统计（配合显示过滤器）

- 分组数量/字节数百分比（同层）
- 绝对分组数量/字节数
- 速率（比特/秒）
- 协议消息统计
  - 结束“分组”
  - 结束字节
  - 结束速率

端点统计/会话统计

- OSI 不同层次统计
  - 数据链路层（解析名称：MAC/IP/PORT）
    - 通讯双方/单端点、分组数、字节数、报文方向、速率、持续时间
  - 网络层
  - 传输层
    - UDP/TCP，端口统计
- 快速应用过滤器及着色规则

HTTP/HTTP2 统计

- HTTP
  - 分组统计：请求方法与响应码统计
  - 请求：基于 Host 和 URI 统计
  - 负载均衡：基于 IP 与 Host 统计
  - 请求序列：对请求同一 Domain 下的 URI 统计
- HTTP2
  - 帧类型统计

TCP 连接信息统计

- 基于 TCP 连接特性统计，可切换方向
  - RTT 时间
  - 吞吐量
  - 窗口大小
  - 序列号

IO 图表与数据流统计

- IO 图表
  - 绘制出不同颜色、各类型（折线、直方、点）图
  - 以时间作为 X 轴（可选择时间间隔）
  - 可设置过滤器下的报文信息为Y轴
    - 报文数量、字节数、统计函数
- 数据流
  - 可选择基于显示过滤器，显示各端之间的数据流量

专家系统

- Error：错误信息，包括 Wireshark 解析失败信息
- Warning：异常警告信息
  - RST 复位关闭、TCP 窗口关闭、TCP 乱序报文等
- Note：正常通信中的异常通信报文
  - TCP 重复 ACK、TCP 重传报文、Keepalive、TLS 复用密钥、零窗口探查等
- Chat：通信的基本信息

扫码试看/订阅极客时间

《Web协议详解与抓包实战》视频课程