
下一代Internet技术与协议

张冬梅

zhangdm@bupt.edu.cn

2. IP地址与地址转换

主要内容

- 2.1 IP地址方案
- 2.2 IP地址解析
- 2.3 IP地址配置

2.1 IP地址方案

- IP地址概述
- IPv4编址方案
- IPv6编址方案

IP地址概述

- 互联网的目标：提供一个无缝的通信系统
- IP协议功能
 - 屏蔽物理网络的具体细节,提供一个虚拟网
- 协议地址(IP地址)
 - 由软件提供,不是计算机物理网络系统的一部分
- IP地址
 - 由软件提供,是给连接在Internet上的主机分配的在全世界范围内唯一识别的协议地址
- IP编址方案
 - IPv4编址方案(32bit)
 - IPv6编址方案(128bit)

IPv4编址方案

□ IP地址的定义

- IP地址是给连接在Internet上的主机分配的在全世界范围内唯一识别的32bit地址

□ IP地址的特点

- IP地址不能反映任何有关主机位置的地理信息
- IP地址是主机与网络的接口的地址
- IP地址有时可用来指明一个网络的地址

IPv4编址方案

□ 地址格式

Net_id	Host_id
--------	---------

net_id: 网络号

host_id: 主机号

先按**IP**地址中的网络号**net_id**把网络找到，再按主机号**host_id**把主机找到

IPv4编址方案

□ 地址类型及表示方法

地址类型：A类、B类、C类、D类、E类



A类	0	net_id	host_id
B类	10	net_id	host_id
C类	110	net_id	host_id
D类	1110	组播地址	
E类	11110	保留为今后使用	

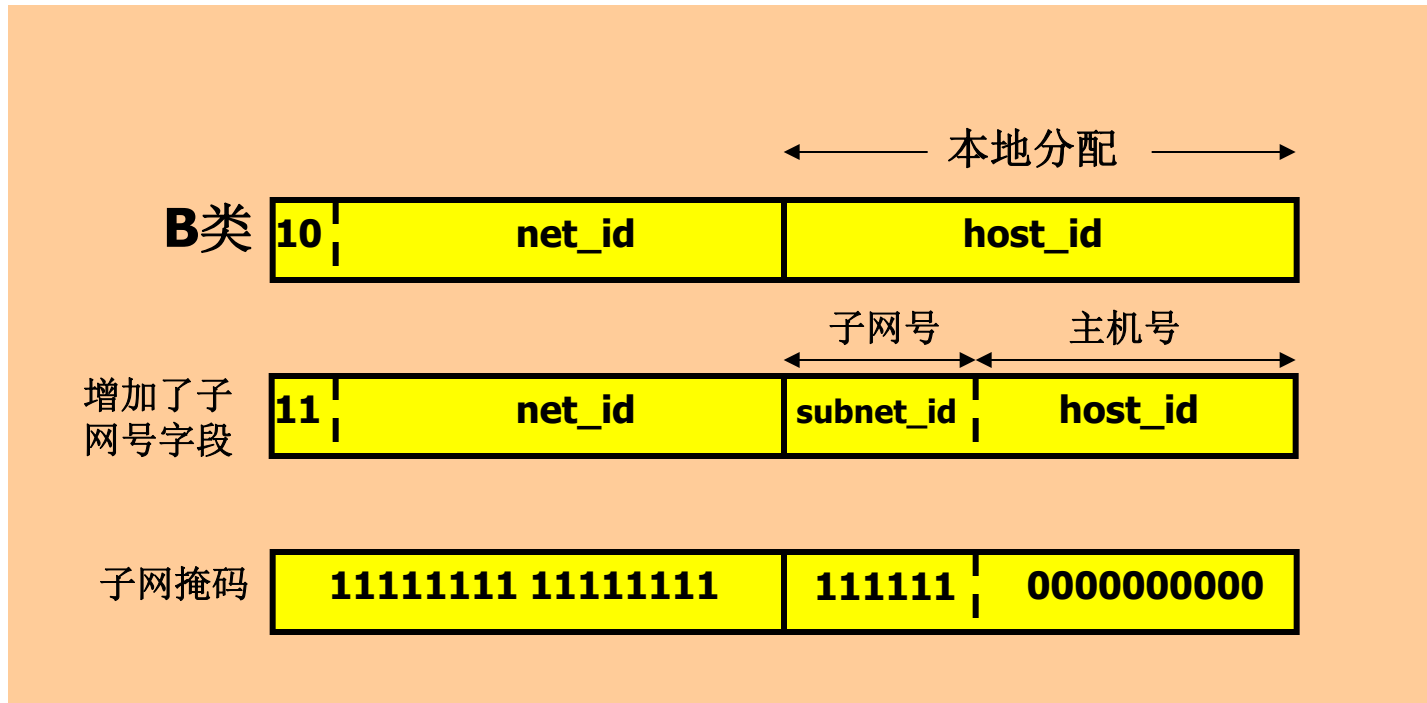
IPv4编址方案

- **公有地址**: A、B、C三类地址中，绝大多数的IP地址都是公有地址，需要向国际互联网信息中心申请注册。
- **私有地址**: 在IPv4地址协议中预留了3个私有IP地址段，供组织机构内部使用。分别位于A、B、C三类地址内：
 - A类地址: **10.0.0.0--10.255.255.255**
 - B类地址: **172.16.0.0--172.31.255.255**
 - C类地址: **192.168.0.0--192.168.255.255**

IPv4编址方案

□ 子网与子网掩码

- 背景：为了使IP地址的使用更加灵活，在IP地址中又增加了一个“子网号字段”



IPv4编址方案

□ 特殊IP地址

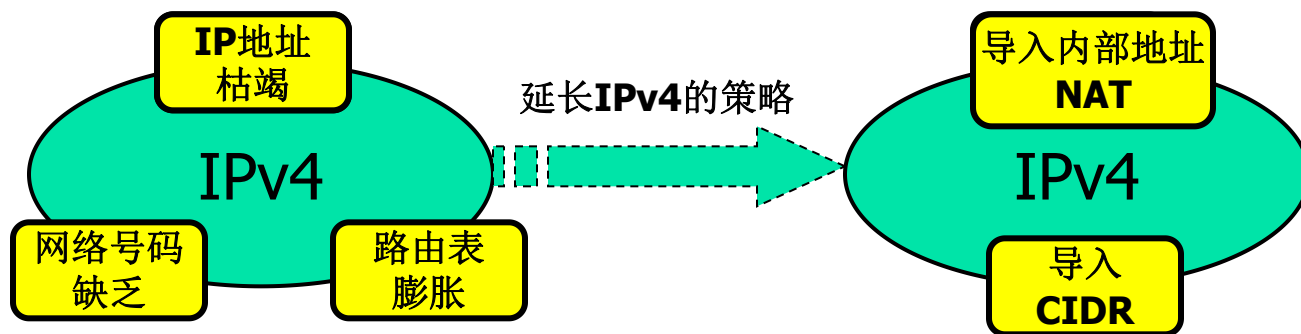
net_id	host_id	源地址使用	目的地址使用	代表的意思
0	0	可以	不可以	在本网络上的本主机
0	host_id	可以	不可以	在本网络上的某台主机
全1	全1	不可以	可以	只在本网络上进行广播 (各路由器均不转发)
net_id	全1	不可以	可以	对net_id上的主机进行广播
127	任何数	可以	可以	用作本地软件回送测试使用

IPv4编址方案

- IPv4地址缺陷
 - IP地址枯竭
 - 网络号码缺乏
 - 路由表膨胀

IPv4编址方案

□ IPv4地址缺陷的补救措施

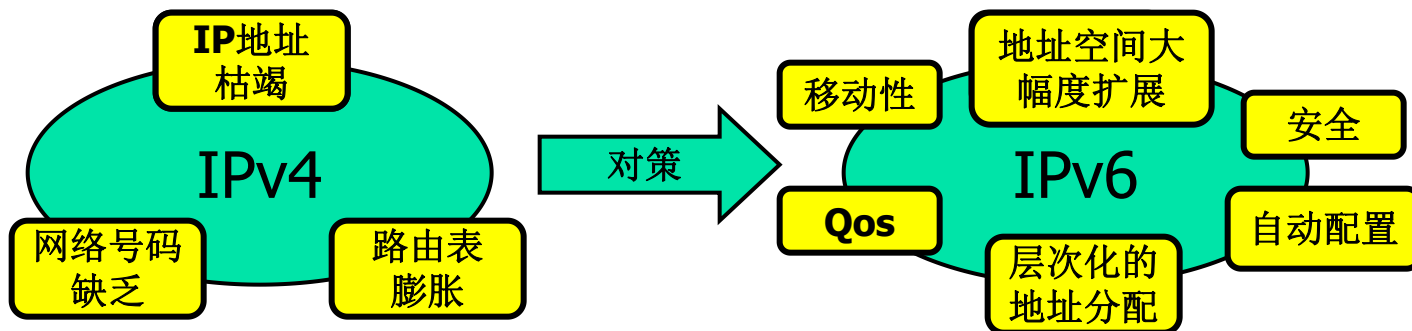


内部地址：面向Intranet的IP地址

CIDR：无类型域间路由选择

IPv6编址方案

- IPv6产生的背景
彻底解决IPv4的不足



IPv6编址方案

□ IPv6地址表示方法

■ 首选地址：标准的IPv6地址表达方式

- 将128位二进制地址按每16位划分为一组，共分8组，用“:”隔开；
- 表示形式-----X:X:X:X:X:X:X:X
- X为4位十六进制整数

0	A	E	5
0000	1010	1110	0101
0	0	0	0
0000	0000	0000	0000

IPv6编址方案

- 压缩表示格式（也称为零压缩表示法）
 - “0”编写规则；0000->0
 - 前导0压缩规则：每段起始位置的0可以省略(压缩)
 - (1) 0001->1
 - (2) 2001:0401:1000:0001:0000:0000:0000:45ff
2001:401:1000:1:0:0:0:45FF
 - 重叠冒号规则；A:0:0:0:B->A::B
 - (3) 2001:401:1000:1:0:0:0:45FF
2001:401:1000:1::45FF

举例

化简前	化简后
ABCD:0000:2345:0000:ABCD:0000:2345:0000	ABCD:0:2345:0:ABCD:0:2345:0
ABCD:2345:0:0:0:0:0:2345	ABCD:2345::2345
ABCD:0:0:0:2345:0:0:2345	ABCD::2345:0:0:2345
ABCD:0:0:2345:ABCD:0:0:2345	ABCD::2345:ABCD:0:0:2345
0:0:0:0:0:0:0:1	::1
ABCD:0:0:0:0:0:0:0:0	ABCD::
0:0:0:0:0:0:0:0	::

IPv6编址方案

□ IPv6前缀和IPv6地址空间

- IPv6地址组成：网络前缀+接口标识符
- IPv6不支持子网掩码，只支持网络前缀标识方法
- IPv6用地址前缀来标识网络、子网和路由(选路)
- 格式： IPv6地址/前缀长度
 - 前缀长度是十进制值(<128)，指出了地址中网络标识的位数
 - 举例：1234:56A1::C956:1A27:2348/55

网络地址空间分配情况

分配情况	地址前缀	所占比例	分配情况	地址前缀	占比
保留	0000 0000	1/256	未分配	101	1/8
未分配	0000 0001	1/256	未分配	110	1/8
为NSAP保留	0000 001	1/128	未分配	1110	1/16
为IPX保留	0000 010	1/128	未分配	1111 0	1/32
未分配	0000 011	1/128	未分配	1111 10	1/64
未分配	0000 1	1/32	未分配	1111 110	1/128
未分配	0001	1/16	未分配	1111 1110 0	1/512
可汇聚全球单播地址	001	1/8	链路本地单播地址	1111 1110 10 FE80::/10	1/1024
未分配	010	1/8	站点本地单播地址	1111 1110 11 FEC0::/10	1/1024
未分配	011	1/8	多播地址	1111 1111, FF00::/8	1/256
未分配	100	1/8			

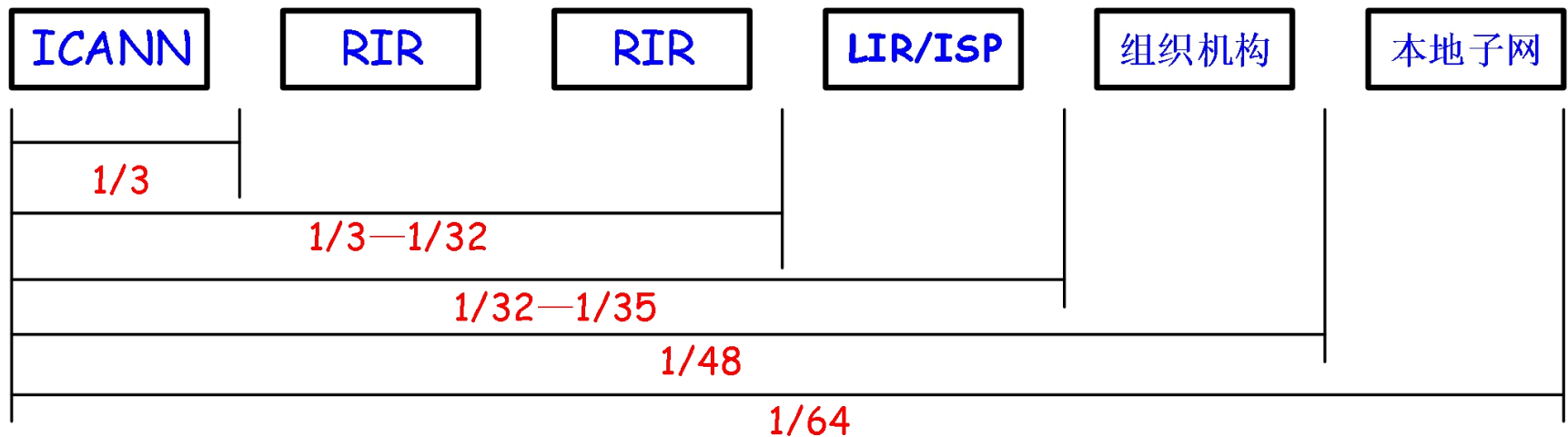
IPv6地址分配

- 地址分配相关角色
 - 权威机构
 - 所有者
- 分配的内容：权威机构一般参与单播地址空间的分配，有时也分配其他类型的地址（多播、特殊用途）。
- 分配的有效时间
 - 不限时地址块
 - 限时地址块

IPv6地址分配机构及前缀长度

□ 地址分配机构

- ICANN
- RIR(区域Internet注册机构)、NIR
- ISP
- 组织机构、本地子网



IPv6地址分配

- 截止2019年底获得4096*/32(即/20)以上的国家/地区

- 2019年分配情况

排名	国家 / 地区	地址数 (/32)	申请数 (个)
1	美国 (US)	50673	6329
2	中国 (CN)	47845	1817
3	德国 (DE)	22429	2563
4	英国 (GB)	20136	1942
5	法国 (FR)	14066	1218
6	俄罗斯 (RU)	12050	2353
7	日本 (JP)	10008	611
8	澳大利亚 (AU)	9324	1389
9	荷兰 (NL)	9265	1674

2019年全球IPv6地址分配数量为36499*/32，获得IPv6地址分配数量列前三位的国家/地区，分别为中国6787*/32，美国5504*/32，俄罗斯3716*/32。

13	波兰 (PL)	5376	811
14	韩国 (KR)	5246	160
15	阿根廷 (AR)	5198	927
16	南非 (ZA)	4757	296
17	欧盟 (EU)	4387	71
18	埃及 (EG)	4106	12

IPv6编址方案

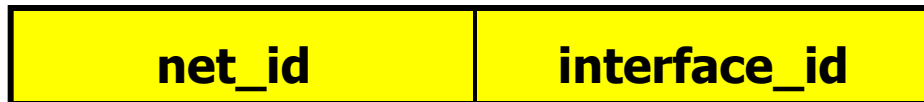
- Ipv6地址类型
 - 单播类型(unicast)
 - 组播类型(multicast)
 - 任播类型(anycast)
 - 特殊地址
 - 未指明地址
 - 环回(回送)地址

地址类型	二进制地址	前缀表示
未指定	00..0(全0)	::/128
环回地址	00...1（最后1位是1）	::1/128

IPv6编址方案

□ 可聚类全球单播地址

- IPv6的地址分成网络号和接口号



- 网络号进一步分为多个层次的网络



- **TLA_ID**: 顶级聚类标识符, 分配给某个骨干网的**ISP(104bit地址块)**
- **NLA_ID**: 次级聚类标识符, 分配给地区/中小的**ISP(80bit地址块)**
- **SLA_ID**: 网点级聚类标识符, 分配给用户(**64bit地址块**)
- **RES**: 为将来使用而保留
- **FP (001)**: 用于可聚类全球单播地址的格式前缀

IPv6编址方案

- 链路本地地址(Link Local Address, LLA)
 - 作用范围：连接在同一链路本地的节点之间，即以路由器为界的单一链路范围内
 - 该地址可以自动生成
 - 格式：特定前缀+接口ID
 - 特定前缀：FE80::/64
 - 接口ID：IEEE EUI-64接口标识符
 - 应用：在没有路由(网关)存在的网络中，主机通过MAC地址自动配置生成的IPv6地址，仅能在本地网络中使用。

MAC地址转换为EUI-64格式

□ MAC地址的EUI-48:

XX-XX-XX-XX-XX-XX

IEEE指定的 制造商指定的
制造商标识符 产品标识符

□ EUI-64:

XX-XX-XX-FF-FE-XX-XX-XX

然后对第1个字节的第七位求反

举例1: 00-AA-00-3F-2A-1C

00000010-AA-00-FF-FE-3F-2A-1C

即: 02-AA-00-FF-FE-3F-2A-1C

举例2: 00-12-34-00-AB-CD

0212:34FF:FE00:ABCD

IPv6编址方案

□ 站点本地地址(Site Local Address, SLA)

- 作用范围：在同一个站点内(一个组织机构单位的网络内)使用
- 该地址通过无状态或有状态地址自动配置方法进行指派
- 该地址对于外部网络站点是不可达的
- 格式：特定前缀(48bit)+子网ID(16bit)+接口ID(64bit)
 - 特定前缀：**FEC0::/48**
 - 子网ID：单位子网的子网ID字段
 - 接口ID：IEEE EUI-64接口标识符

多播地址

- 多播地址格式
- 多播地址的使用
- 预定义的多播地址

多播地址

□ 多播地址格式

8	4	4	112
1111 1111	标志	区域	Group ID

- 标志(ORPT)
 - T=0 永久性地址，所有的主机和路由器都知道；
 - T=1 非永久地址，暂时使用
- 区域: 标识多播地址的有效范围
 - 1: 接口/机器本地范围
 - 2: 链路/子网本地范围（限制在单一链路范围内）
 - 5: 站点本地范围
 - 8: 组织机构本地范围
 - E: 全球范围
- Group ID: 标识多播组，在给定范围内，可以是永久的也可以是暂时的

多播地址

□ 预定义的多播地址

- 全节点地址: Group ID = 1 FF02::1
- 全路由器地址: Group ID = 2 FF02::2
- 被请求的节点地址

Group ID = **FF02:0:0:0:0:1:FFXX:XXXX**

此多播地址由一个节点的单播或任播地址生成
(ICMP在获取邻居节点的链路地址和重复地址
检测要利用被请求的节点地址)

举例: FE80::2AA:FF:FE35:6A8B

FF02::1:FF35:6A8B

多播地址

- 很多IPv6多播地址由IANA分配为永久使用，并故意跨越多个地址范围(可变范围)
- 前缀表示：FF0X
- 举例：FF0X::101为NTP服务器预留地址

地址	含义
FF01::101	同一机器中的所有NTP服务器
FF02::101	同一链路/子网中的所有NTP服务器
FF05::101	同一站点中的所有NTP服务器
FF08::101	同一组织中的所有NTP服务器
FF0E::101	Internet中的所有NTP服务器

IPv6多播地址空间的部分保留地址

I多播地址	含义
节点-本地范围 (node-local)	
FF01::1	所有节点
FF01::2	所有路由器
链路-本地范围 (link-local)	
FF02::1	所有节点
FF02::2	所有路由器
FF02::4	DVMRP路由器
FF02::5	OSPF/IGMP
FF02::D	PIM路由器
FF02::16	支持MLDv2的路由器
FF02::1:2	所有DHCP代理
FF02::1:FFXX:XXXX	请求节点地址范围

I多播地址	含义
站点-本地范围 (site-local)	
FF05::2	所有路由器
FF05::1:3	所有DHCP服务器
可变范围	
FF0X::101	NTP
...	

IPv6多播地址映射为MAC地址

- IPv6多播地址: **FF02::1:FFXX:XXXX**
- 链路层组播地址: **33-33-FF-XX-XX-XX**



举例1: IPv6多播地址 **FF0E:1234::5678:1A3C**
MAC地址 **33-33-56-78-1A-3C**

举例2: 某IPv6地址 **1234:AF0E:1234::1A3C**对应的被请求节点多播地址是多少? 该多播地址映射为MAC多播地址是多少? **FF02::1:FF00:1A3C;**
MAC地址 33-33-FF-00-1A-3C

任播地址

- **定义**：一个地址对应一组网络接口，被哪个接口接收由具体的路由协议定义（“最近的”一个，按照路由协议的测量距离）
- 任播地址存在于**单播地址**中，没有专门的区分。
- 任播地址是根据发送者位置指向不同主机的单播地址
- 应用--**DNS**根域名服务器发现

IPv4与IPv6地址比较

内容	IPv4	IPv6
地址长度(bit)	32	128
地址表示方法	点分十进制	冒分十六进制，零压缩、双冒号简化
分类	A、B、C、D、E五类，CIDR	单播、多播、任播、特殊地址
网络地址标识	子网掩码、前缀长度	前缀长度
环回地址	127.0.0.1或127.X.X.X	::1
公网地址	单播地址	可汇聚全球单播地址
多播地址	224.0.0.0/4	FF00::/8
广播地址	支持	未定义
未指明地址	0.0.0.0	::
局部地址/内部地址	10.0.0.0/8、172.16.0.0/12 192.168.0.0/16	链路本地地址、站点本地地址

主机IPv6地址

- IPv6主机上的同一个网络接口可以分配到的单播地址
 - 链路本地地址 **FF80::/64+接口ID**
 - 可汇聚全局单播地址
 - 环回地址 **::1**
- IPv6主机接口需要监听的地址
 - 以链路本地全节点地址为目的地址的分组 **FF02::1**
 - 以本主机接口的可汇聚全局单播地址为目的地址的分组
 - 属于同组多播地址的分组

路由器IPv6地址

□ IPv6路由器上每个网络接口可分配的单播地址

- 链路本地地址 **FF80::/64+接口ID**
- 可汇聚全局单播地址
- 环回地址 **::1**

□ IPv6主机接口需要监听的地址

- 各类本地地址为目的地址的分组
FF01::1; FF01::2; FF02::1; FF02::2; FF05::1; FF05::2; ...
- 以本主机接口的可汇聚全局单播地址为目的地址的分组
- 属于同组多播地址的分组

主要内容

- 2.1 IP地址方案
- 2.2 IP地址解析
- 2.3 IP地址配置

IP地址解析

- 概述
- 常用地址解析技术
- IPv4使用的地址解析方法
- 其他地址解析方法

概述

□ 通信时为什么需要进行地址解析？

- IP地址不能直接在数据链路层寻址

□ 地址解析的定义

将协议地址翻译成等价的硬件地址的过程叫地址解析

□ 相关说明

- 地址解析只发生在同一个链路的两台机器之间
- 地址解析只有需要发送数据时才进行

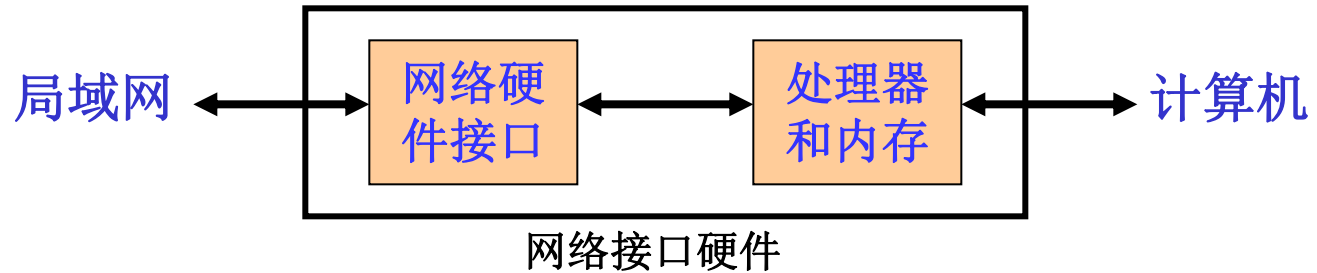
地址解析技术

- 哪些因素影响地址解析方法
 - 协议
 - 硬件编址方案

硬件地址（1）

□ 硬件地址

为每个站点分配的一个唯一的数值



硬件地址（2）

□ 硬件地址编制技术

- 静态编址
- 可配置编址
- 动态编址

□ 硬件地址类型

- 单播
- 广播
- 组播

层间发现：地址(标识符)映射

- 不同层协议实体使用不同地址标识
- 层间地址映射的基本方法
 - 使用**众所周知的**或**手动配置**的标识符
 - 将映射关系**存储在数据库或表**中，提供统一**映射服务**
 - 利用**协议通告**两个标识之间的映射关系
 - 通过一种标识**计算**另一种标识

常用地址解析技术

- 功能：将IP地址转换为对应的物理地址
- 地址解析的三类基本方法
 - 查表法
 - 构造函数法(相近形式计算)
 - 消息交换法

常用地址解析技术

□ 地址解析方法小结

- 适用于任何硬件
- 硬件地址小于协议地址
- 需要硬件广播
- 增加网络通信量
- 最小延迟产生解析结果
- 实现复杂

Internet地址解析方法

- Internet地址解析方法依赖于网络底层硬件所使用的编址方案
- 不同编址方案对应不同地址解析方法
- 典型协议
 - ARP

IP协议的地址解析方法

□ ARP协议

- 作用：将IP地址转换成对应的MAC地址
- 适用范围：IP over Ethernet以太网

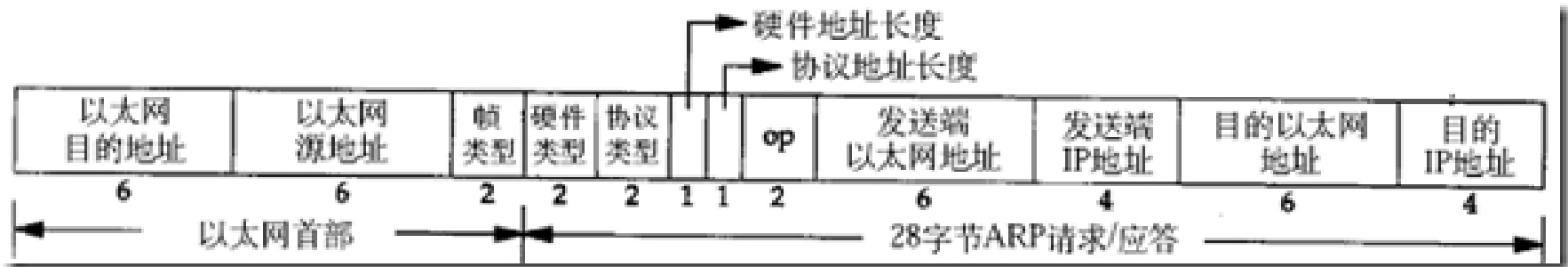
□ IP over ATM(CIPOA)

- 把ATM作为IP的低层数据链路层，而应用层还是基于传统的IP。
- 客户/服务器模式的ATM ARP协议
- 使用地址解析服务器ARS，具有统一的ATM地址，负责维护IP-ATM地址映射表或者高速缓存

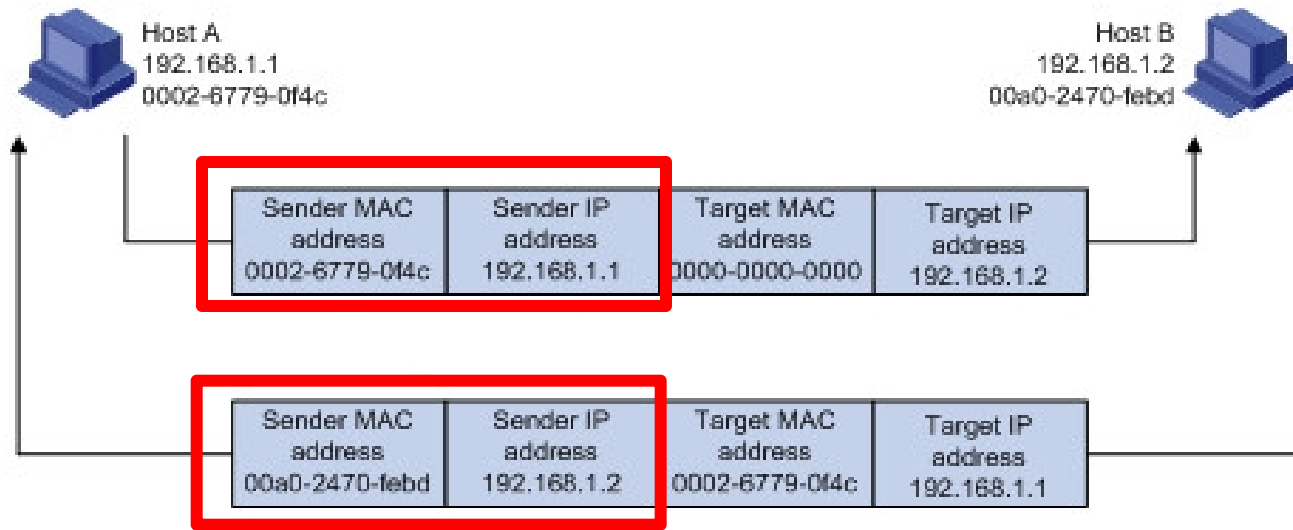
□ IPv6的邻居发现（参见后续部分的讲义）

ARP协议

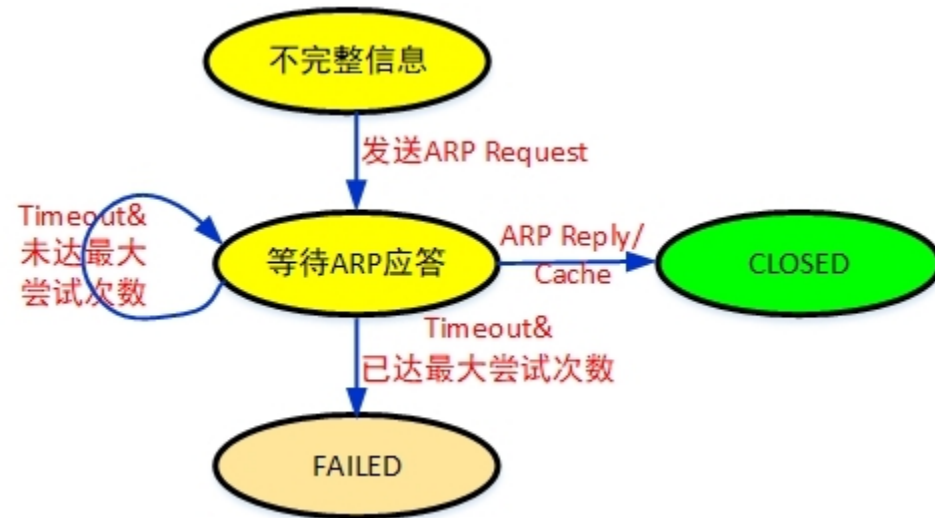
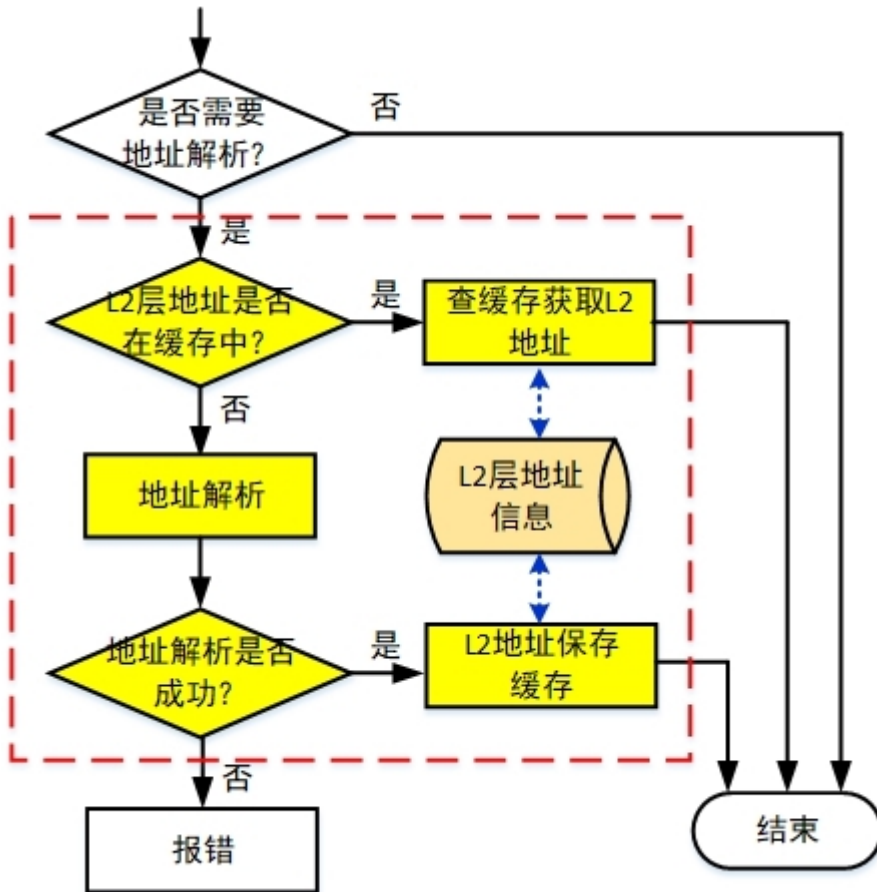
□ ARP的数据包格式(Ethernet type:0x0806)



□ ARP的工作过程: 广播请求, 单播回应



ARP协议



ARP协议

□ ARP缓存

- 缓存MAC地址和IP地址的映射关系
- When: **ARP(请求/响应)报文到达**
- How:
 - 替换: **后到优先原则**
 - 增加: **必要性原则、双向通信原则**
 - 删除: **时效性原则（重启、老化）**

□ ARP缓存: 软状态(状态自动机)

- 有助于网络自动重新配置
- 软状态刷新机制

□ 缓存带来的问题: 地址绑定信息过时

ARP协议

□ 解决方案：免费ARP(Gratuitous ARP)--自问自答

- 广播请求，广播回应
- 发送方IP = 目的方IP
- 以太网头目的MAC = FF:FF:FF:FF:FF:FF

□ 功能

- **加速网络设备状态变化的发现**：允许主机地址信息变更时主动告知缓存有该地址的主机更新地址绑定信息
- **地址重复检测**：允许一台主机检测另一台主机是否配置了与自己相同的IP地址

ARP协议

□ ARP命令

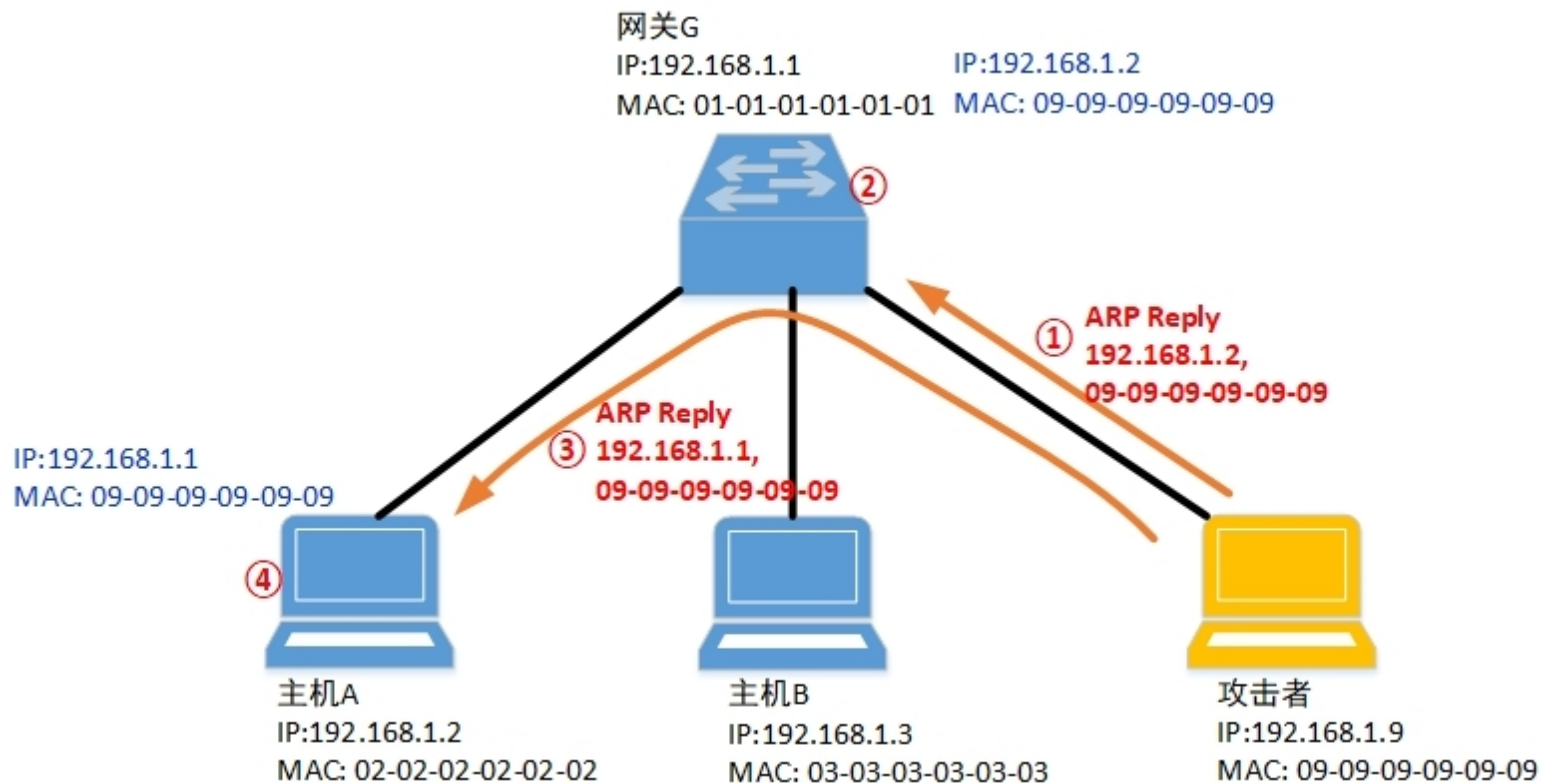
- **arp -a**: 用于查看缓存中的所有项目。
- **arp -a IP**: 如果有多个网卡, 那么使用**arp -a**加上接口的**IP**地址, 就可以只显示与该接口相关的**ARP**缓存项目。
- **arp -s IP 物理地址**: 可以向**ARP**缓存中人工输入一个静态项目。
- **arp -d IP**: 使用该命令能够人工删除一个静态项目

ARP协议

- 关于ARP协议的几个问题
 - 以太网帧格式和ARP数据包格式中均有发送端以太网地址和接收端以太网地址，两者是否重复？
 - 为什么ARP需要先查询缓存再进行地址解析，请说明其合理性。
 - 尝试整理ARP协议处理流程图
 - ARP协议本身存在安全漏洞吗？
- ARP存在的安全问题：**ARP欺骗攻击**

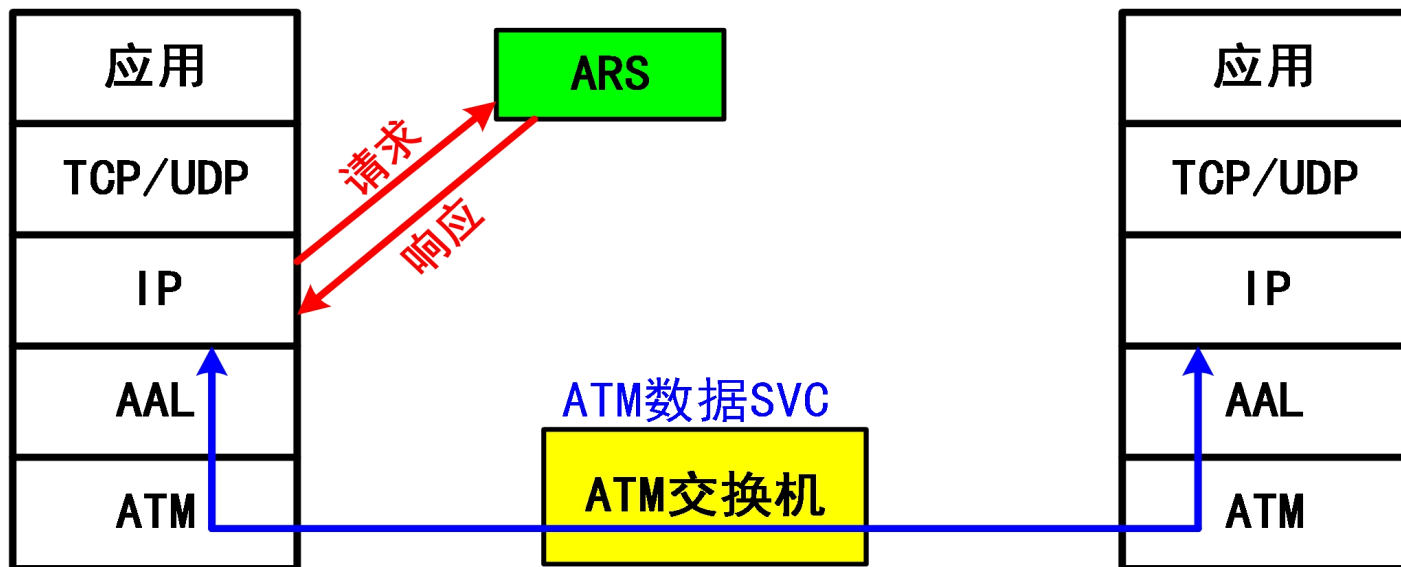
ARP欺骗

- 典型ARP场景
- 过程：伪造ARP reply，刷新缓存
- 效果：无法上网、信息泄露、中间人攻击



CIPOA

- ❑ CIPOA: Classical IP over ATM
- ❑ 工作原理及过程
 - 初始化
 - 主叫→ARP 服务器(ARS) [IP ARP请求]
 - 主叫←ARP 服务器(ARS) [ATM地址]
 - 主叫→被叫 [SVC呼叫请求]

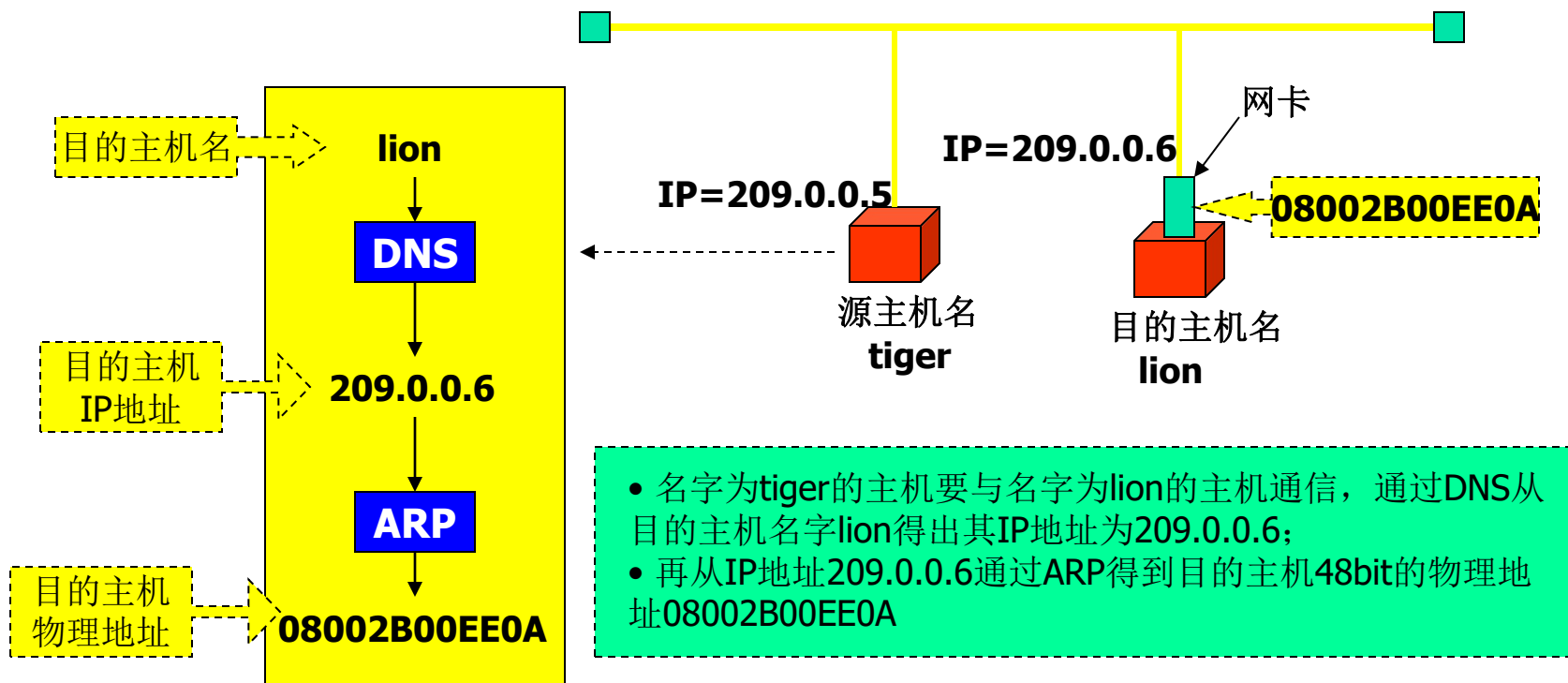


域名服务

□ IP地址不能直接用来通信

- IP地址为网络地址(一种协议地址)，不能直接在链路层寻址，必须转换为物理地址（地址解析）
- 用户不愿意使用难于记忆的主机号，愿意使用易于记忆的主机名字(域名)，故需要在主机名字和IP地址之间进行转换（域名服务）

域名、物理地址和IP地址的转换



DNS

- DNS是互联网最重要的基础服务之一
- 当前结构最复杂、规模最大的分布式数据库系统
 - 将域名信息保存在域名所有者的控制中
 - 增加DNS系统的可扩展性
- 设计之初重点考虑效率问题，对安全性考虑不足
 - DNS服务器缓存
- 采用树形结构的域名地址空间
 - 最高层为根、顶级域名TLD、二级域名SLD
- 迭代查询与递归查询
- DNS服务器信息通过手动或DHCP配置

IPv6域名系统DNS

- IPv6利用DNS实现从主机名称到IPv6地址的映射
 - 正向解析：通过域名得到IPv6地址
 - 反向解析：通过IPv6地址得到域名
- 与IPv6相关的内容
 - IPv6网络资源记录类型，AAAA记录类型
 - 修改DNS查询，支持IPv6地址
- DNS安全扩展DNSSec

自动发现DNS服务器

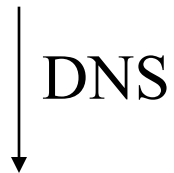
- 不支持DNS服务器的自动配置，仅支持**自动发现DNS服务器**
- **有状态DNS服务器发现**
 - 利用中间服务器(如DHCP服务器等)将DNS服务器的地址、域名和搜索路径等DNS信息通告给网络中的节点。
- **无状态DNS服务器发现**
 - 前提：为子网内部的DNS服务器配置站点范围内的任播地址(也可以使用站点局域多播或链路局域多播地址)
 - 节点以任播地址为目的地址发送DNS服务器请求，询问DNS服务器的地址、域名和搜索路径等
 - DNS服务器接收请求并进行响应
 - 节点配置DNS相关信息

地址转换小结

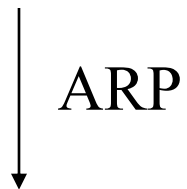
- 物理地址既依赖于低层协议又依赖于硬件
- IP地址独立于机器硬件地址
- 域名是一个便于记忆的名字

□ 当指定一个目的地时

用户使用域名



应用程序使用IP



主机与路由器使用物理地址

主要内容

- 2.1 IP地址方案
- 2.2 IP地址解析
- 2.3 IP地址配置

IP地址配置及协议配置

- 概述
- RARP
- DHCP

概述

- 问题的提出
 - IP地址的配置
 - TCP/IP协议的配置
- 常用的地址配置技术
 - 手工配置
 - 自动配置

RARP(1)

- 协议功能

根据本机的**MAC**地址得到相应的**IP**地址

- 前提

网络上至少有一台**RARP Server**

- 工作过程

- 发送方广播一个**RARP**请求，该请求还包含自己的**MAC**地址；
- 网络上所有机器均接收该请求，只有被授权提供**RARP**服务的机器才回答该请求

RARP(2)

□ 缺点

- RARP在底层操作（而非TCP之上），直接构造RARP Server困难；
- RARP响应分组包含的信息量少（仅包含IP地址）
- RARP使用计算机的MAC地址来识别机器，不能用于动态分配硬件地址的网络

□ 改进上述缺点的方案

- BOOTP（自举协议）
- DHCP（动态主机配置）

DHCP

- DHCP用于给主机动态配置地址、默认路由和其他配置信息
- DHCP功能[RFC2131]
 - 为主机分配一个永久性IP地址;
 - 为主机分配一个临时IP地址
- 采用C/Server模式
 - Client
 - Server

DHCP

- DHCP协议工作过程
 - DHCP服务器发现
 - DHCP服务器提供
 - DHCP请求
 - DHCP ACK
- 优点：即插即用

IPv6地址配置

- IPv6大地址空间需要高效、合理的自动配置机制
- 自动配置
 - 链路本地地址自动生成: $\text{IP地址} = \text{FE80::}/64 + \text{EUI-64}$
 - 无状态地址自动配置(强制的)
 - 接收路由器发送的全局地址前缀(ICMPv6的RA消息)
 - $\text{IPv6地址} = \text{全局地址前缀} + \text{EUI-64}$
 - DHCPv6地址自动配置(可选的)
- 主机接口: 自动配置
- 路由器接口
 - 链路本地地址: 自动配置
 - 其他类型地址及参数: 手工配置或网管配置

DHCPv6

- DHCPv6是针对IPv6编址方案设计，为主机分配IPv6地址和其他网络配置参数的一种应用层协议
- DHCPv6可以为网络接口配置：IPv6网络地址、其他网络参数（如DNS服务器地址等参数）
- DHCPv6的工作模式：C/S模式
 - Client：需要得到网络地址或其他配置信息的节点
 - Server：为Client提供IPv6地址或其他配置信息的节点

DHCPv6

□ UDP端口号

- DHCPv6 报文承载在UDP上。
- 客户端监听的UDP目的端口号是546，服务器、中继代理监听的UDP端口号是547。

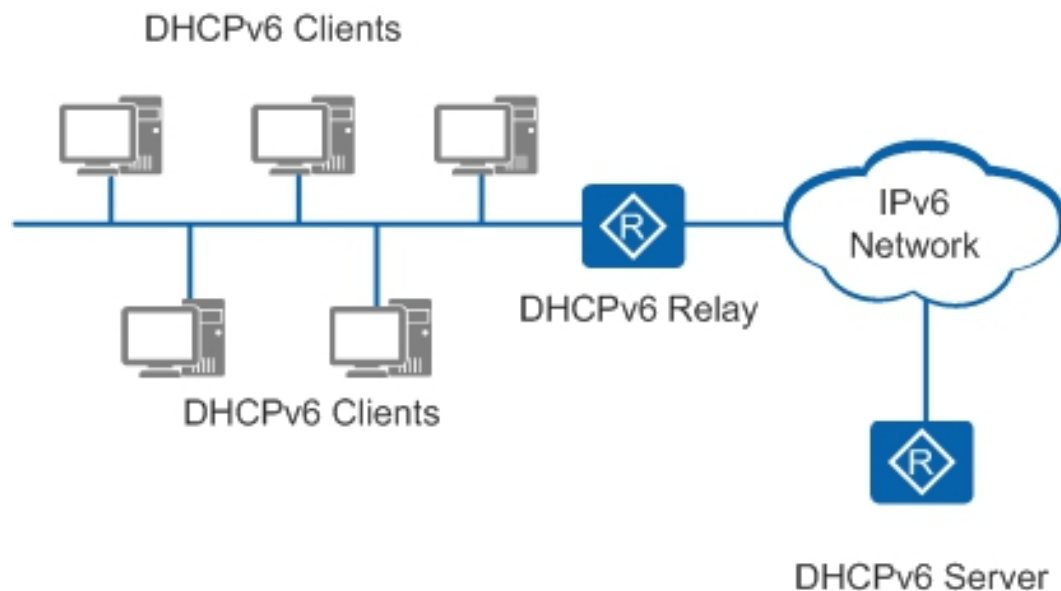
DHCPv6

□ DHCPv6功能角色

- **DHCPv6客户端**: 与DHCPv6服务器进行交互, 获取IPv6地址和网络配置信息, 完成自身的地址配置功能
- **DHCPv6服务器**: 负责处理来自客户端或中继代理的地址分配、地址续租、地址释放等请求, 为客户端分配IPv6地址和其他网络配置信息。

■ DHCPv6中继代理

(DHCPv6客户端与服务器不在同一链路)



DHCPv6

- DHCPv6不支持自动配置，只支持自动发现
 - 自动配置：一般需要通过某种服务来换取配置参数(也可以直接计算)
 - 自动发现：最基础的服务
 - 自动发现服务的特点：就近发现
 - 过程
 - DHCPv6客户端发送目的地址为多播地址的**solicit**消息
 - 通过DHCPv6服务器的**广告advertise**消息来发现服务器

DHCPv6

□ DHCPv6多播地址定义

- **FF02::1:2**---所有**DHCPv6服务器和中继代理**的多播地址，本**链路范围**的所有DHCPv6 服务器和中继代理都是该组的成员。
- **FF05::1:3**---所有DHCPv6服务器多播地址，地址是站点范围的，用于中继代理和服务器的通信，**站点内**的所有DHCPv6服务器都是此组的成员。

DHCPv6基本功能

- 地址分配服务(**DHCPv6有状态自动分配**)
 - 不提供默认路由器地址和网路前缀长度
 - 基本过程
 - 自动计算：链路本地地址
 - 启动DHCPv6交换，配置全球IPv6地址和其他网络配置信息
- 无状态服务(**DHCPv6无状态自动分配**)
 - DHCPv6服务器无需记录状态信息
 - 基本过程
 - 自动计算：无状态地址自动配置获得全球IPv6地址
 - 启动DHCPv6交换，配置其他网络配置信息

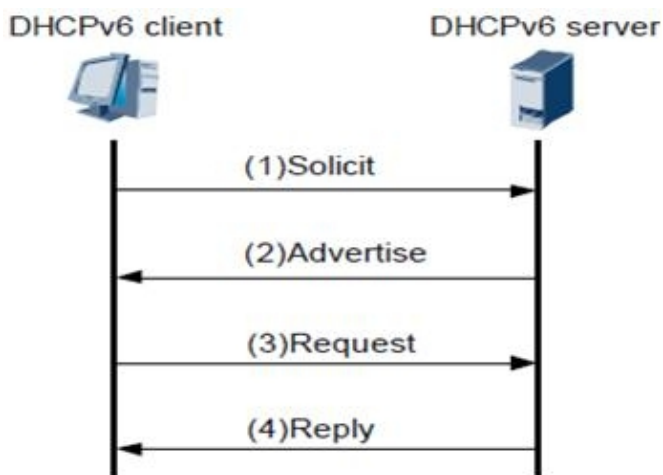
DHCPv6

报文类型	说明
SOLICIT(1)—请求定位	客户端用来定位DHCPv6服务器
ADVERTISE(2)—通告	服务器作为对客户端SOLICIT的响应
REQUEST(3)—请求	客户端用来从服务器获取信息
CONFIRM(4)—确认	客户端校验地址和配置参数是否有效
RENEW(5)—更新	客户端向原始的DHCP服务器续借配置参数
REBIND(6)—重新绑定	客户端用来延长地址的生存期并续借配置参数
REPLY(7)—回复	服务器响应客户端的REQUEST、RENEW等
RELEASE(8)—释放	客户端释放IP地址
DECLINE(9)--拒绝	客户端告知服务器某个已经分配的地址不能使用

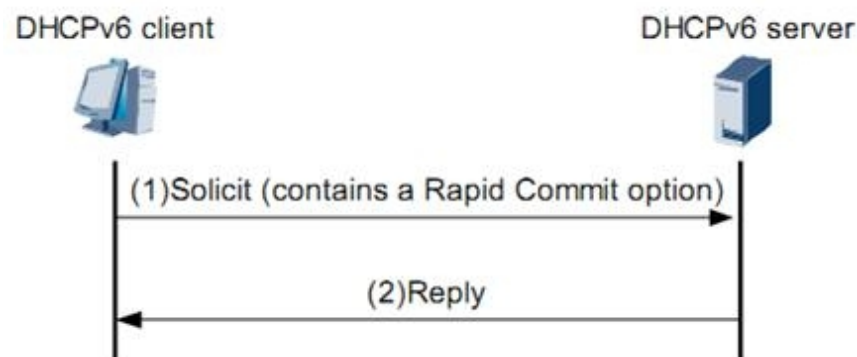
DHCPv6

□ DHCPv6 服务器为客户端分配地址/前缀的过程分为两类

■ 四步交互分配



■ 两步交互快速分配



□ 当客户端申请到IPv6地址后，会对刚申请到的IPv6地址会做**重复地址检测**

DHCPv6

□ DHCPv6服务器对地址的管理

- 通过对**绑定信息表**的维护来管理地址信息
 - DUID –DHCPv6 Unique ID唯一标识符
 - 地址信息
 - 地址生存周期
- 地址冲突: DECLINE
- 地址续借: RENEW
- 地址重新绑定: REBIND
- 地址释放: RELEASE

DHCPv6

□ DHCP的不足

■ 地址唯一性难保证

- 重复地址不能发现网络上非DHCP客户机使用的IP地址
- 多个DHCP服务器存在时，一个DHCP服务器不能查出已被其他服务器租出去的IP地址

■ 地址不确定性：通过DHCP获得的IP地址会变化，具有不确定性，用户被访问难度较大。

■ 安全性

- 非法客户端、恶意服务器
- 耗尽配置资源的Dos攻击

DHCPv6

□ DHCPv6与DHCPv4的相同点

- 服务提供模式：基于Client/Server应用模式
- 目标：S向C提供网络配置信息
- 低层协议：基于UDP
- 当C与S不在同一网络中且C没有地址无法与S正常通信时，都需要代理进行中继转发

□ DHCPv6与DHCPv4的区别

- DHCPv6使用本地链路地址做源地址
- DHCPv6使用单独的多播地址给服务器或中继代理发报文
- DHCPv6支持无状态服务
- DHCPv6无路由器选项和前缀长度选项