# 网络技术与信息安全

## 第5讲：网络基础服务

河南中医药大学信息技术学院
许成刚

# 网络基础服务



- DNS - 域名服务
- DHCP - IP地址管理
- NTP - 网络时间服务

# 一、DNS

## 1.1 认识DNS

# DNS —— 认识DNS



## 为什么需要DNS？

- 根据TCP/IP协议的要求，用户访问互联网上的主机时（例如百度服务器），需要用到该主机的IP地址，但在实际应用中，用户并未输入服务器的IP地址，而是输入域名（例如www.baidu.com、www.hactcm.edu.cn）。
- 记忆很多目的主机的IP地址是一件很困难的事，为了解决这些问题，互联网设计出域名系统（Domain name system，DNS）。域名系统可给互联网主机分配容易记忆的名字（即域名），并且把这些名字与相应的IP地址关联保存起来。用户在访问某个互联网主机时，只需要输入其域名，则互联网的域名系统会自动解析出该域名对应的IP地址，并将其发给用户，接下来，用户的主机就可以通过IP地址访问目的主机了！

# 客户机如何才能获得百度的IP地址？


从表面来看，互联网用户是通过域名www.baidu.com去访问百度服务器的，用户并未使用百度服务器的IP地址。

但实际上，用户主机必须知道百度服务器的IP地址，才能通过互联网（采用TCP/IP协议）访问到百度服务器。

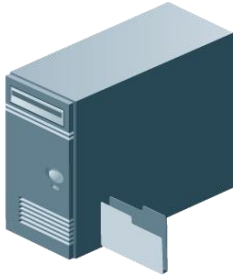
如何解决上述的矛盾？

# 客户机如何才能获得百度的IP地址？


前面的例子中，当用户在浏览器中输入百度网址，就表示发出域名解析请求（即www.baidu.com对应的IP是什么？）。该请求并不是直接发给百度服务器的，而是发给域名系统（DNS）。DNS根据域名（www.baidu.com）解析出其对应的百度服务器的IP地址，并再此IP地址返回给用户，此时，用户就可以通过IP地址访问百度的服务器了。

【动画演示】

# DNS的基本解析过程

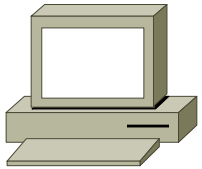


互联网的
DNS系统

用户只知道百度的域名，但
不知道其IP地址

?

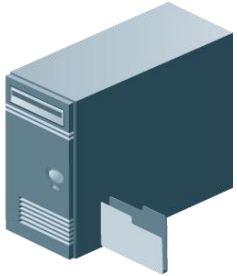
百度的Web服务器



访问：www.baidu.com

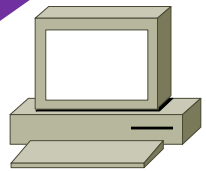
② 请求报文中包含待解析域名，
以UDP方式发给DNS系统

① 向DNS发送域名解析请求



互联网的
DNS系统

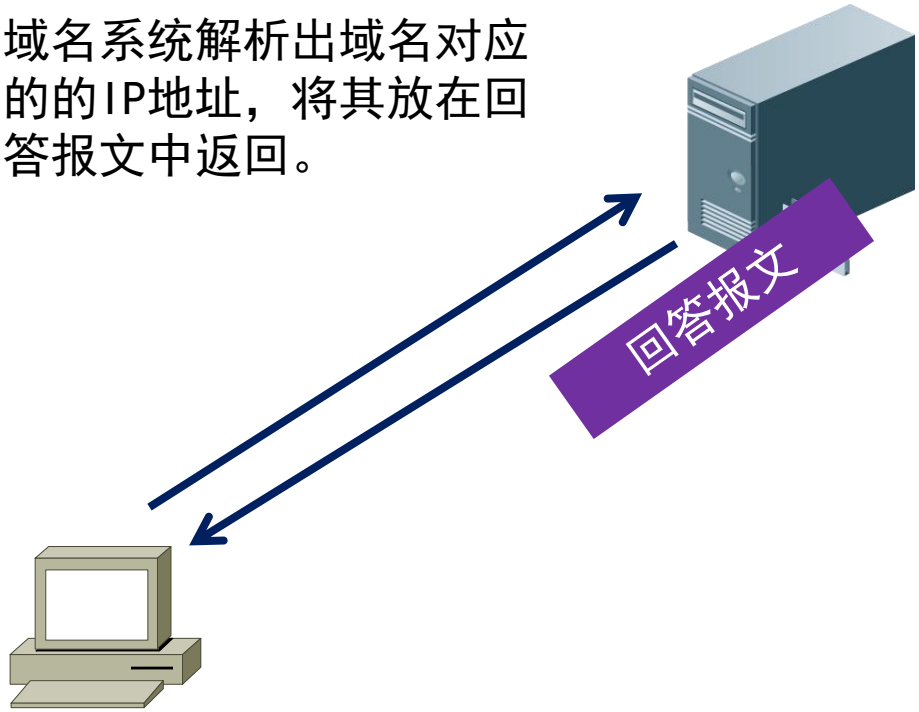
DNS请求报文



访问：www.baidu.com

**Web服务器**

③ 域名系统解析出域名对应的的IP地址，将其放在回答报文中返回。

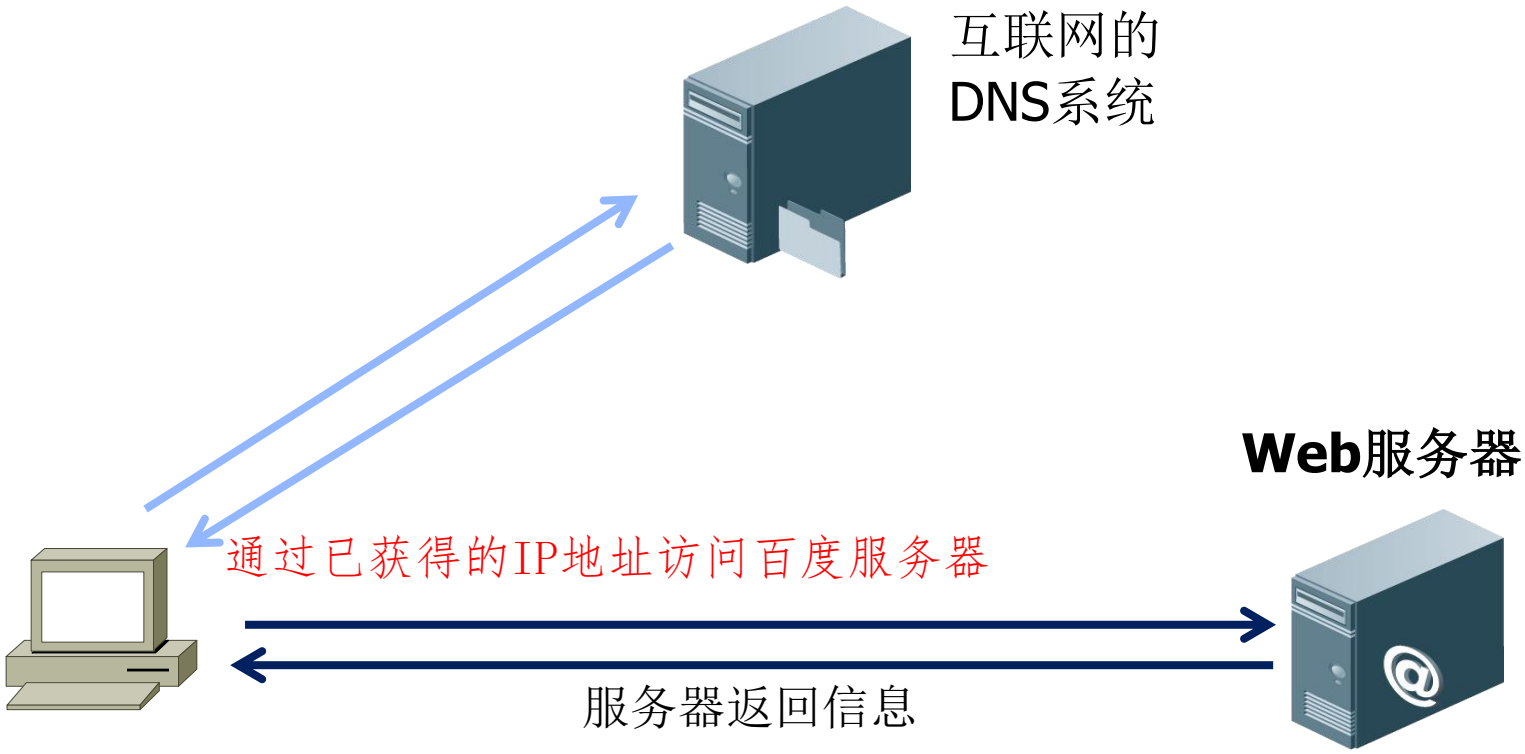



互联网的DNS系统

**Web服务器**

访问：www.baidu.com

现在，用户主机知道百度的IP地址了！


互联网的
DNS系统
Web服务器
通过已获得的IP地址访问百度服务器
服务器返回信息
客户端浏览器将服务器
返回的信息组织成网页
（结束）

# DNS —— 认识DNS



- 为了保证域名的唯一性，域名也需要申请和审批！

DNSPOD　中资源 www.zzy.cn　万网 www.net.cn 阿里云旗下品牌

互联网域名注册服务机构


首页
产品中心
商城
服务与支持
合作伙伴
亲，请登录 | 免费注册 | 用户中心 | 购物车(0) | 管理控制台
DNSPOD
输入您想注册的域名，例如: dnspod
.com
查询域名
.com 55元 .net 55元 .xyz 11元 .cn 25元 | 域名价格总览 | 批量查询
域名首购用户专享
域名礼包买1送3 首购用户领券再减10元
域名续费
便宜到底，操作简单
域名转入
一键转入，管理方便
域名解析
无限域名，实时生效
D+
精准接入，稳定可靠


xuchenggang
.com
查 询
多选模式
中资源
www.zzy.cn
英文域名
中文域名
域名查询结果
哪些新顶级域名后缀支持备案?
xuchenggang.com (已被注册)
详细 访问
xuchenggang.wang (尚未注册)
音同“网”，符合国人认知
¥22元/首年
立即注册
xuchenggang.top (尚未注册)
代表着事物最美好的状态
¥9元/首年
立即注册
xuchenggang.net.cn (尚未注册)
中国国家顶级域名
¥30元/首年
立即注册
xuchenggang.com.cn (尚未注册)
中国国家顶级域名
¥30元/首年
立即注册
xuchenggang.cn (尚未注册)
中国国家顶级域名
¥30元/首年
立即注册
xuchenggang.net (尚未注册)
国际通用顶级域名
¥50元/首年
立即注册
xuchenggang.org.cn (尚未注册)
中国国家顶级域名
¥30元/首年
立即注册
xuchenggang.info (尚未注册)
网络信息服务的首选域名
¥150元/首年
立即注册
xuchenggang.cc (尚未注册)
可理解为Commercial Company，即商业公司
¥300元/首年
立即注册
xuchenggang.biz (尚未注册)
business的缩写，代表着商业领域
¥28元/首年
立即注册
xuchenggang.org (尚未注册)
社会组织机构首选域名
¥80元/首年
立即注册

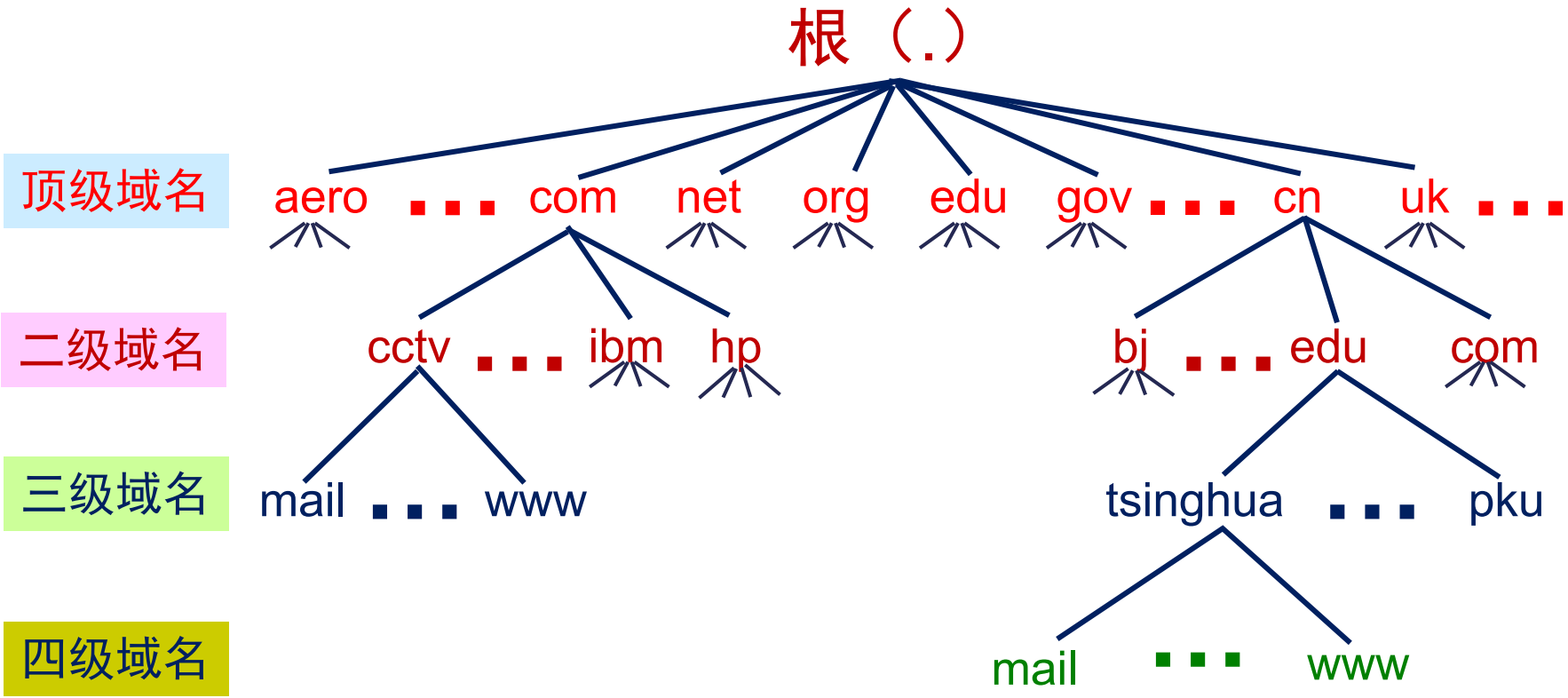
# DNS —— 认识DNS

## 域名的树状层次结构

- 域名采用了倒置树状层次结构的命名方式。
- 所有的域名都以英文的“ . ”开始，是域名的根；
- 根的下面是顶级域名；
- 顶级域名下面还可以有下一级域名，例如二级、三级、四级…….
- 各级域名之间用点隔开

例　www.hactcm.edu.cn

# 互联网的域名空间


根（.）
顶级域名
二级域名
三级域名
四级域名
aero
com
net
org
edu
gov
cn
uk
cctv
ibm
hp
bj
edu
com
mail
www
tsinghua
pku
mail
www

# DNS —— 认识DNS

## 主机名

- 企业或个人申请了域名后，可以根据自身需要在该域名下添加主机名，也可以根据需要创建子域名。
- 主机名表示是该域中的某个主机（通常是服务器）的名字；
- 例如：
  - 河南中医药大学申请的域名是　　．hactcm.edu.cn

# 举例：根据工作需要，河南中医药大学设置了一台Web服务器和一台邮件服务器

mail 是主机名

http://mail.hactcm.edu.cn


www 是主机名

http://www.hactcm.edu.cn

# DNS —— 认识DNS

## 完全限定域名（FQDN）

- 域名是全球唯一的，“主机名+域名”肯定也是全球唯一的。
- “主机名+域名”称为完全限定域名，即FQDN。
- FQDN是Fully Qualified Domain Name的缩写，含义是完整的域名。
- 例如：　www.hactcm.edu.cn
- 我们通常所说的网站的网址，严格来说是完全限定域名。

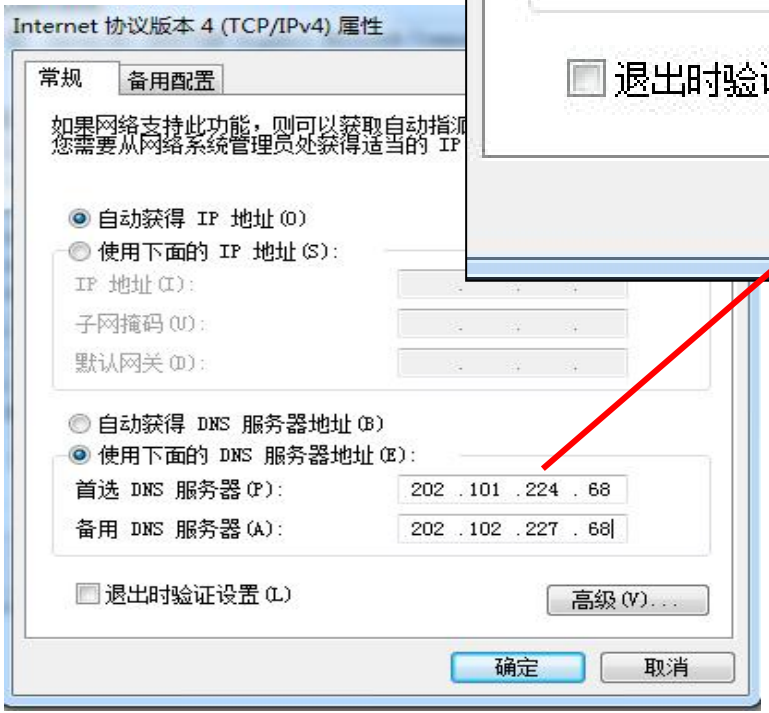
# 一、DNS

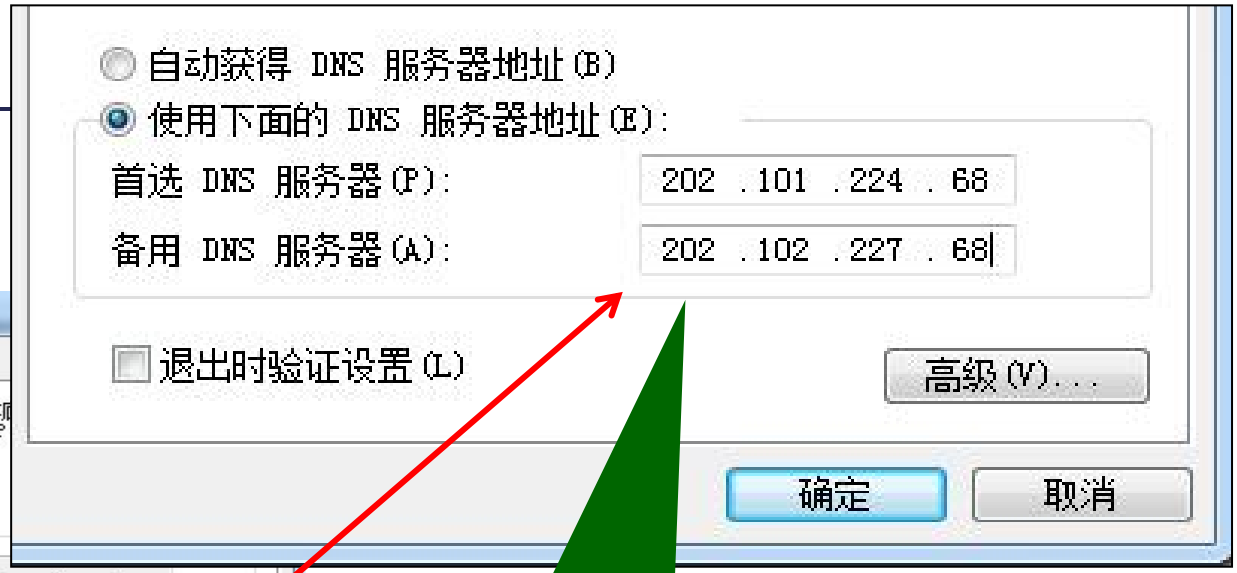
## 1.2 域名服务器的工作

# DNS —— 域名服务器

- 域名服务器的作用（简化描述）
  - 可以把互联网上的“域名——IP地址”的对应关系看成是一个数据库；
  - 假设把这个“数据库”放入一台计算机，这台计算机通过域名解析程序，专门向互联网上的用户提供“域名——IP地址”的解析和查询服务，被称作“域名服务器”；
  - 思考：
    - 互联网用户要想使用域名服务，就必须事先知道域名服务器的IP地址；
    - 配置举例

# 客户机的配置

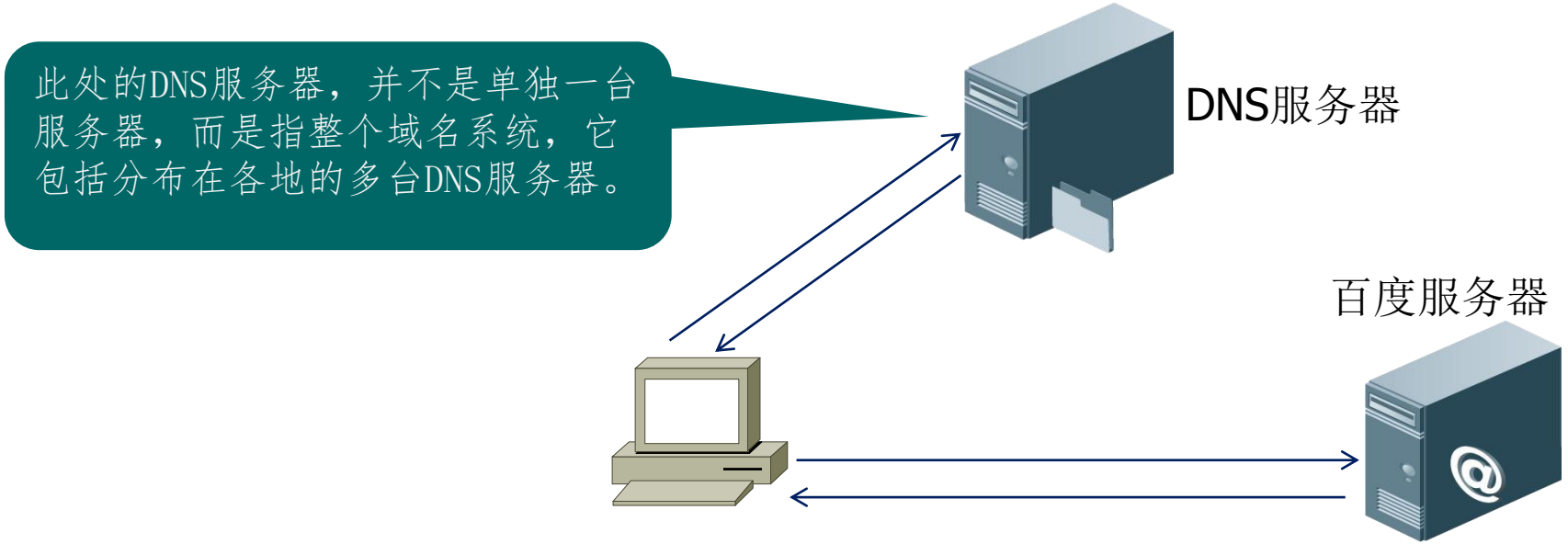



客户机事先要知道DNS服务器的IP地址

# DNS —— 域名服务器

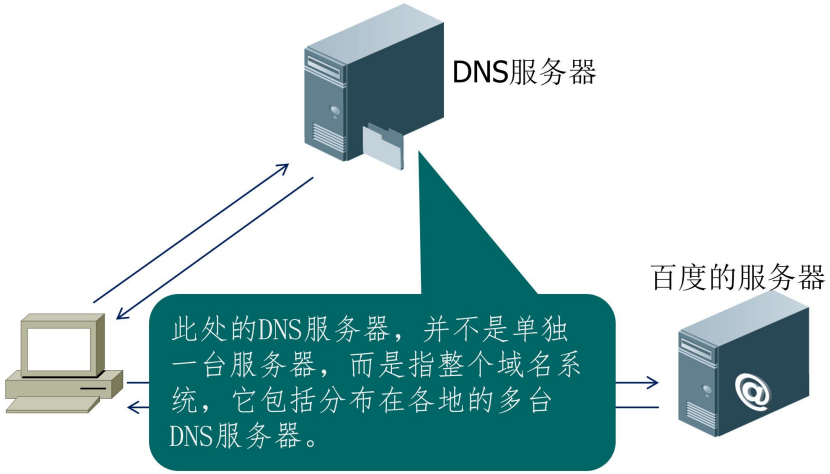
- 引申分析：能让一台DNS服务器负责全球域名的解析吗？
  - 全球的域名解析需要一个健壮的、可扩展的域名解析体系架构，即要把域名解析的任务分摊到多个DNS服务器上。



# 对域名系统（DNS）的进一步认识

- 前面提到：“互联网用户要想使用域名服务，就必须事先知道域名服务器的IP地址”

问题：互联网上的域名系统中，有非常多的域名服务器，我需要事先知道哪一个的IP地址？



# DNS —— 域名服务器

- 域名服务器的分类
  - 根据域名服务器所起的作用，可以把域名服务器划分为以下四种不同的类型：

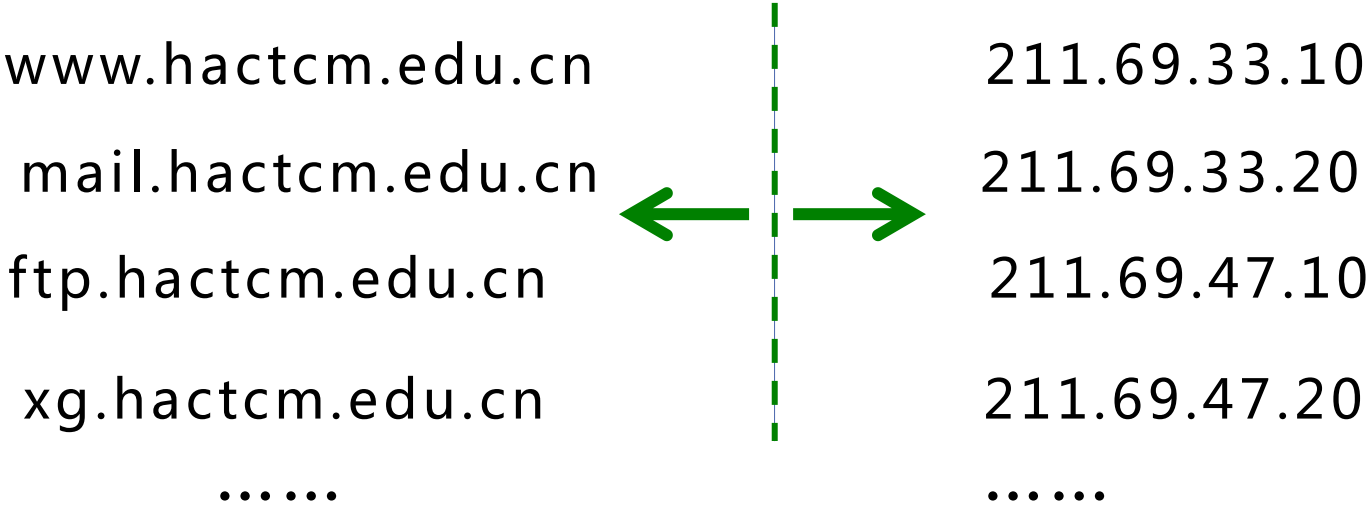
根域名服务器
顶级域名服务器
权限域名服务器

本地域名服务器

# DNS —— 域名服务器

- 整个域名系统的服务，是通过分布在各地的域名服务器来实现的。
- 互联网上的DNS域名服务器是按照层次和区域安排的；每一个域名服务器都只对整个域名体系中的一部分进行管辖；
  - 一个DNS服务器所负责管辖的范围叫做区。一个区内设置的DNS服务器通常叫做权限域名服务器，用来保存该区中所有主机的域名到IP地址的映射（即域名记录）。

# 例：河南中医药大学有很多网站，对应的有IP地址

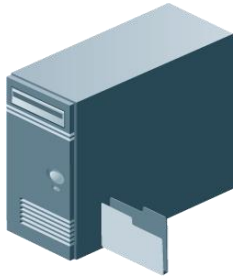



这种映射关系，由中医药大学内部的一台DNS服务器（假设其IP地址是211.69.32.8）负责解析

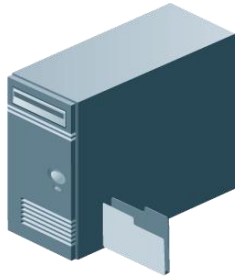
# DNS —— 域名服务器

- 我们可以“告诉”自己的PC：若想访问www.hactcm.edu.cn，就去找DNS服务器211.69.32.8行解析。
- 问题：
  1. 若我想访问www.baidu.com，该找谁来解析？
  2. 若北京的一台PC想访问www.hactcm.edu.cn，他怎么知道该找211.69.32.8来解析？

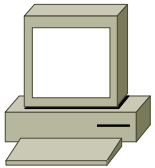
DNS_b



DNS_c

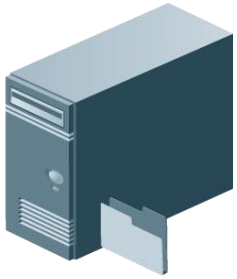


域名解析请求到底发给谁？

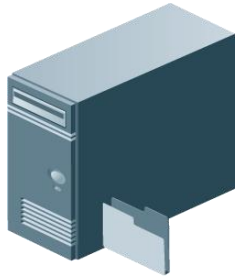


用户主机

DNS_a

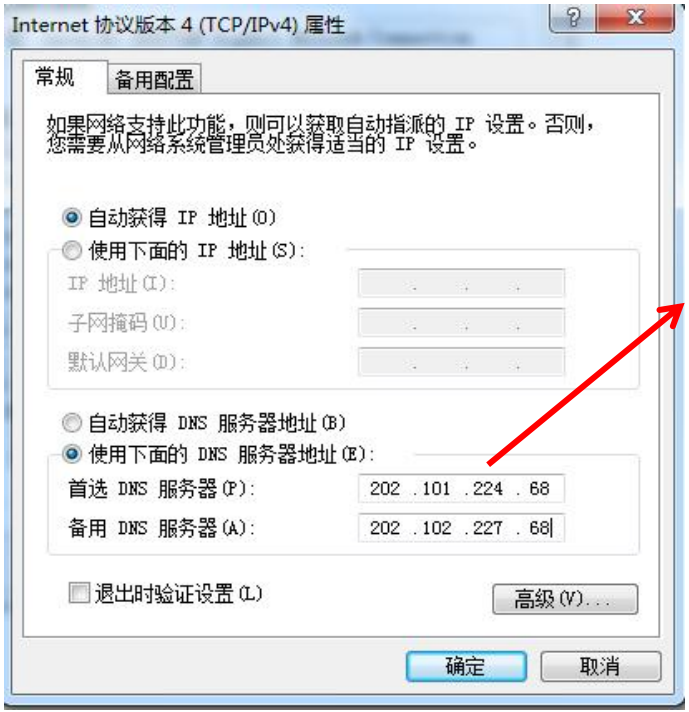


DNS_d



# DNS —— 域名服务器

- 本地域名服务器
  - 用户在本机系统中所设置的DNS服务器，就被认为是本地域名服务器；




# DNS —— 域名服务器

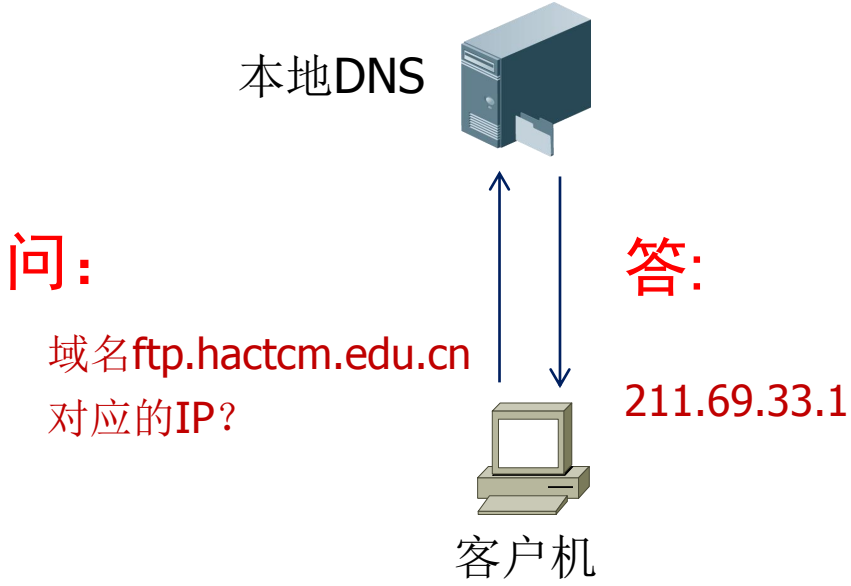
- 本地域名服务器
  - 当客户机发出 DNS 请求时，这个请求报文就首先发送给本地域名服务器。
  - 每一个互联网服务提供者 ISP，或一个大学，甚至一个大学里的系，都可以提供一个域名服务器，用作本区域客户机的本地域名服务器；
  - 本地域名服务器在域名解析过程中起着重要作用，帮助客户机从互联网的域名系统中获得域名解析结果，并将结果发回给客户机。

# DNS —— 域名服务器

- 本地域名服务器
  - 举例：
  - 河南中医药大学校园网内部有一台DNS服务器（假设其IP地址是211.69.32.8），该服务器内部记录有河南中医药大学内部各应用服务器（例如ftp、Web、mail等服务器）的主机名和IP地址的映射关系；
  - 校园网用户可以把该服务器作为自己的本地DNS服务器，通过该服务器来进行域名解析，例如访问ftp.hactcm.edu.cn，通过该DNS服务器可解析出其对应的IP地址。

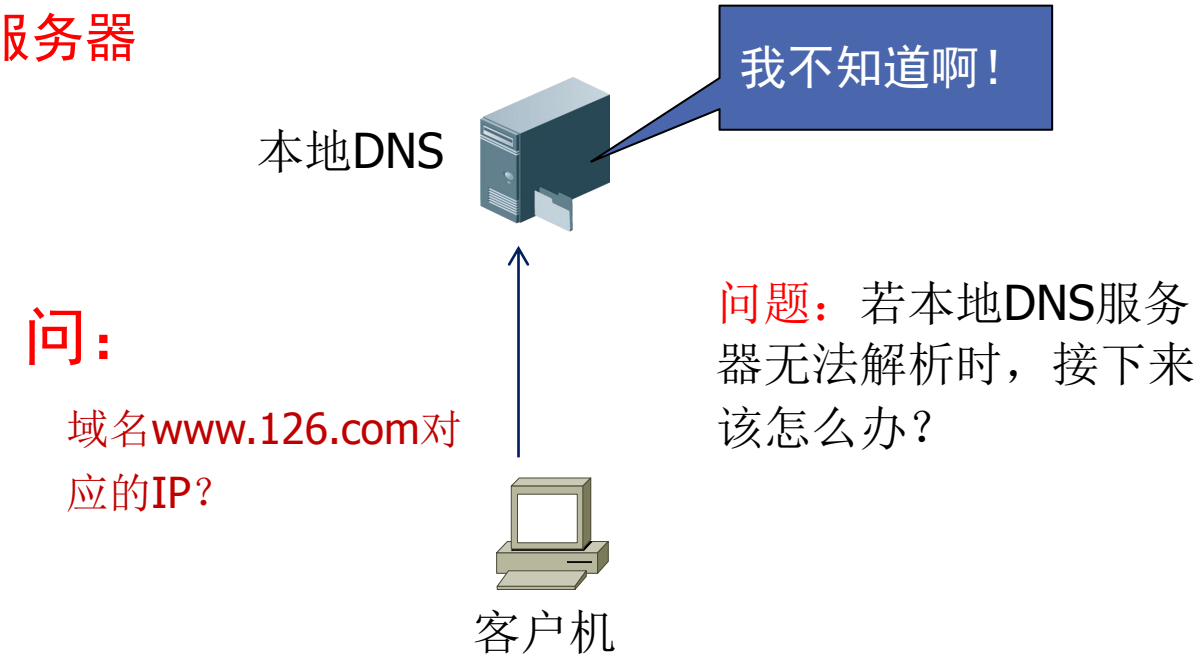
# DNS —— 域名服务器

- 本地域名服务器



# DNS —— 域名服务器

- 本地域名服务器



# DNS —— 域名服务器

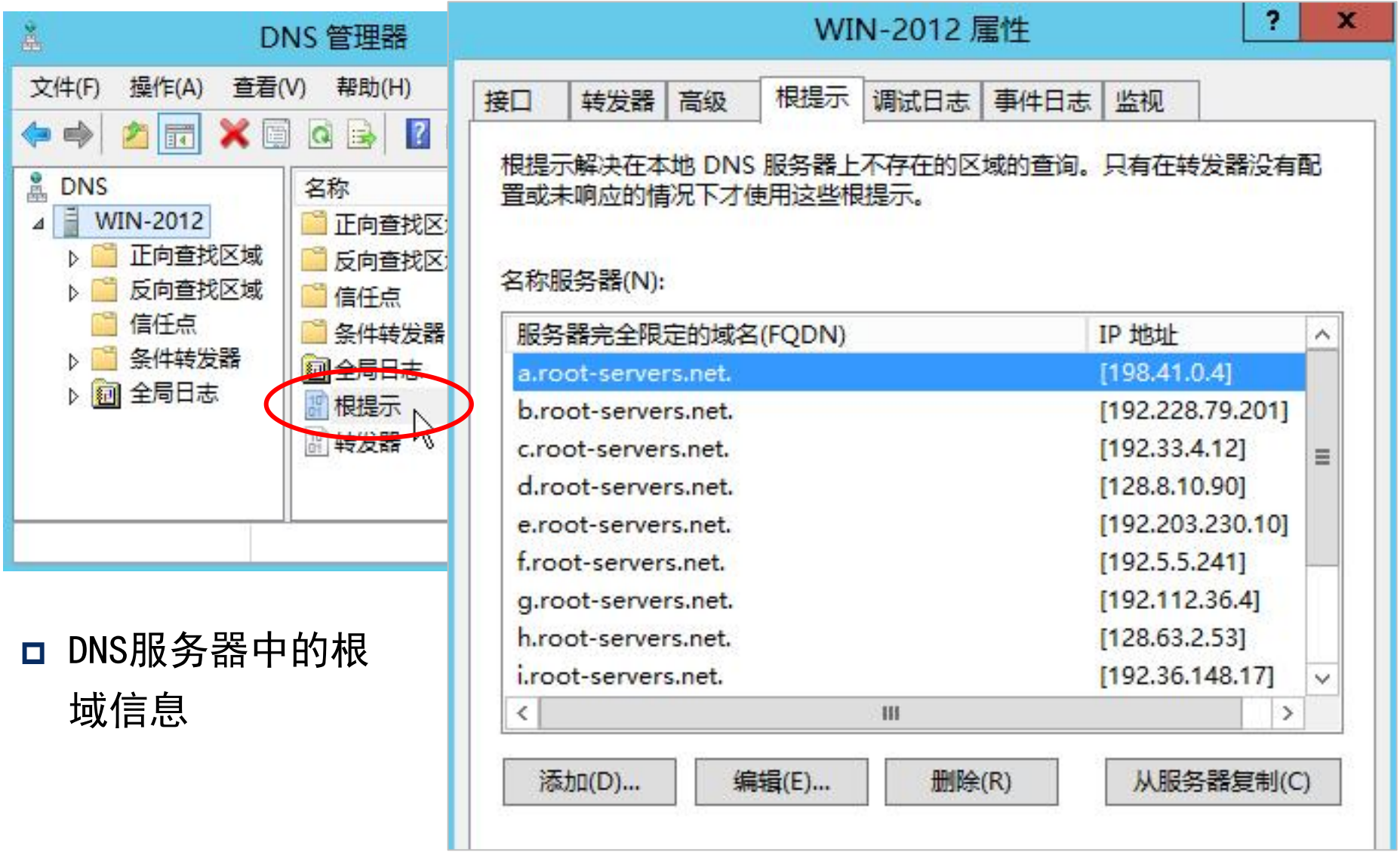
- 根域名服务器
  - 在给一台服务器安装DNS服务程序时，会自动安装根域名服务器（共13套）的相关信息，包括每台根域名服务器的域名和对应的IP地址。因此，当本地DNS服务器不知道待查域名的IP地址时，就把请求发给根域服务器；
  - 根DNS服务器是由互联网管理机构配置建立的，是最高层次的DNS服务器，负责对互联网上所有顶级DNS服务器进行管理，含有全部顶级DNS服务器的IP地址和域名映射。
  - 根DNS服务器并不直接用于域名解析，仅负责管理顶级DNS服务器的相关记录。当本地DNS服务器解析不了某个域名时，告诉本地DNS服务器去找哪个顶级DNS服务器。【我不知道目的地在哪？但我知道下一步怎么走！】

# DNS —— 域名服务器

- 根域名服务器
  - 在互联网上共有13 套不同 IP 地址的根域名服务器，它们的名字是用一个英文字母命名，从a 一直到 m（前13 个字母）。相应的域名分别是：

    a.rootservers.net
    b.rootservers.net
    ……
    m.rootservers.net

  - 到 2021 年，全球共有1375个根域名服务器在运行。这样做的目的是为了方便用户，使世界上大部分 DNS 域名服务器都能就近找到一个根域名服务器




- DNS服务器中的根域信息

# DNS -

- 全球

表 5-02 13 台主根 DNS 服务器的管理机构和 IP 地址

| 名称 | 管理单位及设置地点 | IP 地址 |
|---|---|---|
| A | INTERNIC.NET（美国，弗吉尼亚州） | 198.41.0.4 |
| B | 美国信息科学研究所（美国，加利弗尼亚州） | 128.9.0.107 |
| C | PSINet 公司（美国，弗吉尼亚州） | 192.33.4.12 |
| D | 马里兰大学（美国马里兰州） | 128.8.10.90 |
| E | 美国航空航天管理局（美国加利弗尼亚州） | 192.203.230.10 |
| F | 因特网软件联盟（美国加利弗尼亚州） | 192.5.5.241 |
| G | 美国国防部网络信息中心（美国弗吉尼亚州） | 192.112.36.4 |
| H | 美国陆军研究所（美国马里兰州） | 128.63.2.53 |
| I | Autonomica 公司（瑞典，斯德哥尔摩） | 192.36.148.17 |
| J | VeriSign 公司（美国，弗吉尼亚州） | 192.58.128.30 |
| K | RIPE NCC（英国，伦敦） | 193.0.14.129 |
| L | IANA（美国，弗吉尼亚州） | 198.32.64.12 |
| M | WIDE Project（日本，东京） | 202.12.27.33 |

# DNS —— 域名服务器

- 顶级域名服务器
  - 负责管理在该顶级域名服务器注册的所有二级域名。
  - 当收到 DNS 查询请求时，就给出相应的回答，可能是最后的结果，也可能是下一步应当找的域名服务器（权限域名服务器）的 IP 地址。

# DNS —— 域名服务器

- 权限域名服务器（又被称为权威域名服务器）
  - 这就是前面已经讲过的负责一个区域的域名服务器。
  - 当一个权限域名服务器还不能给出最后的查询回答时，就会告诉发出查询请求的 DNS 客户，下一步应当找哪一个权限域名服务器。
  - 例如 211.69.32.8　就是河南中医药大学的 权限域名服务器，它由河南中医药大学负责建设维护，负责河南中医药大学内部的服务器的域名解析，该DNS服务器在其上级域中有备案。

# 一、DNS

## 1.3 域名解析过程

# 举例：

一台客户机想访问www. 126. com

首先，客户机先在本机上查找关于www.126.com的记录

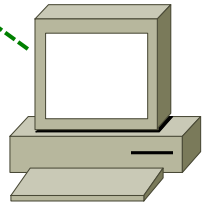
# 第1步：

客户机所做的的工作

www.126.com

IP地址?

访问：www.126.com



（1）步骤1：查询自己的缓存，看看有没有记录www.126.com对应的IP地址，若有直接获得。

否

（2）步骤2：查询自己的hosts文件，看看有没有记录www.126.com对应的IP地址，若有直接获得。

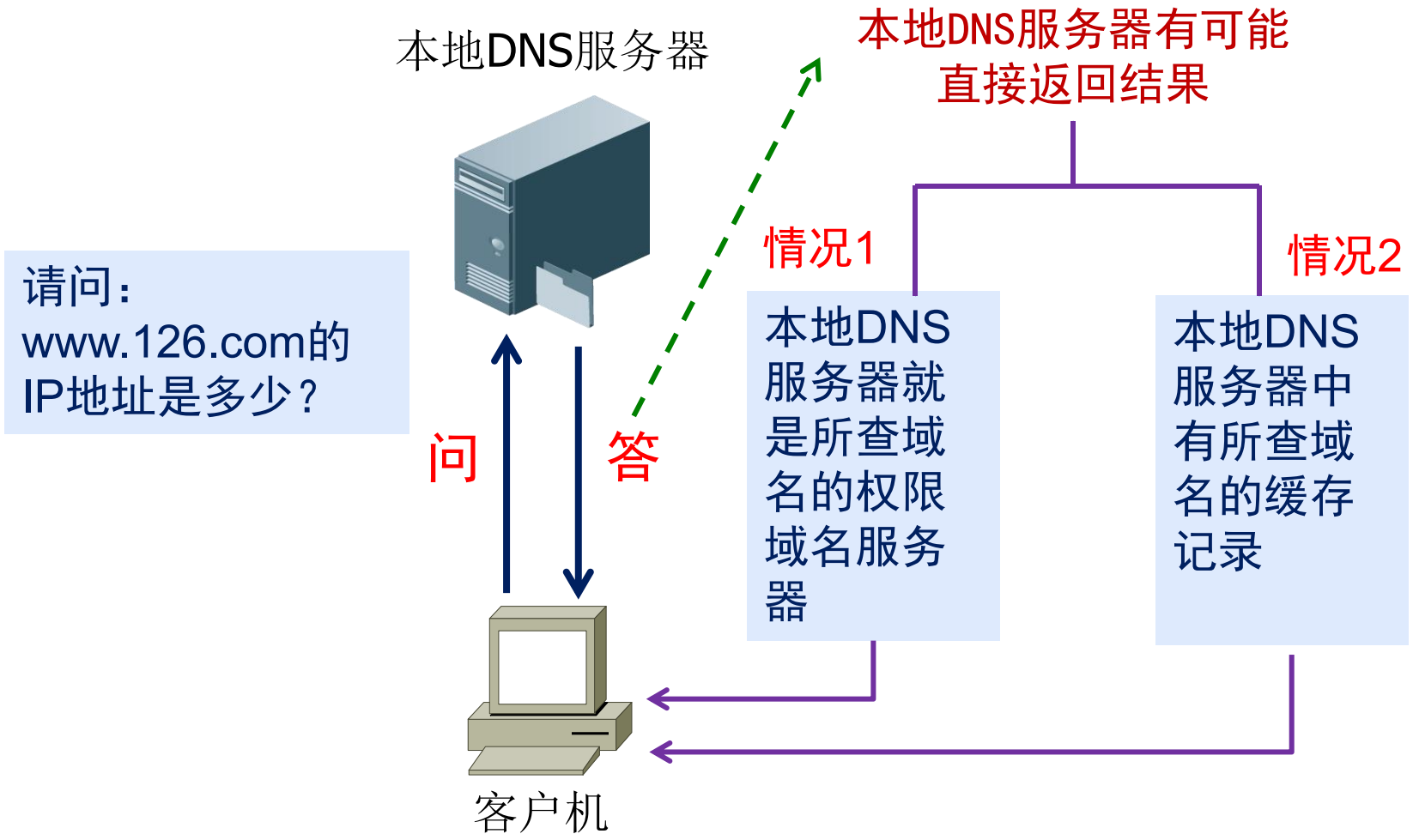
否

（3）步骤3：向本地DNS服务器发出域名解析请求。

# 域名解析过程举例

若本机上没有关于www.126.com的记录，则客户机把DNS解析请求发给本地DNS服务器

假设： 本地DNS服务器是 211.69.32.8


本地DNS服务器
本地DNS服务器有可能
直接返回结果
请问：
www.126.com的
IP地址是多少？
问
答
情况1
本地DNS
服务器就
是所查域
名的权限
域名服务
器
情况2
本地DNS
服务器中
有所查域
名的缓存
记录
客户机

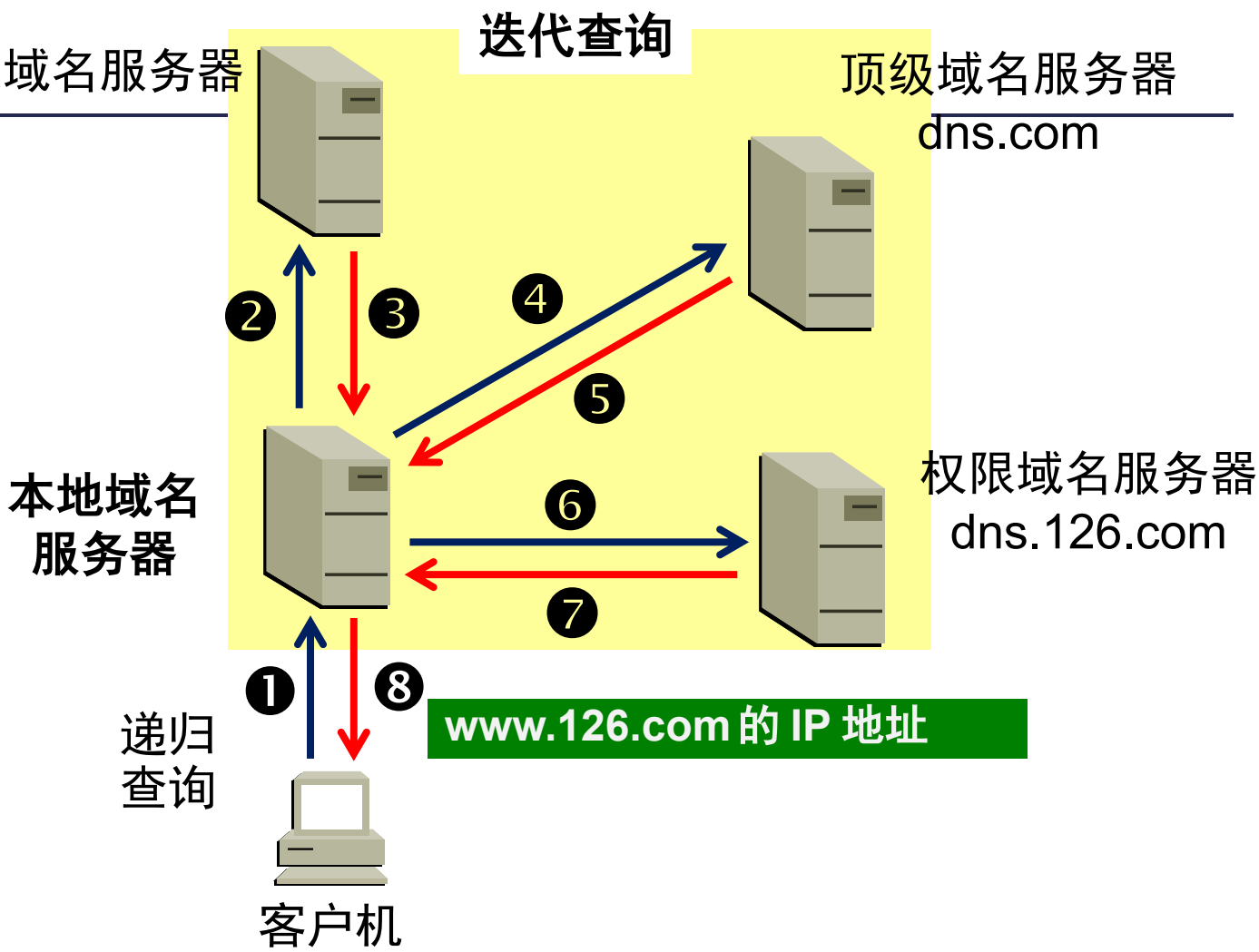
# 域名解析过程举例

如果本地DNS服务器不能解决问题，怎么办？

如果本地DNS服务器无法解析域名 www.126.com，则本地DNS服务器就向互联网上的域名系统发出解析请求。

具体步骤如下：

本地域名服务器采用迭代查询



# 域名的解析过程

- 主机向本地域名服务器的查询一般都是采用递归查询。如果本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向根域名服务器继续发出查询请求报文。
- 本地域名服务器向根域名服务器的查询通常是采用迭代查询。当根域名服务器收到本地域名服务器的迭代查询请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地域名服务器进行后续的查询。
- 以此类推，直至结束。

# 例2：一个电信用户访问 www. hactcm.edu.cn

# 举例：一个电信用户访问 www. hactcm.edu.cn

1. 用户主机提出域名解析请求，并将该请求发给本地DNS服务器（电信的公共DNS）。
2. 本地DNS服务器收到请求后就去查询自己的缓存，如果有该条记录，则会将查询的结果返回给客户端。
3. 本地DNS服务器无法解析该域名，因此，本地域名服务器就以 DNS 客户的身份向根DNS（13台根DNS服务器的IP信息默认均存储在DNS服务器中，当需要时就会去有选择性的连接）发出解析请求。

# 举例：一个电信用户访问 www. hactcm.edu.cn

4. 根DNS服务器收到请求后，也不知道该域名的IP地址，但是，它判断这个域名的顶级域名是cn，根DNS服务器就会把. cn的顶级域名DNS服务器的IP地址返回给本地DNS服务器。
5. 本地DNS服务器收到这个地址后，就开始联系dns. cn，并将此请求发给他。该顶级域名服务器经过解析，把dns. edu. cn的地址返回给本地域名服务器。

- 含义：我虽然不知道www. hactcm. edu. cn的IP，但我知道该域名是属于edu. cn域的，而我知道dns. edu. cn这台域名解析服务器的IP，你去找它问问吧。

# 举例：一个电信用户访问 www. hactcm.edu.cn

6. 本地DNS服务器收到dns. edu. cn域名服务器的地址后，就会重复上面的动作。
7. dns. edu. cn收到请求后，进行解析。它也不知道www. hactcm. edu. cn的IP，但它知道该域名属于. hactcm. edu. cn这个域，而它知道dns. hactcm. edu. cn这个权限域名服务器的地址，因此它把该地址返回给本地DNS。

- 注意：此处的dns. hactcm. edu. cn就是一个权限域名服务器。

# 举例：一个电信用户访问 www. hactcm.edu.cn

8. 本地DNS服务器收到这个权限域名服务器地址后，再次重复上面的动作，找到dns.hactcm.edu.cn这台权限域名服务器，并把域名解析请求发给它；
9. 该DNS服务器在自己的数据库中查到了www.hactcm.edu.cn这个域名所对应的IP，并把地址返回给本地DNS服务器。

准确的讲：　www.hactcm.edu.cn —— 211.69.32.5　是权限域名服务器（dns.hactcm.edu.cn）的数据库当中的一条记录（A记录）。

至此，域名系统的解析工作完成了。

# 举例：一个电信用户访问 www. hactcm.edu.cn

- 现在，本地DNS服务器终于获得www.hactcm.edu.cn的IP，然后把这个IP返回给客户机，整个解析工作全部完成。接下来，客户端主机（该电信用户）根据此IP去访问www.hactcm.edu.cn。
- 提醒：
  - 可以看出，在整个解析过程中，客户端主机把域名解析请求发给本地域名服务器以后，就一直处理等待状态，他不需要做任何事，也做不了什么。
  - 本地域名服务器收到该请求，就代替客户端主机向因特网的域名解析系统发出查询请求。直到把结果返回给客户端主机。（注意：查询析结果可能失败）

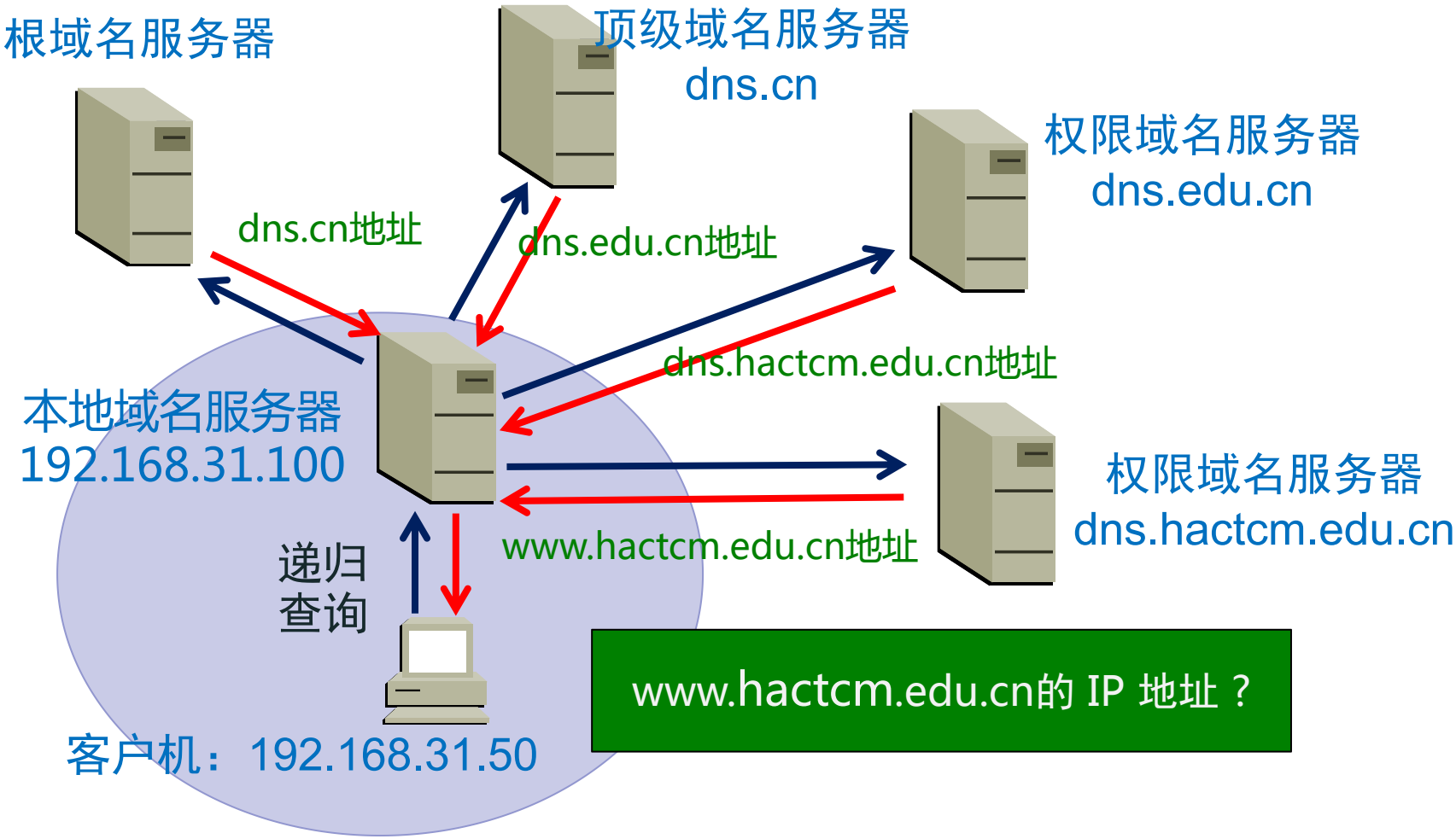
# 例3：抓包分析域名解析过程

（自主学习）

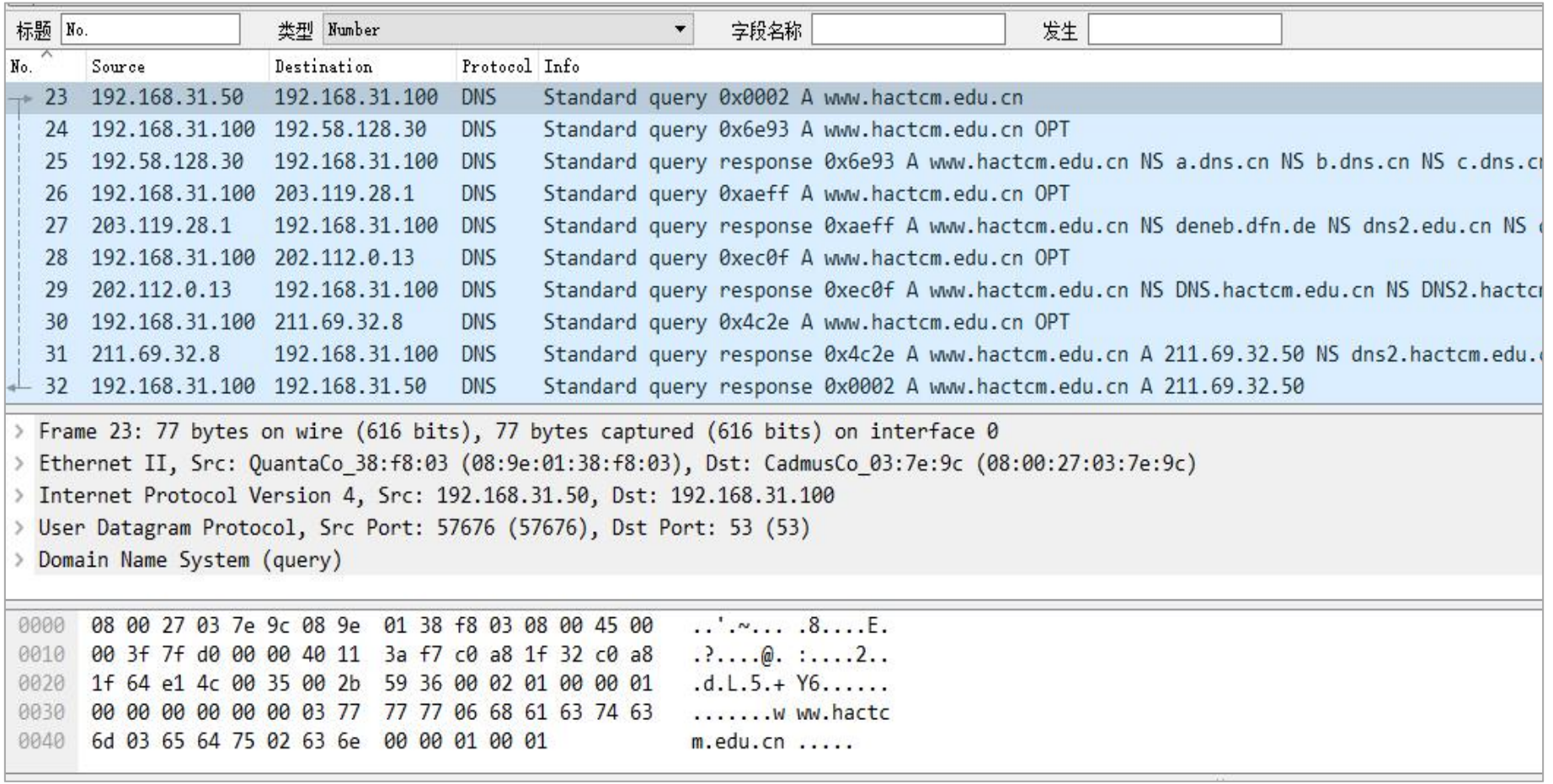
# 【案例】抓包分析域名解析过程

- 场景描述
  - 用户在家中上网，通过无线路由器NAT接入互联网（ISP是河南电信）
  - 用户主机IP：192.168.31.50，本地DNS是192.168.31.100
  - 用户现在访问www.hactcm.edu.cn，即部署在河南中医药大学的一台WWW服务器
  - 域名.hactcm.edu.cn对应的权限DNS地址是211.69.32.8，该域名及对应的权限DNS服务器已经在中国教科网（ISP）中进行了注册；
  - 假设，本地DNS中（包括缓存中），没有www.hactcm.edu.cn对应的域名记录信息。

## ➢ 域名解析过程总体描述


根域名服务器
顶级域名服务器
dns.cn
权限域名服务器
dns.edu.cn
dns.cn地址
dns.edu.cn地址
dns.hactcm.edu.cn地址
本地域名服务器
192.168.31.100
递归
查询
www.hactcm.edu.cn地址
权限域名服务器
dns.hactcm.edu.cn
www.hactcm.edu.cn的 IP 地址？
客户机：192.168.31.50

# ➢ 域名解析过程的整体报文一览

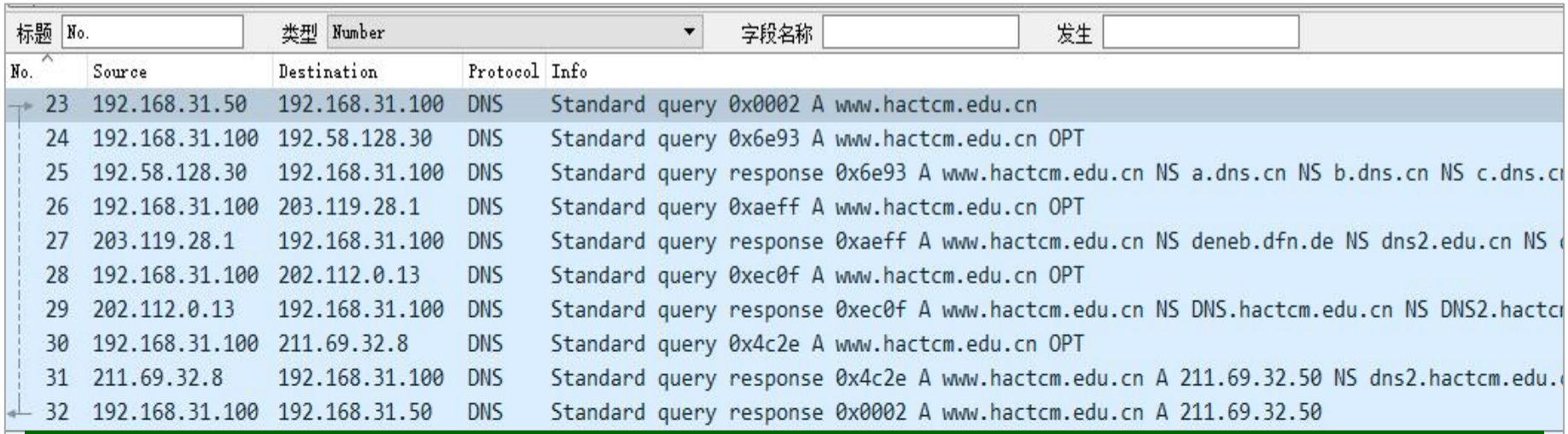


标题 No. 类型 Number 字段名称 发生

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 23 | 192.168.31.50 | 192.168.31.100 | DNS | Standard query 0x0002 A www.hactcm.edu.cn |
| 24 | 192.168.31.100 | 192.58.128.30 | DNS | Standard query 0x6e93 A www.hactcm.edu.cn OPT |
| 25 | 192.58.128.30 | 192.168.31.100 | DNS | Standard query response 0x6e93 A www.hactcm.edu.cn NS a.dns.cn NS b.dns.cn NS c.dns.cn |
| 26 | 192.168.31.100 | 203.119.28.1 | DNS | Standard query 0xaeff A www.hactcm.edu.cn OPT |
| 27 | 203.119.28.1 | 192.168.31.100 | DNS | Standard query response 0xaeff A www.hactcm.edu.cn NS deneb.dfn.de NS dns2.edu.cn NS |
| 28 | 192.168.31.100 | 202.112.0.13 | DNS | Standard query 0xec0f A www.hactcm.edu.cn OPT |
| 29 | 202.112.0.13 | 192.168.31.100 | DNS | Standard query response 0xec0f A www.hactcm.edu.cn NS DNS.hactcm.edu.cn NS DNS2.hactcm |
| 30 | 192.168.31.100 | 211.69.32.8 | DNS | Standard query 0x4c2e A www.hactcm.edu.cn OPT |
| 31 | 211.69.32.8 | 192.168.31.100 | DNS | Standard query response 0x4c2e A www.hactcm.edu.cn A 211.69.32.50 NS dns2.hactcm.edu. |
| 32 | 192.168.31.100 | 192.168.31.50 | DNS | Standard query response 0x0002 A www.hactcm.edu.cn A 211.69.32.50 |

```
> Frame 23: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
> Ethernet II, Src: QuantaCo_38:f8:03 (08:9e:01:38:f8:03), Dst: CadmusCo_03:7e:9c (08:00:27:03:7e:9c)
> Internet Protocol Version 4, Src: 192.168.31.50, Dst: 192.168.31.100
> User Datagram Protocol, Src Port: 57676 (57676), Dst Port: 53 (53)
> Domain Name System (query)
```

```
0000  08 00 27 03 7e 9c 08 9e  01 38 f8 03 08 00 45 00   ..'.~... .8....E.
0010  00 3f 7f d0 00 00 40 11  3a f7 c0 a8 1f 32 c0 a8   .?....@. :....2..
0020  1f 64 e1 4c 00 35 00 2b  59 36 00 02 01 00 00 01   .d.L.5.+ Y6......
0030  00 00 00 00 00 00 03 77  77 77 06 68 61 63 74 63   .......w ww.hactc
0040  6d 03 65 64 75 02 63 6e  00 00 01 00 01            m.edu.cn .....
```




(23)192.168.31.50 → 192.168.31.100 客户机 → 本地DNS

(24)192.168.31.100 → 192.58.128.30 本地DNS → 根DNS

(25)192.58.128.30 → 192.168.31.100 根DNS → 本地DNS

(26) 192.168.31.100 → 203.119.28.1 本地DNS → 顶级DNS( .cn )

(27) 203.119.28.1 → 192.168.31.100 顶级DNS(.cn) → 本地DNS

(28) 192.168.31.100 → 202.112.0.13 本地DNS → 权限DNS( .edu.cn)

(29) 202.112.0.13 → 192.168.31.100 权限DNS(.edu.cn) → 本地DNS

(30) 192.168.31.100 → 211.69.32.8 本地DNS → 权限DNS (.hactcm.edu.cn )

(31) 211.69.32.8 → 192.168.31.100 权限DNS( .hactcm.edu.cn) → 本地DNS

(32) 192.168.31.100 → 192.168.31.50 本地DNS → 客户机

## (23)192.168.31.50 → 192.168.31.100 客户机 → 本地DNS

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 23 | 192.168.31.50 | 192.168.31.100 | DNS | Standard query 0x0002 A www.hactcm.edu.cn |

客户机向本地DNS服务器发出解析请求

客户机是192.168.31.50，本地DNS服务器是192.168.31.100

## (24) 192.168.31.100 → 192.58.128.30　　本地DNS → 根DNS

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 23 | 192.168.31.50 | 192.168.31.100 | DNS | Standard query 0x0002 A www.hactcm.edu.cn |

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 24 | 192.168.31.100 | 192.58.128.30 | DNS | Standard query 0x6e93 A www.hactcm.edu.cn OPT |

本地DNS服务器（192.168.31.100）把解析请求发给一台根域名服务器，此处为192.58.128.30。

## (25) 192.58.128.30 → 192.168.31.100 根DNS → 本地DNS

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 24 | 192.168.31.100 | 192.58.128.30 | DNS | Standard query 0x6e93 A www.hactcm.edu.cn OPT |

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 25 | 192.58.128.30 | 192.168.31.100 | DNS | Standard query response 0x6e93 A www.hactcm.edu.cn |

NS a.dns.cn NS b.dns.cn NS c.dns.cn NS d.dns.cn NS e.dns.cn NS…

根域名服务器（192.58.128.30）并不知道www.hactcm.edu.cn对应的IP地址是什么，不过，它发现www.hactcm.edu.cn的顶级域名是. cn，而它知道顶级域名服务器dns.cn的IP地址（203.119.28.1 ），于是，它告诉了（即应答）本地DNS服务器（192.168.31.100）

## (25) 192.58.128.30 → 192.168.31.100 根DNS → 本地DNS

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 25 | 192.58.128.30 | 192.168.31.100 | DNS | Standard |
| 26 | 192.168.31.100 | 203.119.28.1 | DNS | Standard |
| 27 | 203.119.28.1 | 192.168.31.100 | DNS | Standard |

```
> Frame 25: 558 bytes on wire (4464 bits), 558 bytes
> Ethernet II, Src: XiaomiCo_1d:4f:3a (f0:b4:29:1d:4f
> Internet Protocol Version 4, Src: 192.58.128.30, Ds
> User Datagram Protocol, Src Port: 53 (53), Dst Port
v Domain Name System (response)
    [Request In: 24]
    [Time: 0.194208000 seconds]
    Transaction ID: 0x6e93
  > Flags: 0x8000 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 8
    Additional RRs: 9
  > Queries
  > Authoritative nameservers
  > Additional records
```

根DNS反馈的.cn 域名服务器的地址 203.119.28.1

```
  Authority RRs: 8
  Additional RRs: 9
> Queries
                                                dns.cn
                                                dns.cn
                                                dns.cn
                                                dns.cn
                                                dns.cn
                                                ns.cernet.net
  > cn: type DS, class
  > cn: type RRSIG, class
v Additional records
  > a.dns.cn: type A, class IN, addr 203.119.25.1
  > b.dns.cn: type A, class IN, addr 203.119.26.1
  > c.dns.cn: type A, class IN, addr 203.119.27.1
  > d.dns.cn: type A, class IN, addr 203.119.28.1
  > e.dns.cn: type A, class IN, addr 203.119.29.1
  > ns.cernet.net: type A, class IN, addr 202.112.0.44
  > a.dns.cn: type AAAA, class IN, addr 2001:dc7::1
  > d.dns.cn: type AAAA, class IN, addr 2001:dc7:1000::1
  > <Root>: type OPT
```

## (26) 192.168.31.100 → 203.119.28.1 本地DNS → 顶级DNS .cn

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 26 | 192.168.31.100 | 203.119.28.1 | DNS | Standard query 0xaeff A www.hactcm.edu.cn OPT |

本地DNS服务器(192.168.31.100)向203.119.28.1发出解析请求（query）。而203.119.28.1是 .cn顶级域名服务器中的一台（即d.dns.cn）

## (27) 203.119.28.1 → 192.168.31.100 顶级DNS .cn → 本地DNS

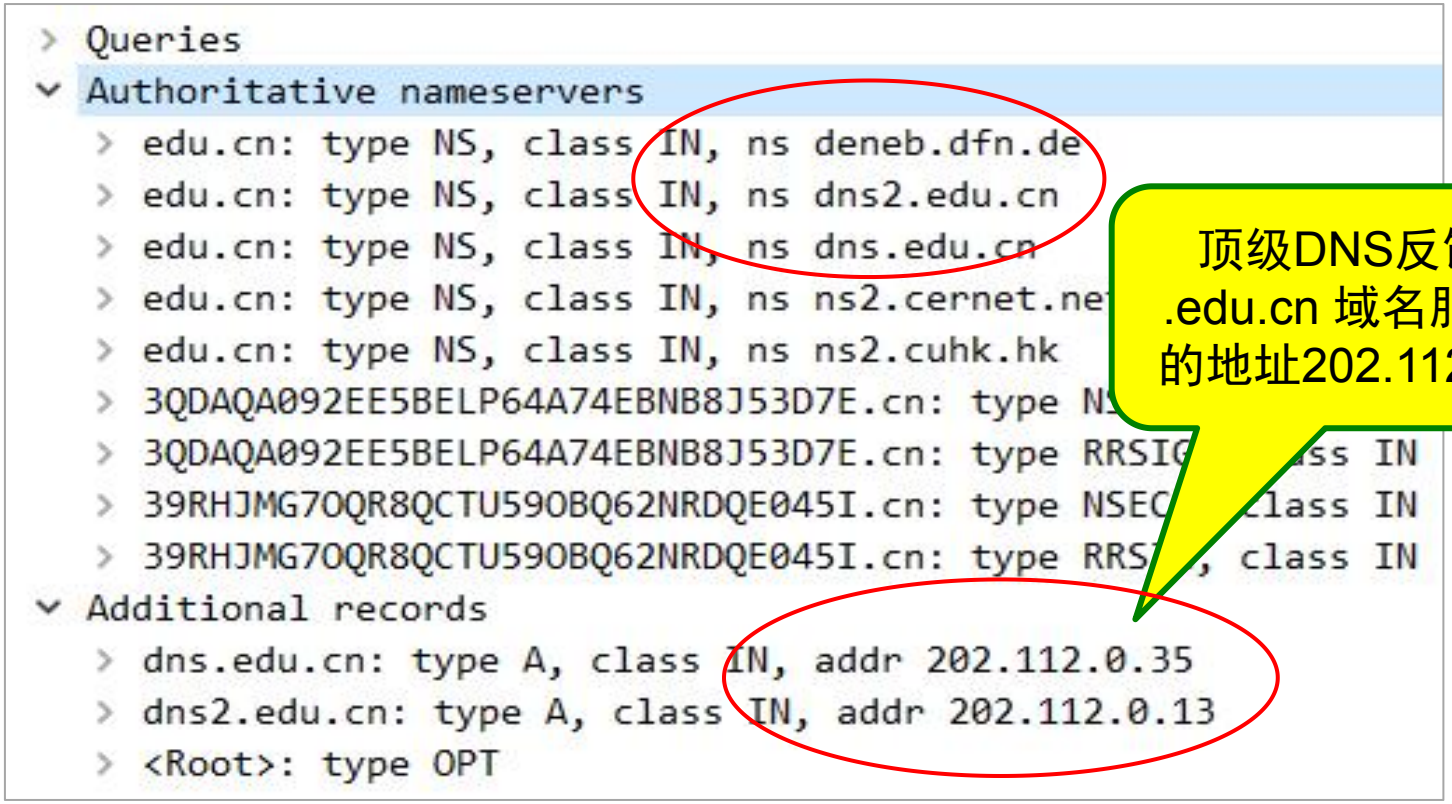
| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 26 | 192.168.31.100 | 203.119.28.1 | DNS | Standard query 0xaeff A www.hactcm.edu.cn OPT |

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 27 | 203.119.28.1 | 192.168.31.100 | DNS | Standard query response 0xaeff |

A www.hactcm.edu.cn NS deneb.dfn.de NS dns2.edu.cn NS dns.edu.cn NS n…

. cn的顶级域名服务器（203.119.28.1）也不知道www.hactcm.edu.cn对应的IP地址是什么，不过，它发现www.hactcm.edu.cn的二级域名是.edu，而它知道域名服务器dns.edu.cn的IP地址（ 202.112.0.13 ），于是，它告诉了（即应答）本地DNS服务器192.168.31.100。

## (27) 203.119.28.1 → 192.168.31.100 顶级DNS .cn → 本地DNS



## (28) 192.168.31.100 → 202.112.0.13　　本地DNS → 权限DNS .edu.cn

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 28 | 192.168.31.100 | 202.112.0.13 | DNS | Standard query 0xec0f A www.hactcm.edu.cn OPT |

本地DNS服务器(192.168.31.100)向202.112.0.13发出解析请求（query）。而202.112.0.13是 .edu.cn域名服务器中的一台（即dns2.edu.cn）。

## (29) 202.112.0.13 → 192.168.31.100 权限DNS .edu.cn → 本地DNS

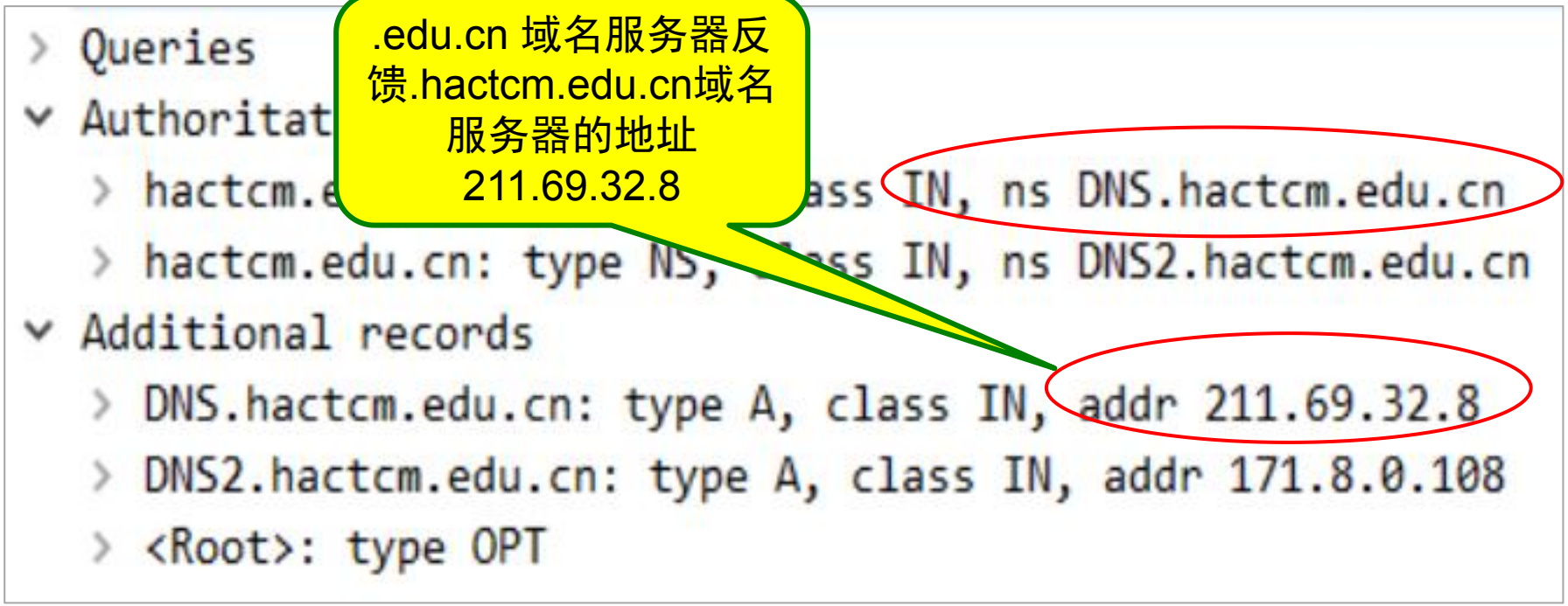
| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 28 | 192.168.31.100 | 202.112.0.13 | DNS | Standard query 0xec0f A www.hactcm.edu.cn OPT |

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 29 | 202.112.0.13 | 192.168.31.100 | DNS | Standard query response 0xec0f A www.hactcm.edu.cn |

NS DNS.hactcm.edu.cn NS DNS2.hactcm.edu.cn A 211.69.32.8 A 171.8.0.1…

. edu.cn的域名服务器（202.112.0.13）也不知道www.hactcm.edu.cn对应的IP地址是什么，不过，它发现www.hactcm.edu.cn的三级域名是.hactcm，而它知道域名服务器dns.hactcm.edu.cn的IP地址，于是，它告诉了（即应答）本地DNS服务器。

## (29) 202.112.0.13 → 192.168.31.100 权限DNS .edu.cn → 本地DNS



## (30) 192.168.31.100 → 211.69.32.8　　本地DNS → 权限DNS .hactcm.edu.cn

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 30 | 192.168.31.100 | 211.69.32.8 | DNS | Standard query 0x4c2e A www.hactcm.edu.cn OPT |

本地DNS服务器(192.168.31.100)向211.69.32.8发出解析请求（query）。而211.69.32.8是 域名服务器dns.hactcm.edu.cn的IP地址。

## (31) 211.69.32.8 → 192.168.31.100 权限DNS .hactcm.edu.cn → 本地DNS

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 30 | 192.168.31.100 | 211.69.32.8 | DNS | Standard query 0x4c2e A www.hactcm.edu.cn OPT |

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 31 | 211.69.32.8 | 192.168.31.100 | DNS | Standard query response 0x4c2e |

A www.hactcm.edu.cn A 211.69.32.50 NS dns2.hactcm.edu.cn NS dns.hactcm.edu.cn …

域名服务器dns.hactcm. edu.cn（211.69.32.8）就是域名www.hactcm.edu.cn的权限域名服务器，在其数据库中保存有域名www.hactcm.edu.cn对应的IP地址（即一条A记录），经过解析，它告诉了（即应答）本地DNS服务器（192.168.31.100）

(31) 211.69.32.8 → 192.168.31.100 权限DNS .hactcm.edu.cn → 本地DNS

(32) 192.168.31.100 → 192.168.31.50　　本地DNS → 客户机

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 32 | 192.168.31.100 | 192.168.31.50 | DNS | Standard query response 0x0002 A www.hactcm.edu.cn A 211.69.32.50 |

本地DNS服务器(192.168.31.100)向客户机Host-1（192.168.31.50）发回解析请求的结果

www.hactcm.edu.cn的 IP 地址 是 211.69.32.50

# DNS服务器的高速缓存

- 为了提高查询效率，每个域名服务器都维护一个高速缓存，存放最近用过的名字以及从何处获得名字映射信息的记录。例如，本地的DNS服务器虽然自身没有存放域名数据库信息，但当它获得一个解析结果后（即取得IP地址后），会将这条记录写入自己的缓存，以备后用。
- 通过利用缓存可大大减轻根域名服务器的负荷，使因特网上的 DNS 查询请求和回答报文的数量大为减少。
- 为保持高速缓存中的内容正确，域名服务器应为每项内容设置计时器，并处理超过合理时间的项（例如，每个项目只存放1天）。

【结合实验自主学习】

# 一、DNS

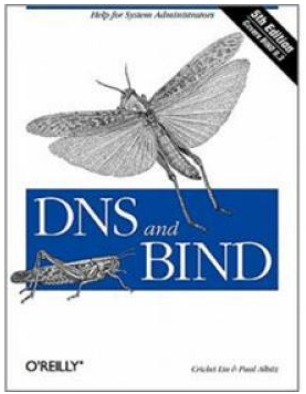
## 1.4 域名服务的配置

# DNS —— 域名服务的配置

## 认识BIND

- Linux下构建DNS服务器通常是使用BIND来实现的。
- BIND是Berkeley Internet Name Domain Service的简称，是一款实现DNS服务器的开源服务软件,已经成为世界上使用最为广泛的DNS服务器软件，目前Internet上绝大多数的DNS服务器都是用BIND来构建的。

CentOS + BIND



# DNS —— 域名服务的配置

- 安装BIND
  - BIND服务有关的软件包有如下几个：
  - **Bind:** BIND服务器端软件，即BIND 主程序。
  - **bind-chroot:** 为bind提供一个伪装的根目录以增强安全性（将“/var/named/chroot/文件夹作为BIND的根目录”）
  - **bind-utils:** 客户端搜索主机名的相关命令，提供nslookup及dig等测试工具
  - **bind-libs:** BIND相关的库文件

# DNS —— 域名服务的配置

- 使用yum命令安装BIND软件包，命令格式是：

```
yum -y install bind bind-chroot bind-utils bind-libs
```

# DNS —— 域名服务的配置

- 使用yum命令安装BIND软件包，操作截图

```
[root@localhost ~]# yum -y install bind bind-chroot bind-utils bind-libs
已加载插件：fastestmirror
base
extras
updates
(1/4): extras/7/x86_64/primary_db
(2/4): base/7/x86_64/group_gz
(3/4): base/7/x86_64/primary_db
(4/4): updates/7/x86_64/primary_db
Determining fastest mirrors
 * base: mirror.neu.edu.cn
 * extras: ftp.sjtu.edu.cn
 * updates: ftp.sjtu.edu.cn
正在解决依赖关系
--> 正在检查事务
---> 软件包 bind.x86_64.32.9.9.4-29.el7_2.3 将被 安装
---> 软件包 bind-chroot.x86_64.32.9.9.4-29.el7_2.3 将被 安装
---> 软件包 bind-libs.x86_64.32.9.9.4-29.el7_2.3 将被 安装
--> 正在处理依赖关系 bind-license = 32:9.9.4-29.el7_2.3，它被软件包 32:bind-libs-9.9
---> 软件包 bind-utils.x86_64.32.9.9.4-29.el7_2.3 将被 安装
--> 正在检查事务
---> 软件包 bind-license.noarch.32.9.9.4-18.el7 将被 升级
```

# DNS —— 域名服务的配置

- 使用yum命令安装BIND软件包，操作截图

```
================================================================================
 Package                架构      版本                       源          大小
================================================================================
正在安装:
 bind                   x86_64    32:9.9.4-29.el7_2.3        updates     1.8 M
 bind-chroot            x86_64    32:9.9.4-29.el7_2.3        updates      83 k
 bind-libs              x86_64    32:9.9.4-29.el7_2.3        updates     1.0 M
 bind-utils             x86_64    32:9.9.4-29.el7_2.3        updates     200 k
为依赖而更新:
 bind-libs-lite         x86_64    32:9.9.4-29.el7_2.3        updates     724 k
 bind-license           noarch    32:9.9.4-29.el7_2.3        updates      82 k

事务概要
================================================================================
安装  4 软件包
升级             ( 2 依赖软件包)

总下载量：3.8 M
```

# DNS —— 域名服务的配置

- BIND安装完成后会生成以下文件

| | |
|---|---|
| /etc/named.conf | bind主配置文件 |
| /etc/named.rfc1912.zones | 区域声明文件 |
| /var/named/named.localhost | 区域配置样例文件 |
| /var/named/named.ca | 根域名文件 |

# DNS —— 域名服务的配置

- BIND主要有三类配置文件
  - BIND的主配置文件：BIND主配置文件即 /etc/named.conf，里面有BIND的全局设置；
  - 区域声明文件：/etc/named.rfc1912.zones，里面列举了本机中各个区域记录配置文件的位置/类型/性质。在主配置文件named.conf中，使用“Include "/etc/named.rfc1912.zones"”语句来调用区域声明文件。
  - 区域配置文件：一个DNS服务器中可以设置多个区域配置文件，每一个区域配置文件指明了本DNS服务器所负责解析的某个区域中IP 和域名的对应关系，即各种记录内容，例如A记录、NS记录等。区域配置文件存放在/var/named目录下。

# ➢ 查看BIND主配置文件内容（1/4）

```
[root@localhost ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {    option语句
        listen-on port 53 { 127.0.0.1; };  侦听地址（IPv4）
        listen-on-v6 port 53 { ::1; };   侦听地址（IPv6）
        directory       "/var/named";    工作目录
        dump-file       "/var/named/data/cache_dump.db";  缓存文件
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; };  访问控制

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;  递归查询

        dnssec-enable yes;
        dnssec-validation yes;
```

# ➢ 查看BIND主配置文件内容（2/4）

```
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {  日志语句，用来记录日志
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN   zone语句，定义一个查找区域，此处定义的是根域
        type hint;
        file "named.ca";   指明根域配置文件的名字
};

include "/etc/named.rfc1912.zones";   include 语句，用来调用文件
include "/etc/named.root.key";

[root@localhost ~]#
```

# ➢ 查看BIND主配置文件内容（3/4）

- BIND配置文件中主要有10种命令语句。

| 命令语句 | 解释说明 |
| --- | --- |
| acl | 定义 IP 地址访问控制列表 |
| controls | 宣告认得 utility 使用的控制通道（channel） |
| include | 包含一个文件 |
| key | 设置密钥信息，它应用在通过 TSIG 进行授权和认证配置中 |
| logging | 设置日志服务器，和日志信息的发送地 |
| options | 控制服务器的全局配置选项和其它语句设置默认值 |
| server | 在一个单服务器基础上设置特定的配置选项 |
| trusted-keys | 定义信任的 DNSSED 密钥 |
| view | 定义一个视图 |
| zone | 定义一个域 |

# ➢ 查看BIND主配置文件内容（4/4）

- 关于根域配置文件named.ca
  - 在主配置文件named.conf中，定义了根域“.”，其对应的区域配置文件为named.ca。当DNS服务器无法解析某个域名时，就可以根据named.ca文件中的记录信息，向根域名服务器发出查询请求。
  - named.ca文件存放在 /var/named 目录中，使用 vi命令进行查看
    - named.ca文件的内容见下页

# ➢ 根域配置文件named. ca文件内容

```
;; ANSWER SECTION:
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3600000 IN      A       198.41.0.4
a.root-servers.net.     3600000 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3600000 IN      A       192.228.79.201
c.root-servers.net.     3600000 IN      A       192.33.4.12
d.root-servers.net.     3600000 IN      A       199.7.91.13
d.root-servers.net.     3600000 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3600000 IN      A       192.203.230.10
f.root-servers.net.     3600000 IN      A       192.5.5.241
f.root-servers.net.     3600000 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3600000 IN      A       192.112.36.4
h.root-servers.net.     3600000 IN      A       128.63.2.53
h.root-servers.net.     3600000 IN      AAAA    2001:500:1::803f:235
i.root-servers.net.     3600000 IN      A       192.36.148.17
i.root-servers.net.     3600000 IN      AAAA    2001:7fe::53
j.root-servers.net.     3600000 IN      A       192.58.128.30
j.root-servers.net.     3600000 IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     3600000 IN      A       193.0.14.129
k.root-servers.net.     3600000 IN      AAAA    2001:7fd::1
l.root-servers.net.     3600000 IN      A       199.7.83.42
l.root-servers.net.     3600000 IN      AAAA    2001:500:3::42
m.root-servers.net.     3600000 IN      A       202.12.27.33
m.root-servers.net.     3600000 IN      AAAA    2001:dc3::35
```

所有的根DNS服务器的相关记录

# ➢ 修改主配置文件的内容（1/2）

## 修改主配置文件中的侦听地址

- 配置named.conf，修改侦听地址，并允许所有主机可以访问。
- 在文件中找到：

```
listen-on port 53 { 127.0.0.1; };
allow-query       { localhost; };
```

- 改为：

```
listen-on port 53 { any; };
allow-query       { any; };
```

# ➢ 修改主配置文件的内容（2/2）

- 在主配置文件named.conf中定义查找区域
  - 在主配置文件中设置若干个查找区域，并在每个查找区域中指明该区域对应的区域配置文件。这样，在执行主配置文件时，就可以读取相应的区域配置文件，并查询其中的DNS记录。
  - 举例，此处定义一个名为“xuchenggang.net”的正向查找区域。

```
zone "xuchenggang.net" IN {
// 定义一个区域名称为“xuchenggang.net”的正向查找区域；
        type master;          // 区域类型为主要区域
        file "xuchenggang.net.zone";
// 将该查找区域的区域配置文件命名为“ xuchenggang.net.zone”。注意，此处为相对路径，即表示该文件将被放置在 /var/named下，也可写成绝对路径；
        allow-update { none; };
};
```

# DNS —— 域名服务的配置

- 创建区域配置文件
  - 注意，在上一步骤中，我们只是在主配置文件（named.conf）文件中定义（即声明）了一个区域xuchenggang.net，并且定义了这个区域的配置文件名。但是，相应的区域配置文件并没有创建。
  - 接下来要创建区域配置文件xuchenggang.net.zone，并在文件中添加“域名—IP地址”的有关记录。
  - 注意，这个文件要创建在 /var/named目录中。

```
# vi /var/named/xuchenggang.net.zone
```

# DNS —— 域名服务的配置

```
$TTL 1D
@       IN SOA dns.xuchenggang.net.  root.xuchenggang.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@               IN                      NS                      dns.xuchenggang.net.
dns             IN                      A                       192.168.31.100
ftp             IN                      A                       192.168.31.200
www             IN                      A                       192.168.31.201
mail            IN                      A                       192.168.31.202
web             IN                      CNAME                   www.xuchenggang.net.
@               IN                      MX  10                   mail.xuchenggang.net.
```

# DNS —— 域名服务的配置

- 对区域配置文件的说明：
  - @ 代表相应的域名，例如此处代表 xuchenggang.net，表示一个区域记录定义的开始。
  - IN表示后面的数据使用的是INTERNET标准。
  - SOA 表示授权开始，其后面跟权威DNS服务器的主机名称（FQDN），此处为“dns.xuchenggang.net.”。 **注意，最后面的“.”不能丢，因为此处的“.”表示一个完整主机名称的结束，如果不加点，则系统会默认在原主机名称后再加上“xuchenggang.net”，即变成了“dns.xuchenggang.net.xuchenggang.net”。**

# DNS —— 域名服务的配置

- 对区域配置文件的说明：
  - root.xuchenggang.net.表示管理员邮件地址。注意，这里的邮件地址中用.来代替常见的邮件地址中的@，因为@ 用来表示本区域。
  - serial：定义正向解析区域的序列号。
  - refresh：定义自动刷新间隔时间。
  - retry：定义刷新重试时间。
  - expire：定义数据的有效期限。
  - minimum：定义最小默认的生存时间。

# DNS —— 域名服务的配置

- 对区域配置文件的说明：
  - NS：表示记录类型为NS记录。
  - A：表示记录类型为A记录。
  - MX：表示记录类型为MX记录，后面紧跟的数值为优先级数值。
  - CNAME：表示记录类型为别名记录。
  - www、mail、ftp：表示主机名。

# DNS —— 域名服务的配置

- 区域配置文件xuchenggang.net.zone中的A记录含义：

| 域名 | 对应的IP |
| --- | --- |
| dns.xuchenggang.net | 192.168.31.100 |
| ftp.xuchenggang.net | 192.168.31.200 |
| www.xuchenggang.net | 192.168.31.201 |
| mail.xuchenggang.net | 192.168.31.202 |

# DNS —— 域名服务的配置

## DNS的记录

- 区域配置文件中，定义了各种记录，其含义如下：
- 主机记录（A）
  - 主机记录（A）在DNS区域中通常完成具体域名到IP地址的映射。
- AAAA记录
  - AAAA资源记录类型用来将一个合法域名解析为IPv6地址，与IPv4所用的A资源记录类型相兼容。
- 别名记录（CNAME）
  - 别名记录（CNAME）也被称为规范名称。这种记录允许操作者将多个名称映射到同一台计算机。

# DNS —— 域名服务的配置

- DNS的记录
  - 邮件交换记录（MX）
    - 邮件交换记录（MX）用于电子邮件程序发送邮件时，根据收信人的地址后缀来定位邮件服务器。
  - NS记录
    - NS记录是域名服务器记录，用于标识解析该域或其它域（例如子域）各种主机记录的域名服务器。
  - SOA记录
    - 起始授权机构记录（SOA），是用来识别域名中由哪一个域名服务器负责信息授权。

# DNS —— 域名服务的配置

- DNS的记录
  - PTR记录
    - PTR记录用于IP地址解析到域名，它被视为反向A记录。
  - SRV记录
    - SRV记录是DNS服务器的数据库中支持的一种资源记录的类型，它记录了哪台计算机提供了哪个服务。

# 二、DHCP

## 2.1 DHCP的作用

# DHCP —— DHCP的作用

## 使用DHCP自动配置主机IP地址

- 当网络中只有少数几台计算机时，只需要通过手动的方式为每台计算机配置IP地址。但如果网络中有成百上千台计算机，显然用手工方式为每一台计算机配置IP地址，会有很高的管理成本！
- DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议，使用UDP协议工作。
- 通过DHCP服务，DHCP服务器可以为网络中安装了DHCP客户端程序的计算机自动分配IP地址和其他相关配置（DNS，网关等），而不需要管理员对每个主机进行逐一配置，极大的降低了管理成本。

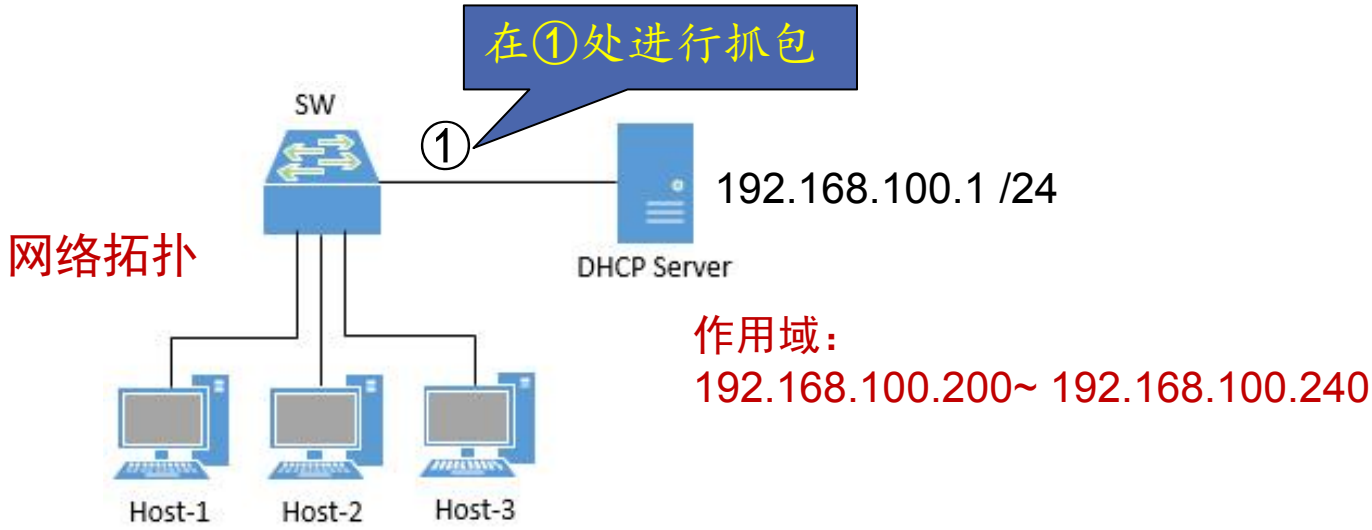
# 二、DHCP

## 2.2 通过DHCP获取IP地址的过程

# DHCP —— 通过DHCP获取IP地址的过程

## 网络环境描述

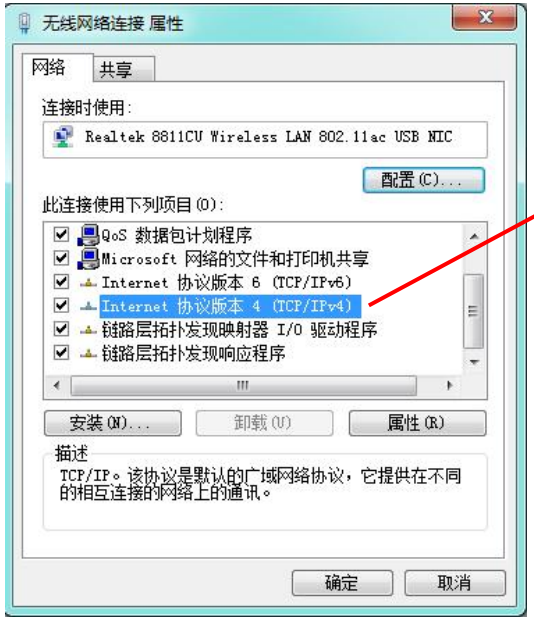
- 局域网中，部署一台DHCP服务器，用户主机若干台。在①处抓包分析。
- DHCP作用域：是DHCP服务器能够进行分配的IP地址段，需要网管员在服务器上事先配置好。例如，若配置作用域为192.168.1.1～192.168.1.254，则DHCP服务器只能把该作用域中的IP地址分配给DHCP客户端。



# DHCP —— 通过DHCP获取IP地址的过程

## 网络中用户主机设置

- 管理员将网络中用户主机的IP地址，设置成“自动获得IP地址”，使之成为DHCP客户端。





用户主机的IP地址配置

# DHCP —— 通过DHCP获取IP地址的过程

## DHCP服务的8种类型报文

- DHCP协议包含8种报文，在进行IP地址配置和管理时，客户端和服务器会通过发送不同的报文实现相互通信，从而完成IP地址等信息的获取。

| | |
|---|---|
| • DHCP Discover | • DHCP NAK |
| • DHCP Offer | • DHCP Release |
| • DHCP Request | • DHCP Decline |
| • DHCP ACK | • DHCP INFORM |

基础报文4个，用于获取IP地址的基本过程

其他报文4个，用于特殊情况（例如获取到的IP地址不可用）时的处理

# DHCP —— 通过DHCP获取IP地址的过程

- 第1步：客户端发出 DHCP Discover报文（发现报文）
  - 客户机发出发现报文：DHCP客户端在启动时会自动发出DHCP Discover报文，该报文是广播报文，用于向DHCP服务器申请IP地址等参数；
  - 局域网中的其他主机（包括DHCP服务器）都会收到DHCP Discover报文，但只有DHCP服务器会进行响应，其他用户主机收到后会丢弃。
  - 运输层的封装：Discover报文在运输层进行封装时，使用UDP协议，使用UDP68端口作为源端口，使用UDP67端口作为目的端口。（注：DHCP客户使用的UDP端口是68，而DHCP服务器使用的UDP端口是67）

# DHCP —— 通过DHCP获取IP地址的过程

- 第1步：客户端发出 DHCP Discover报文（发现报文）
  - 网络层的封装：Discover报文在网络层进行封装时，由于客户机还没有IP地址，它会使用0.0.0.0作为源地址，使用255.255.255.255作为目标IP地址来广播。
  - 数据链路层的封装：发现报文在数据链路层进行封装时，使用DHCP客户机的MAC地址作为源地址，使用ff:ff:ff:ff:ff:ff作为目的MAC地址，进行广播。
  - 在discover报文数据字段中，包含有DHCP客户机的标识信息（即MAC地址），以便DHCP服务器知道这是谁发的DHCP Discover报文
  - DHCP Discover报文的首部地址和报文内容见下页。

# DHCP discover报文 - 首部地址信息


源MAC：客户机MAC地址

目的MAC：广播地址

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 6.895000 | 0.0.0.0 | 255.255.255.255 | DHCP | 410 | DHCP Discover - Transaction |
| 7 | 7.956000 | 192.168.100.1 | 192.168.100.203 | DHCP | 342 | DHCP Offer - Transaction |
| 8 | 8.907000 | 0.0.0.0 | 255.255.255.255 | DHCP | 410 | DHCP Request - Transaction |
| 9 | 8.923000 | 192.168.100.1 | 192.168.100.203 | DHCP | 342 | DHCP ACK - Transaction |

```
Frame 5: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits) on interface 0
Ethernet II, Src: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Discover)
```

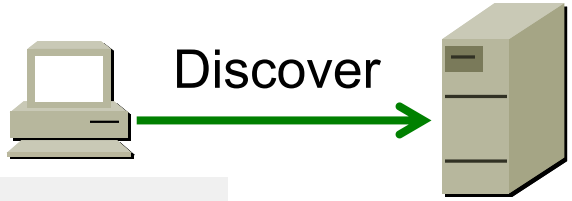
源IP：全0地址

目的IP：全1广播地址

有限广播地址

报文内容见下页

# DHCP discover报文 - 报文内容（1/2）




```
Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0000512a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

此时客户端的IP地址是全0

# DHCP discover报文 - 报文内容（2/2）


```
▷ Option: (53) DHCP Message Type (Discover)
◢ Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95)
◢ Option: (55) Parameter Request List
    Length: 9
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (28) Broadcast Address
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (184) Unassigned
▷ Option: (255) End
  Padding: 000000000000000000000000000000000000000000000000...
```

客户端标识符（即MAC地址），用于向DHCP服务器表明自己的身份

默认向DHCP服务器申请这些参数

# DHCP —— 通过DHCP获取IP地址的过程

- 第2步：服务器发出 DHCP Offer报文（提供报文）
  - 当局域网中的DHCP服务器（可能不止一台）接收到DHCP客户端发来的DHCP Discover报文时，它就在自己的IP地址池（即作用域）中查找是否有合法的IP地址提供给客户机。如果有，DHCP服务器就将此IP地址做上标记，暂时不再分配给其他客户机，然后返回一个DHCP Offer报文，告诉客户端自己可以提供的IP地址等信息内容。
  - Offer报文可以是单播报文，也可以是广播报文，具体要看客户端主机在完成IP地址配置前是否能接收单播报文（具体规则查看RFC2131 ）
  - DHCP Offer报文的首部地址和报文内容见下页。

# DHCP Offer报文 - 首部地址信息


源MAC：服务器MAC

目的MAC：客户端MAC

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 82 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Discover - Transact |
| 83 | 192.168.100.1 | 192.168.100.202 | DHCP | DHCP Offer - Transact |
| 85 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Request - Transact |
| 86 | 192.168.100.1 | 192.168.100.202 | DHCP | DHCP ACK - Transact |

```
> Frame 83: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: 08:00:27:c1:97:81, Dst: 54:89:98:f3:0a:28
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.202
> User Datagram Protocol, Src Port: 67, Dst Port: 68
> Dynamic Host Configuration Protocol (Offer)
```

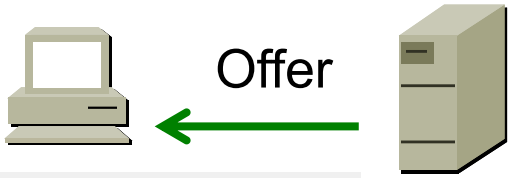
报文内容见下页

源IP：服务器IP

目的IP：准备分配给客户端的IP

源端口：67（服务器端）
目的端口：68（客户端）

# DHCP Offer报文 - 报文内容（1/2）




```
Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x0000503f
  Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.100.202
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: HuaweiTe_f3:0a:28 (54:89:98:f3:0a:28)
  Client hardware address padding: 00000000000000000000
```

准备分配给客户端的IP地址

表明offer报文所响应的客户端的MAC地址

# DHCP Offer报文 - 报文内容（2/2）


```
> Option: (53) DHCP Message Type (Offer)
v Option: (54) DHCP Server Identifier (192.168.100.1)
    Length: 4
    DHCP Server Identifier: 192.168.100.1
v Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (43200s) 12 hours
v Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
v Option: (3) Router
    Length: 4
    Router: 192.168.100.254
^ Option: (6) Domain Name Server
    Length: 4
    Domain Name Server: 8.8.8.8
```

DHCP服务器IP，表明是谁提供的地址

IP租约时间12小时

准备配置给客户端的子网掩码

准备配置给客户端的默认网关地址

准备配置给客户端的域名服务器IP地址

# DHCP —— 通过DHCP获取IP地址的过程

- 第3步：客户端发出 DHCP Request报文（请求报文）
  - DHCP客户端发出Discover报文后，有可能收到多个DHCP服务器回应的DHCP Offer报文，DHCP客户端一般只选择接受第一个收到的Offer报文。
  - DHCP客户端会根据所选中的Offer报文中的服务器地址信息，发出DHCP Request报文。该报文中包含为该客户端提供IP配置的服务器的IP地址，表明客户机选中了哪台服务器。并且，DHCP Request是广播报文（目的IP是255.255.255.255），以便能通知到本网内所有的DHCP服务器。
  - 注意，虽然此时客户机已经收到某个服务器提供的IP地址，但是因为还没有最终确认并配置该IP地址，所以，在DHCP Request报文中仍然使用0.0.0.0作为源IP地址。
  - DHCP Request报文的首部地址和报文内容见下页。

DHCP Request首部地址信息与Discover相同


源MAC：客户机MAC地址

目的MAC：广播地址

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 82 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Discover - Tran |
| 83 | 192.168.100.1 | 192.168.100.202 | DHCP | DHCP Offer - Tran |
| 85 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Request - Tran |
| 86 | 192.168.100.1 | 192.168.100.202 | DHCP | DHCP ACK - Tran |

```
> Frame 85: 410 bytes on wire (3280 bits), 410 bytes captured (3280 b
> Ethernet II, Src: 54:89:98:f3:0a:28, Dst: ff:ff:ff:ff:ff:ff
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
```

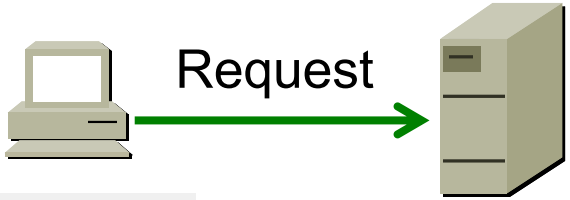
报文内容见下页

源IP：0.0.0.0

源端口：68（客户端）
目的端口：67（服务器端）

目的IP：
255.255.255.255

# DHCP Request报文－报文内容（1/2）




```
Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0000503f
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 54:89:98:f3:0a:28
    Client hardware address padding: 00000000000000000000
    Server host name not given
```

指明是Request报文

此时客户端的IP地址还是全0

# DHCP Request报文－报文内容（2/2）


```
> Option: (53) DHCP Message Type (Request)
v Option: (54) DHCP Server Identifier (192.168.100.1)
    Length: 4
    DHCP Server Identifier: 192.168.100.1
v Option: (50) Requested IP Address (192.168.100.202)
    Length: 4
    Requested IP Address: 192.168.100.202
v Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: 54:89:98:f3:0a:28
v Option: (55) Parameter Request List
    Length: 4
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
> Option: (255) End
```

DHCP服务器的标识(IP地址)，表明客户机请求使用该服务器分配的IP地址

客户机申请的IP地址

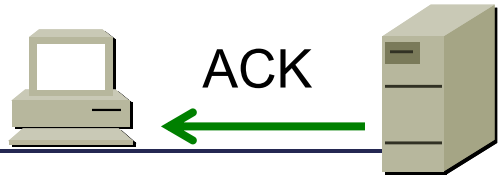
客户端标识（即MAC地址）表明“谁”在提出请求

客户端所申请的网络参数列表，包括子网掩码、默认网关、DNS等信息。

# DHCP —— 通过DHCP获取IP地址的过程

- 第4步：服务器发出 DHCP ACK报文（确认报文）
  - DHCP服务器接收到客户端发来的DHCP Request报文后，会查看报文中的服务器标识（即服务器IP地址）字段，以确定自己是否被选中。
    - 若被选中，会返回DHCP ACK报文，作为最后的确认。若未被选中，则取消前期的IP地址提供。
  - 客户机收到DHCP ACK报文后，是否就可以直接配置自己的IP地址了？
    - DHCP客户端收到DHCP ACK报文后，对所分配的IP地址参数进行最终检测和记录。例如地址复用（冲突）检测，如果所分配的地址已经被网络中其他主机占用，则Client会发送DECLINE报文（告诉服务器该地址不能用），随后在一定时间后重启DHCP交互过程
  - DHCP ACK报文的首部地址和报文内容见下页。

# DHCP ACK报文首部地址信息与Offer报文相同




源MAC：服务器MAC

目的MAC：客户端MAC

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 82 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Discover - Transacti |
| 83 | 192.168.100.1 | 192.168.100.202 | DHCP | DHCP Offer - Transacti |
| 85 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Request - Transacti |
| 86 | 192.168.100.1 | 192.168.100.202 | DHCP | DHCP ACK - Transacti |

```
> Frame 86: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: 08:00:27:c1:97:81, Dst: 54:89:98:f3:0a:28
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.202
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
```

报文内容见下页

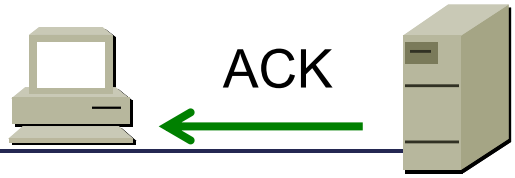
源IP：服务器IP

目的IP：准备分配给客户端的IP

源端口：67（服务器端）

目的端口：68（客户端）

# DHCP ACK报文－报文内容




```
Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0000503f
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.100.202
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 54:89:98:f3:0a:28
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier (192.168.100.1)
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (255) End
```

DHCP消息类型

ACK报文的内容与Offer报文相似

准备分配给客户端的IP地址

表明ACK报文所响应的客户端的MAC地址

DHCP服务器标识

服务器提供给客户端的其他配置信息

# DHCP —— 通过DHCP获取IP地址的过程

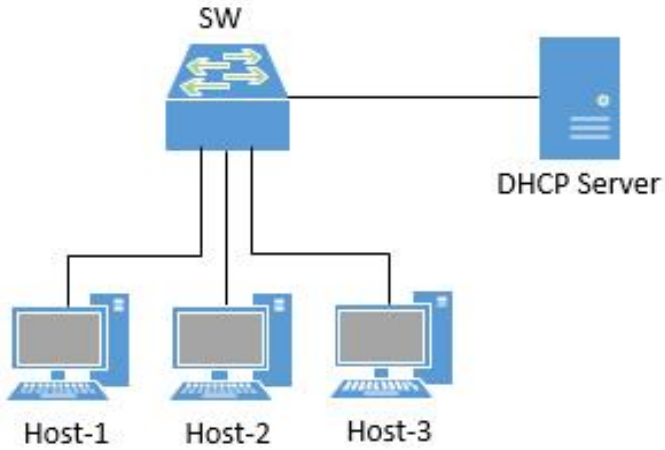
- 其他4种DHCP报文的含义
  - DHCP NAK（应答报文）：通知客户端无法分配合适的IP地址。
  - DHCP Release（请求报文）：请求释放相应的IP地址。
  - DHCP Decline（请求报文）：告知服务器分配的IP地址不可用，希望获取新的IP地址。
  - DHCP INFORM（请求报文）：DHCP客户端需要从DHCP服务器获取更为详细的配置信息时，则向DHCP服务器发送DHCP INFORM请求报文。

# 二、DHCP

## 2.3 DHCP中继的作用

# DHCP- DHCP中继

- 为什么会用到DHCP中继？
  - 由于DHCP客户端在获取IP地址时，是通过广播方式发送报文的，因此DHCP协议是一个局域网（一个广播域）协议。
  - 但是，通常一个园区网内部有多个局域网（即多个广播域），网络管理者并不愿意在每一个网络内都部署一台DHCP服务器，因为这样会使DHCP服务器的数量太多，采用DHCP中继（DHCP Relay）可以解决这一问题。



# DHCP- DHCP中继

➢ IP地址规划：

Host-1: 192.168.0.1~192.168.0.100 /24

Host-2: 192.168.1.1~192.168.1.100 /24

Host-3: 192.168.2.1~192.168.2.100 /24

Host-4: 192.168.3.1~192.168.3.100 /24

Host-5: 192.168.4.1~192.168.4.100 /24

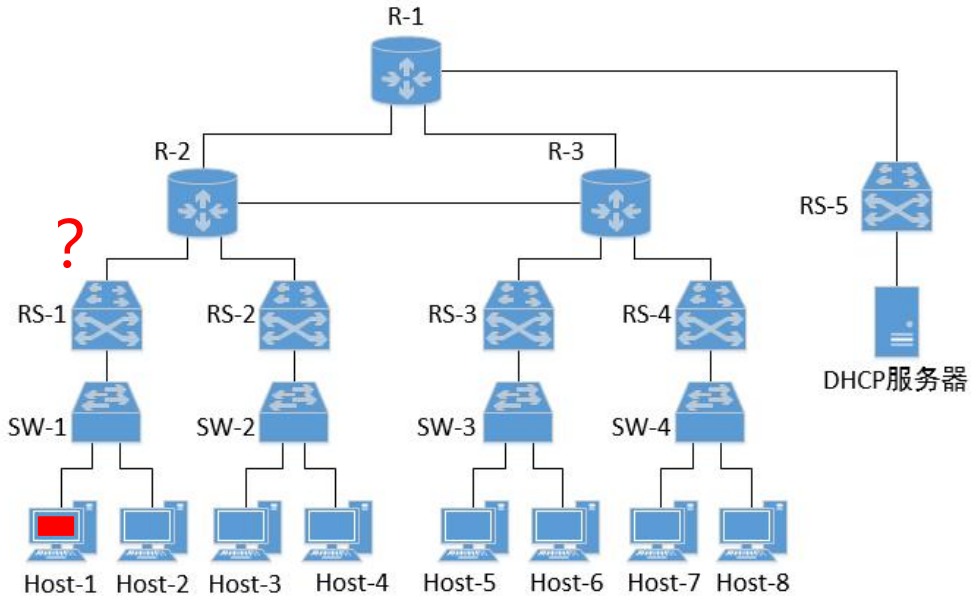
Host-6: 192.168.5.1~192.168.5.100 /24

Host-7: 192.168.6.1~192.168.6.100 /24

Host-8: 192.168.7.1~192.168.7.100 /24

DHCP服务器： 192.168.100.1 /24

注：PC分属于不同的VLAN




问题：Host-1发出的DHCP Discover（发现报文）能被谁收到？

# DHCP- DHCP中继

- 如何应用DHCP中继
  - 为了使全网都能获得同一台DHCP服务器提供的服务，需要在每个子网络的默认网关处（想想为什么？），配置DHCP中继。
  - 某个子网（或VLAN）中的主机通过DHCP中继获取IP地址的过程如下：
    1. DHCP客户机发出的DHCP报文（例如Discover）会首先到达本网络中的DHCP中继；
    2. DHCP中继上配置有DHCP服务器的IP地址信息，因此，DHCP中继会将收到的DHCP客户机发来的DHCP报文，转发给DHCP服务器,且以单播方式转发DHCP报文；
    3. DHCP服务器返回的报文，会先以单播方式发到DHCP中继（因为DHCP中继自身有IP地址），然后再由DHCP中继转发给DHCP客户机。
    4. 最终，DHCP客户机获取到IP地址。

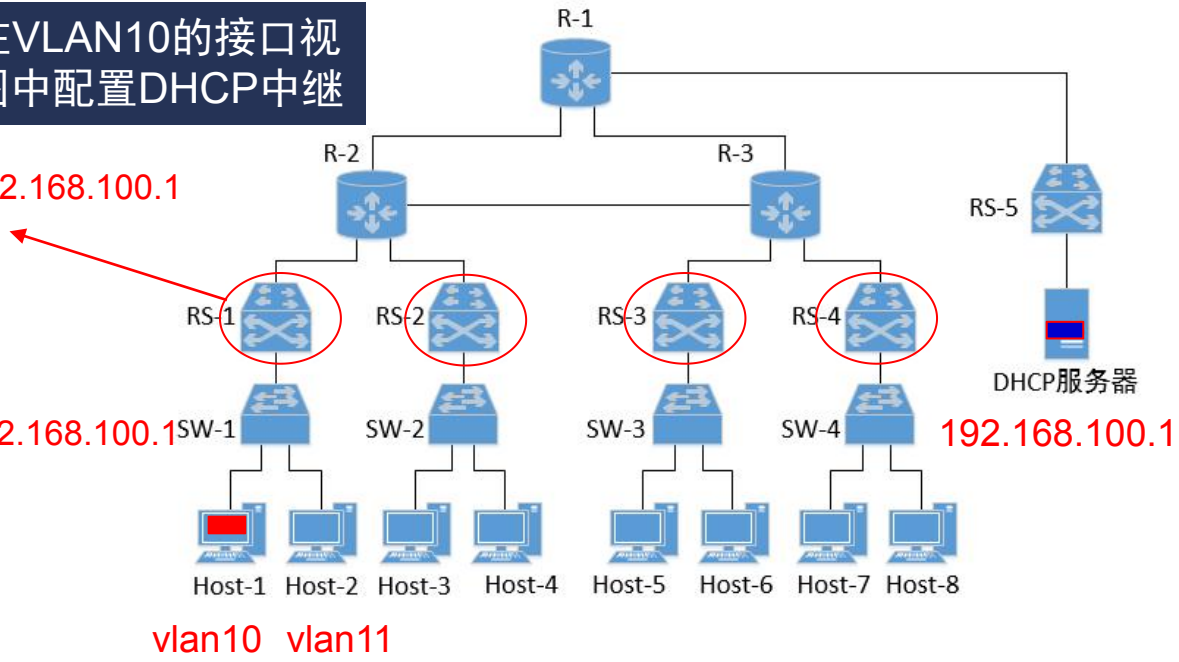
# ➢ DHCP 中继配置举例（华为s5700）

➢ 分别给VLAN10、VLAN11的子网络配置DHCP中继：

[RS-1] dhcp enable
[RS-1] interface vlanif 10
[RS-1-Vlanif10] dhcp select relay
[RS-1-Vlanif10] dhcp relay server-ip 192.168.100.1
[RS-1-Vlanif10] quit

[RS-1] interface vlanif 11
[RS-1-Vlanif11] dhcp select relay
[RS-1-Vlanif11] dhcp relay server-ip 192.168.100.1
[RS-1-Vlanif11] quit

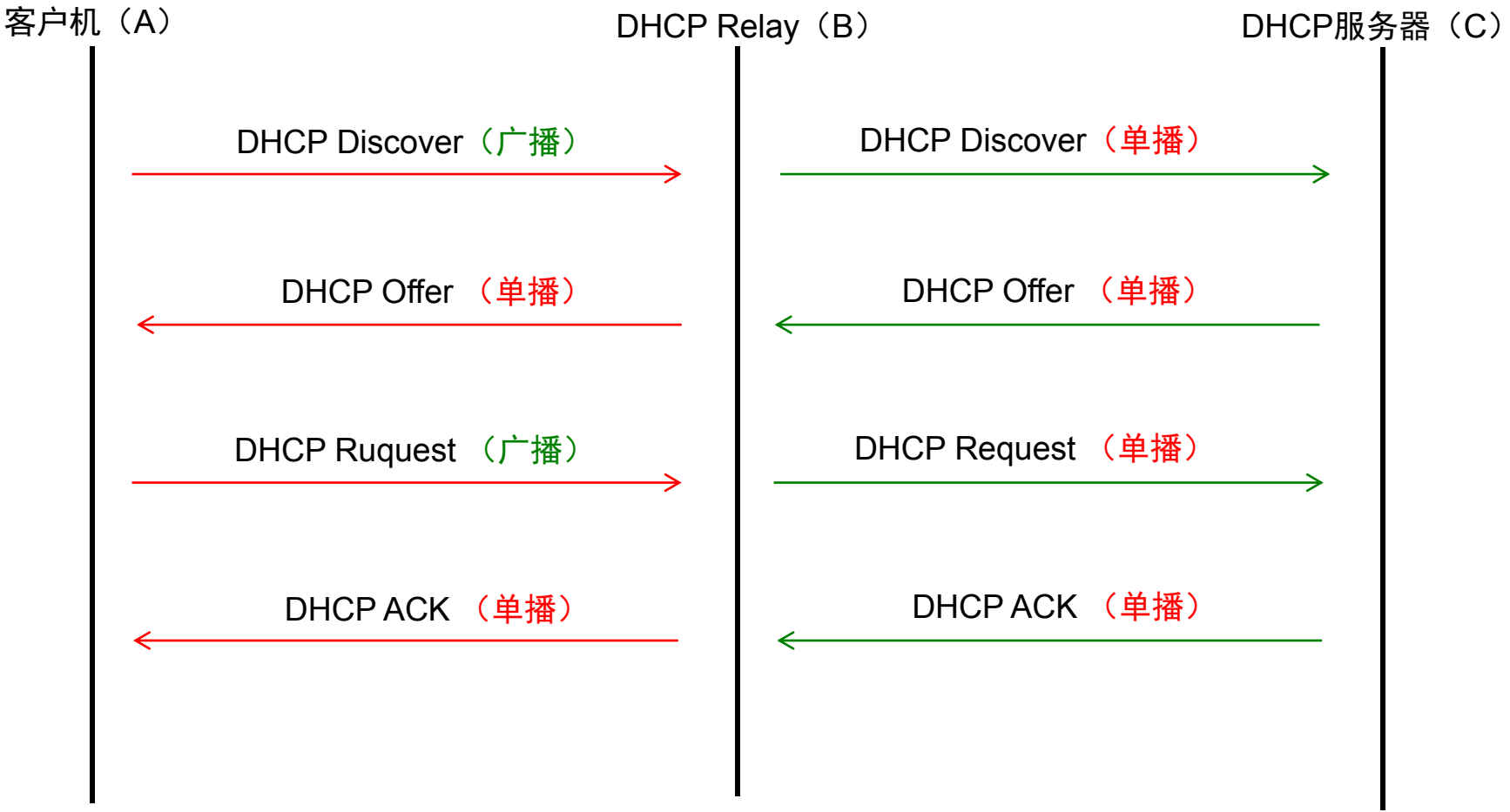
在VLAN10的接口视图中配置DHCP中继




针对每个用户VLAN，在网关处配置DHCP中继。

在RS-1~RS-4上配置DHCP中继

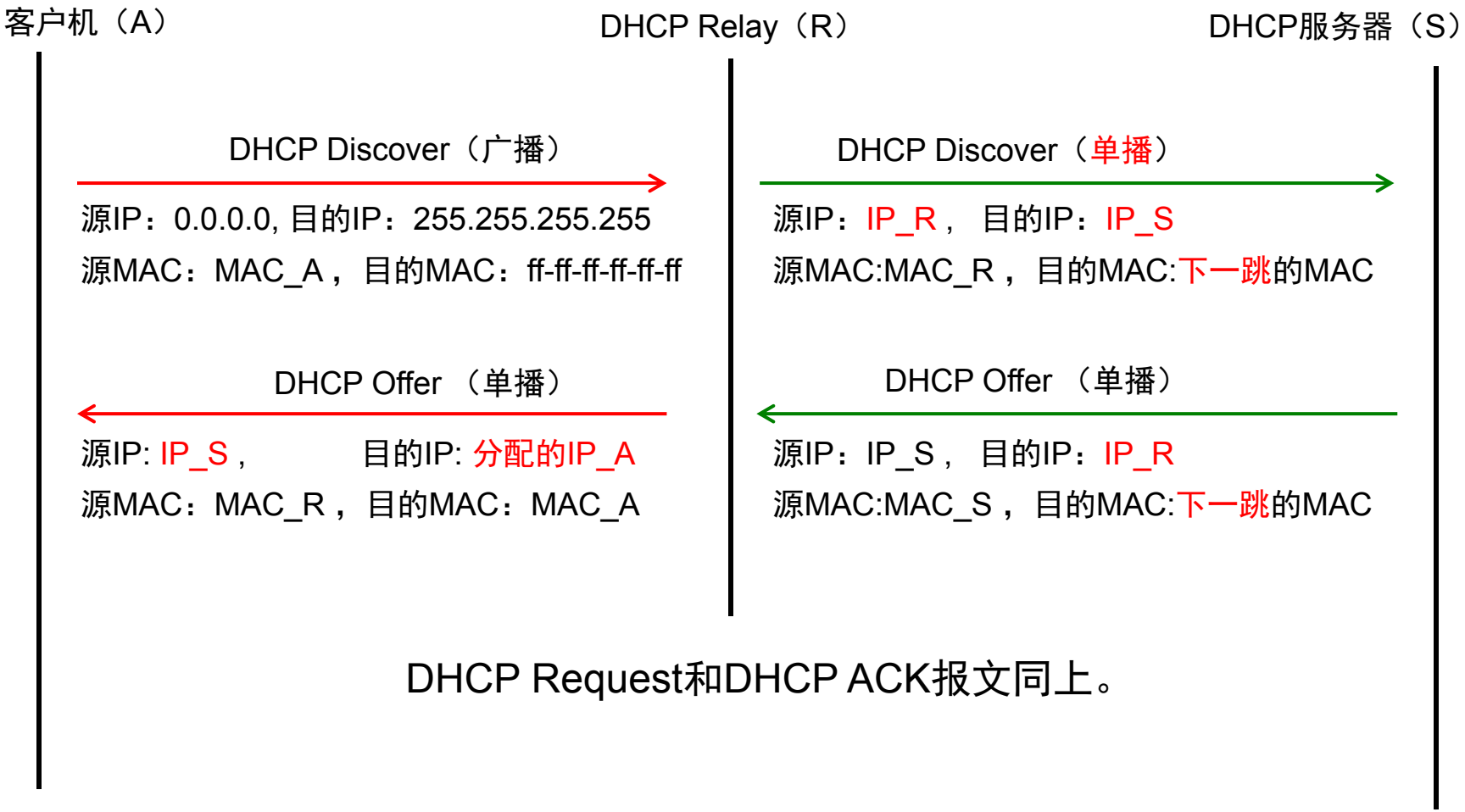
# DHCP Relay的工作过程（假设DHCP客户端能接收单播报文）



# DHCP- DHCP中继

- DHCP中继的工作特点
  - DHCP客户端通过DHCP中继代理从DHCP服务器获取IP地址的过程与直接从DHCP服务器获取IP地址的过程相类似，都需要经历发现、提供、选择和确认四个阶段。
  - 中继代理只是充当一个中介代理角色，负责转发DHCP客户端与DHCP服务器之间交互的请求和应答报文。
  - 但是，DHCP中继在转发DHCP报文时，需要重新封装报文，因此报文首部的地址会发生变化。总结如下页

# ➢ DHCP Relay工作过程中报文首部地址变化（假设客户端能接收单播报文）




DHCP Request和DHCP ACK报文同上。

【结合实验自主学习】

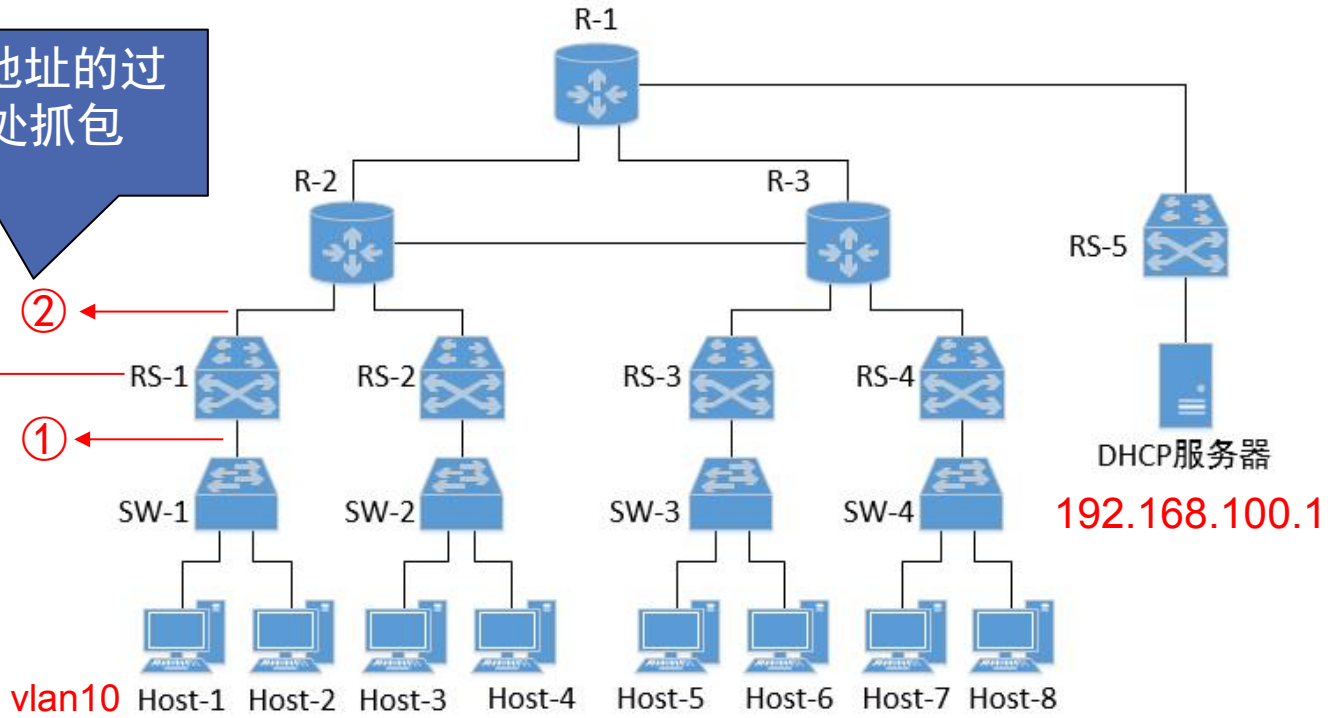
# 二、DHCP

## 2.4 抓包分析DHCP Relay的工作过程

# ■ 抓包分析DHCP Relay的工作过程

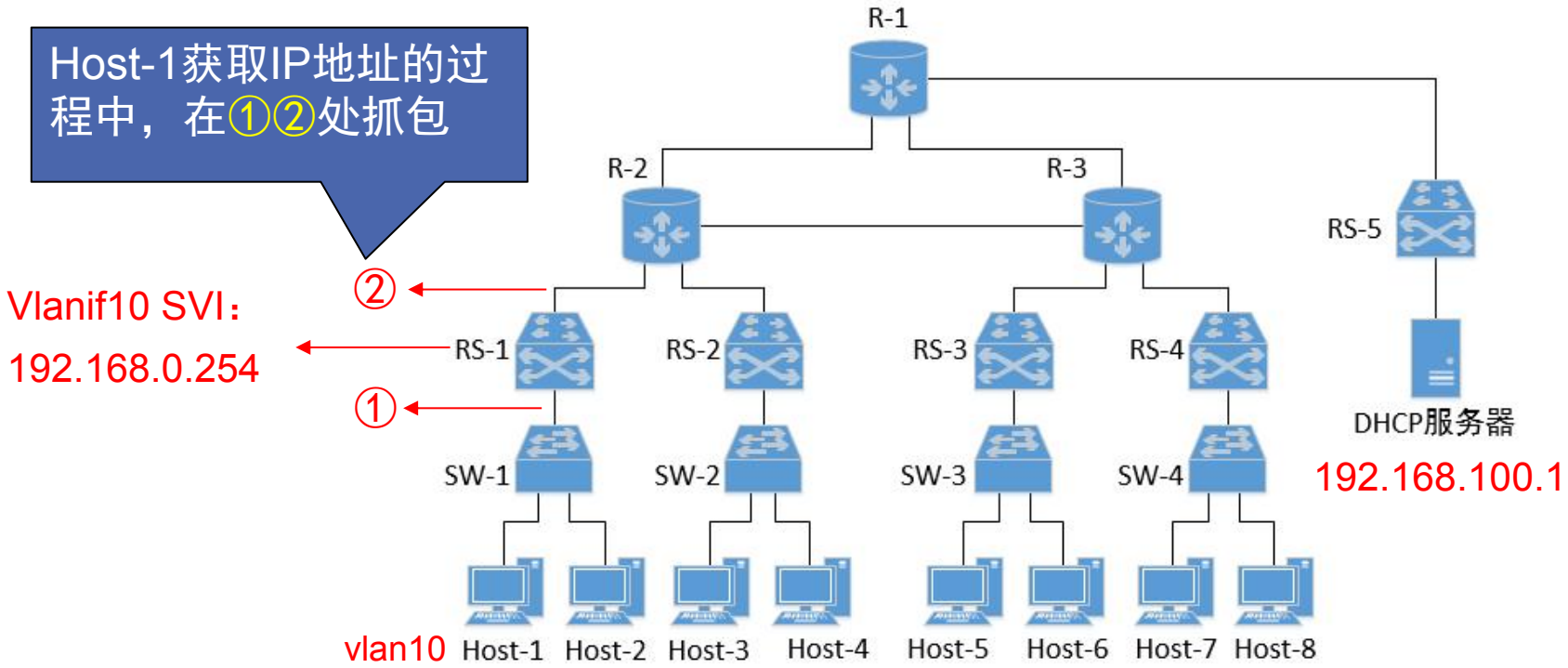
Host-1获取IP地址的过程中，在①②处抓包

Vlanif10 SVI：
192.168.0.254




Host-1获取192.168.0.1~192.168.0.100中的IP地址

# ■ 抓包分析DHCP Relay的工作过程




Host-1获取192.168.0.1~192.168.0.100中的IP地址

# ■ 抓包分析DHCP Relay的工作过程

1. Host-1发出DHCPDISCOVER广播报文，该报文可到达位于三层交换机RS-1的DHCP中继（即vlanif10）。

Host-1 ←→ DHCP 中继（RS-1）

①

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 3.525000 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Discover - |
| 4 | 3.619000 | 192.168.100.1 | 192.168.0.1 | DHCP | 346 | DHCP Offer - |
| 7 | 5.522000 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Request - |
| 8 | 5.584000 | 192.168.100.1 | 192.168.0.1 | DHCP | 346 | DHCP ACK - |

2. Vlanif10发现这是一个DISCOVER报文，根据管理员配置的DHCP服务器地址，将该报文重新封装后发给DHCP服务器（单播报文），首部地址如图所示。报文中包含客户端MAC和中继的IP

DHCP 中继（RS-1）←→ DHCP服务器

②

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 6.489000 | 192.168.0.254 | 192.168.100.1 | DHCP | 410 | DHCP Discover - |
| 6 | 6.552000 | 192.168.100.1 | 192.168.0.254 | DHCP | 342 | DHCP Offer - |
| 9 | 8.455000 | 192.168.0.254 | 192.168.100.1 | DHCP | 410 | DHCP Request - |
| 10 | 8.502000 | 192.168.100.1 | 192.168.0.254 | DHCP | 342 | DHCP ACK - |

Vlanif10： 192.168.0.254　　DHCP服务器：192.168.100.1　　Host-1获取IP：192.168.0.1

# ■ 抓包分析DHCP Relay的工作过程

4. DHCP中继收到服务器发回的offer报文后，根据报文中的客户端MAC和所分配的IP地址，对offer报文重新封装后，发给客户端（单播）

Host-1 ←→ DHCP 中继（RS-1）

①

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 3.525000 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Discover - |
| 4 | 3.619000 | 192.168.100.1 | 192.168.0.1 | DHCP | 346 | DHCP Offer - |
| 7 | 5.522000 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Request - |
| 8 | 5.584000 | 192.168.100.1 | 192.168.0.1 | DHCP | 346 | DHCP ACK - |

3. DHCP服务器从收到的discover报文中获取了DHCP中继的IP地址和客户端的MAC地址，然后向DHCP中继发回offer报文（单播报文），报文首部的IP地址如图所示。

DHCP 中继（RS-1）←→ DHCP服务器

②

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 6.489000 | 192.168.0.254 | 192.168.100.1 | DHCP | 410 | DHCP Discover - |
| 6 | 6.552000 | 192.168.100.1 | 192.168.0.254 | DHCP | 342 | DHCP Offer - |
| 9 | 8.455000 | 192.168.0.254 | 192.168.100.1 | DHCP | 410 | DHCP Request - |
| 10 | 8.502000 | 192.168.100.1 | 192.168.0.254 | DHCP | 342 | DHCP ACK - |

Vlanif10： 192.168.0.254　　DHCP服务器：192.168.100.1　　Host-1获取IP：192.168.0.1

# ■ 抓包分析DHCP Relay的工作过程

5. Host-1发出request报文（包含所申请的地址信息等），广播报文，该报文可到达位于三层交换机RS-1的DHCP中继（即vlanif10）。

Host-1 ←→ DHCP 中继（RS-1）

①

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 3.525000 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Discover - |
| 4 | 3.619000 | 192.168.100.1 | 192.168.0.1 | DHCP | 346 | DHCP Offer - |
| 7 | 5.522000 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Request - |
| 8 | 5.584000 | 192.168.100.1 | 192.168.0.1 | DHCP | 346 | DHCP ACK - |

6. Vlanif10发现这是一个request报文，根据管理员配置的DHCP服务器地址，将该报文重新封装后发给DHCP服务器（单播报文），首部地址如图所示。报文中包含客户端MAC和中继的IP

DHCP 中继（RS-1）←→ DHCP服务器

②

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 6.489000 | 192.168.0.254 | 192.168.100.1 | DHCP | 410 | DHCP Discover - |
| 6 | 6.552000 | 192.168.100.1 | 192.168.0.254 | DHCP | 342 | DHCP Offer - |
| 9 | 8.455000 | 192.168.0.254 | 192.168.100.1 | DHCP | 410 | DHCP Request - |
| 10 | 8.502000 | 192.168.100.1 | 192.168.0.254 | DHCP | 342 | DHCP ACK - |

Vlanif10： 192.168.0.254　　DHCP服务器：192.168.100.1　　Host-1获取IP：192.168.0.1

# ■ 抓包分析DHCP Relay的工作过程

8. DHCP中继收到服务器发回的ACK报文后，根据报文中的客户端MAC和所分配的IP地址，对ACK报文重新封装后，发给客户端（单播）

Host-1 ←→ DHCP 中继（RS-1）

①

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 3.525000 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Discover - |
| 4 | 3.619000 | 192.168.100.1 | 192.168.0.1 | DHCP | 346 | DHCP Offer - |
| 7 | 5.522000 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Request - |
| 8 | 5.584000 | 192.168.100.1 | 192.168.0.1 | DHCP | 346 | DHCP ACK - |

7. DHCP服务器从收到的request报文中获取了DHCP中继的IP地址和客户端的MAC地址，然后向DHCP中继发回ACK报文（单播报文），报文首部的IP地址如图所示。

DHCP 中继（RS-1）←→ DHCP服务器

②

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 6.489000 | 192.168.0.254 | 192.168.100.1 | DHCP | 410 | DHCP Discover - |
| 6 | 6.552000 | 192.168.100.1 | 192.168.0.254 | DHCP | 342 | DHCP Offer - |
| 9 | 8.455000 | 192.168.0.254 | 192.168.100.1 | DHCP | 410 | DHCP Request - |
| 10 | 8.502000 | 192.168.100.1 | 192.168.0.254 | DHCP | 342 | DHCP ACK - |

Vlanif10： 192.168.0.254　　DHCP服务器：192.168.100.1　　Host-1获取IP：192.168.0.1

# 三、NTP

## 3.1 时间同步的重要性

# NTP - 谈谈时间同步的重要性

## 计算机中的时间

计算机时间包括硬件时间和系统时间。

- 硬件时间
  - 计算机主板上的RTC（实时时钟）以振荡器为时钟源，通过振荡器产生脉冲信号的振荡频率计时。由CMOS电池为RTC和CMOS供电，RTC计时并将时间存储到CMOS。
- 系统时间
  - 计算机运行时CPU内核振荡器产生高频脉冲信号，为系统时钟提供了一个精确的脉冲信号周期时间（如：时钟频率为1GHz，周期为1ns）。系统时钟也基于对CPU的振荡器产生脉冲信号的频率进行系统计时。
  - 计算机启动时通过BIOS程序从CMOS读取硬件时间，根据系统时区确定系统时间。

# NTP - 谈谈时间同步的重要性

## 为什么会出现不同步？

- 随着计算机网络的迅猛发展，网络中的设备种类和业务类型越来越多，服务器的数量也与日俱增。传统上，各种服务器、网络设备使用的时间都是由设备内部时钟来提供的。
- 在网络中，由于不同设备本地时钟频率、运行环境的不同，进行过时钟校准的设备运行一段时间后会出现时间不一致。
- 由于服务器、网络设备本身的时钟误差是不可避免的，尽管这种误差每天不大，但经过一段时间的累积就会出现大的时间差，从而导致网络中各服务器、网络设备的时间不一致。而这种不一致，将会对网络服务产生较大影响。

# NTP - 谈谈时间同步的重要性

- “不同步”带来的问题
  - 案例1：医院的医生工作站开具处方，并保存在服务器中。若服务器时间不正确，则无法进行正常的处方回溯；
  - 案例2：安全设备的时间策略，例如防火墙。因为时间的不一致，无法正常实现安全策略。
  - 案例3：服务器系统监控，因为时间的不统一，就无法判定出业务（或故障）具体发生时间。
  - 案例4：研究生考试，不同考场的时间若不同步，影响考试的公平性。

# NTP - 谈谈时间同步的重要性

- 随着网络拓扑的日益复杂，整个网络内设备的时钟同步将变得十分重要。如果依靠管理员手工修改系统时钟，不仅工作量巨大，而且时钟的准确性也无法得到保证。
  - 需要解决两个问题
    - 标准的时间源
    - 网络内的时间同步方式

# 三、NTP

## 3.2 谈谈标准的时间源

# NTP-谈谈标准的时间源

- 时间如何确定？
  - “天”是怎么来的？
    - 观察太阳。由于地球的自转，人们可以看到日出日落，所以就把这一周期现象定义为“天”。进而有了时、分、秒
  - 世界时
    - 确定了天文规律，人们开始制造钟表，把时间表示出来。所以，在1927年，人们以基于天文现象和钟表计时，确立了第一套时间标准，也就是世界时（Universal Time，简称 UT），并被广泛用于全球标准时间。

# NTP-谈谈标准的时间源

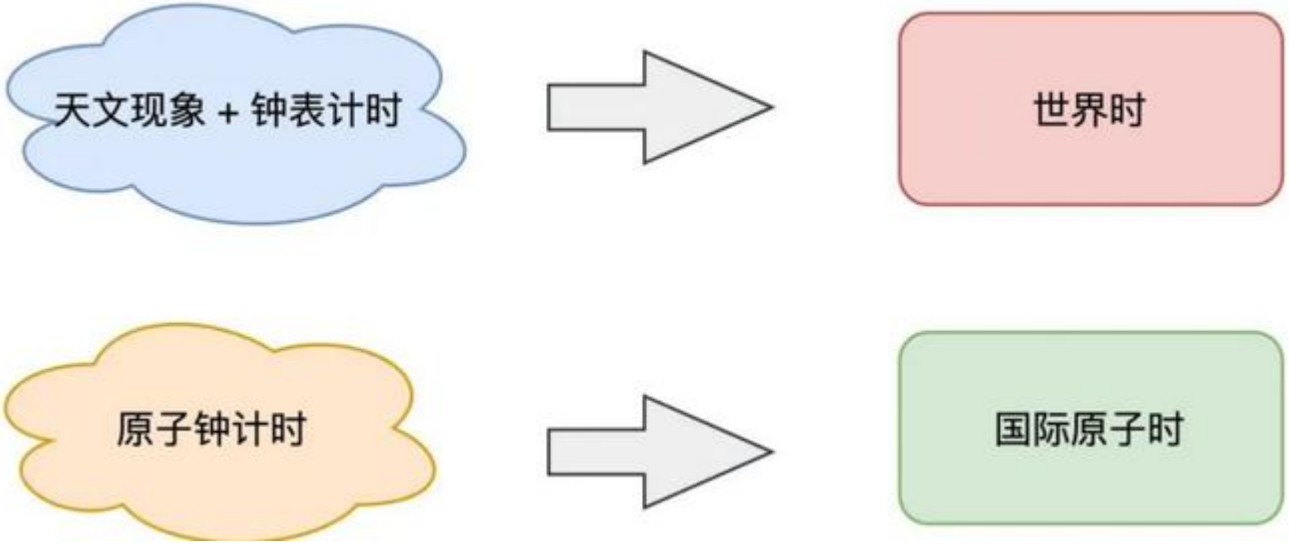
- 时间如何确定？
  - 国际原子时
    - 通过天文观测的世界时的不精准性，地球自转在减慢；
    - 从微观层面探索“秒”的定义！希望每一秒是固定的！
    - 人们发现，原子内的电子发生跃迁时，原子会吸收或放出一定能量的电磁波，这类电磁波就是一种周期运动，我们也可以把它看成原子内部的振荡。基于这个原理，科学家们开始不断地试验、研究，终于发现铯原子内部的振荡周期比其它原子都要更短、更稳定，而且，这个过程基本不受环境因素的干扰。

# NTP-谈谈标准的时间源

- 时间如何确定？
  - 国际原子时
    - 科学家们就以之前定义的"秒"为基础，去测量一秒内这个铯原子内部电子周期运动的次数，测量出来的结果为9192631770 次。
    - 基于此，科学家们决定抛弃原来基于天文测量的秒，重新定义"秒"的时长，就是这个高度稳定的运动周期。
    - 因此，在1967年国际度量衡大会决定采用，以铯原子跃迁 9192631770 个周期所持续的时间长度定义为1秒，而基于这个铯原子振荡制造出来的时钟，被称为原子钟。
    - 有了原子钟，人们基于原子钟又确立了一套新的时间标准，叫做国际原子时（International Atomic Time，简称 TAI）。

# NTP-谈谈标准的时间源

- 两套时间标准存在的问题
  - 这就出现两套时间标准



# NTP-谈谈标准的时间源

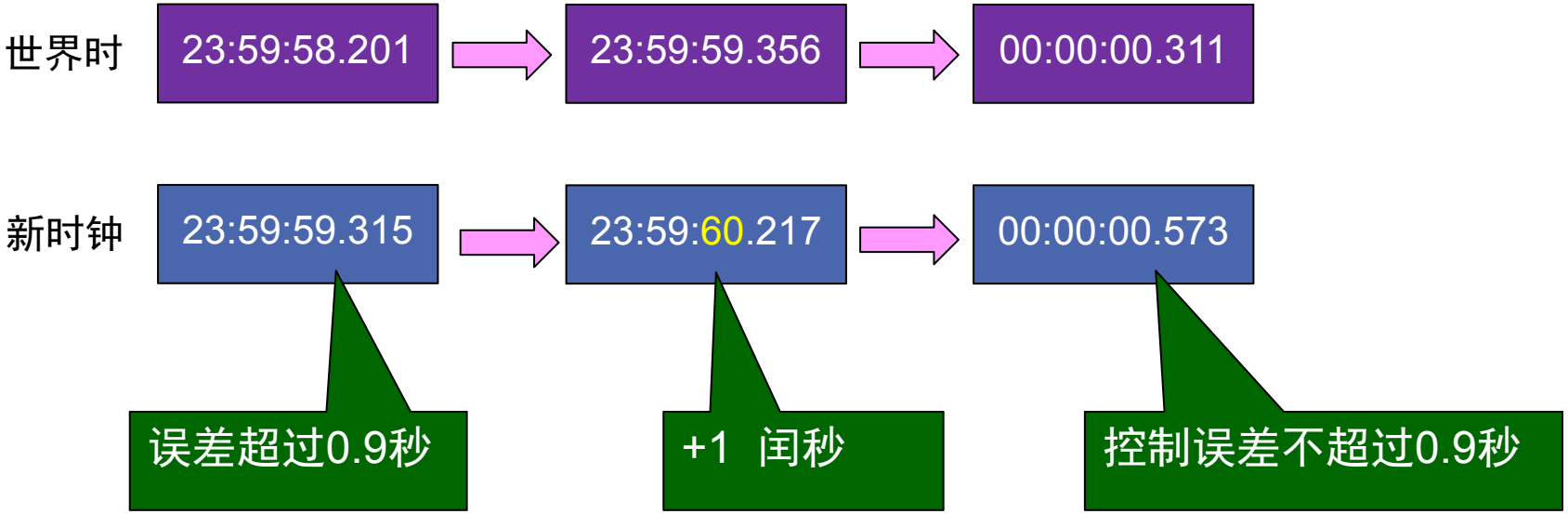
- 两套时间标准存在的问题
  - 假设我们以国际原子时为时间标准，那会发生什么现象呢？因为原子时非常稳定，但世界时随着地球自转变慢，会越来越慢，就会发生这种现象，原子时走得快，世界时走得慢，时间越久，两者差距越来越大，一般来说一至二年会差大约1秒时间。
  - 基于天文测算的世界时，已经指导我们人类生活了上千年，人类早已习惯了这种时间标准，直接被原子时取代，肯定是不能接受的。但我们又需要原子时这种高度稳定的计时标准，来发展科学研究，两者发生矛盾，这怎么办？

# NTP-谈谈标准的时间源

- 一个互相兼容的解决方案！
  - 我们可以再建立一套新的时间标准，这套时间以原子时为基准，开始计时，走的每一秒都是稳定、精确的。同时，为了兼顾基于天文测量的世界时，人类会持续观测这个新时钟与世界时的差距。如果发现两者相差过大时，我们就人为地调整一下这个时钟（加一秒或减一秒），让两者相差不超过 0.9 秒，而加的这一秒，科学家把它定义为闰秒。
  - 例如：若地球自转变慢，原子时误差将超过+0.9秒时，便人为地加进1秒，反之则要扣去1秒钟。
  - 国际上规定，这种闰秒由国际时间局根据实际情况来随时处理，但加减必须在特定的时刻进行:12月31日或6月30日最后一分钟的最后一秒之后。

# NTP-谈谈标准的时间源

- 一个互相兼容的解决方案！
  - 举例：闰秒的应用



# NTP-谈谈标准的时间源

- UTC (Universal Time Coordinated) 协调世界时
  - 这个兼容性方案的好处在于，新时钟的每一秒的计时依旧是精确的，而且还兼顾了日常生活使用的世界时，一举两得。由于这个时钟是基于原子时 + 世界时协调得出的，所以科学家们把它定义为协调世界时（Coordinated Universal Time，简称 UTC）。
  - 有了这个研究成果，有技术能力的国家都纷纷制造自己的原子钟，然后计算协调世界时。中国会在自己算出的世界协调时的基础上，再加8个小时（中国在东八区），最终得出来的时间，就是北京时间。至此，全新的世界标准时间确立了，这套时间标准于1972年正式确定，一致沿用至今。

# NTP-谈谈标准的时间源

## 协调世界时——闰秒

- 2015年，全球进行闰秒调整。当时，国际标准时UTC在闰秒调整前后的时间标记为：2015年06月30日的23时59分59秒、2015年06月30日23时59分60秒、2015年07月01日00时00分00秒。
- 由于我国位于东八区（UTC+8），闰秒调整出现在北京时间2015年07月01日上午，当时北京时间的闰秒调整顺序为：2015年07月01日07时59分59秒、2015年07月01日07时59分60秒、2015年07月01日08时00分00秒。


2015年1月，中科院国家授时中心宣布，我国将在北京时间2015年7月1日的7时59分59秒和全球同步进行闰秒调整，届时会出现07:59:60的特殊现象

# 三、NTP

## 3.3 网络内的时间同步方式

# NTP - 网络内的时间同步方式

- 有了标准时间，如何进行同步？
  - 通常，国家授时中心产生时间后会通过一系列方式，例如无线电波、网络、电话等，把这个时间广播出去，这个过程，就叫做授时。
  - 一般无线电波的传播速度更快、传播误差小，所以授时中心会通过这种方式，把时间发送给全国各地的时间服务器。
  - 时间服务器有了准确的时间后，再通过其它方式（例如网络）广播到下一层的终端用户使用。

# NTP - 网络内的时间同步方式

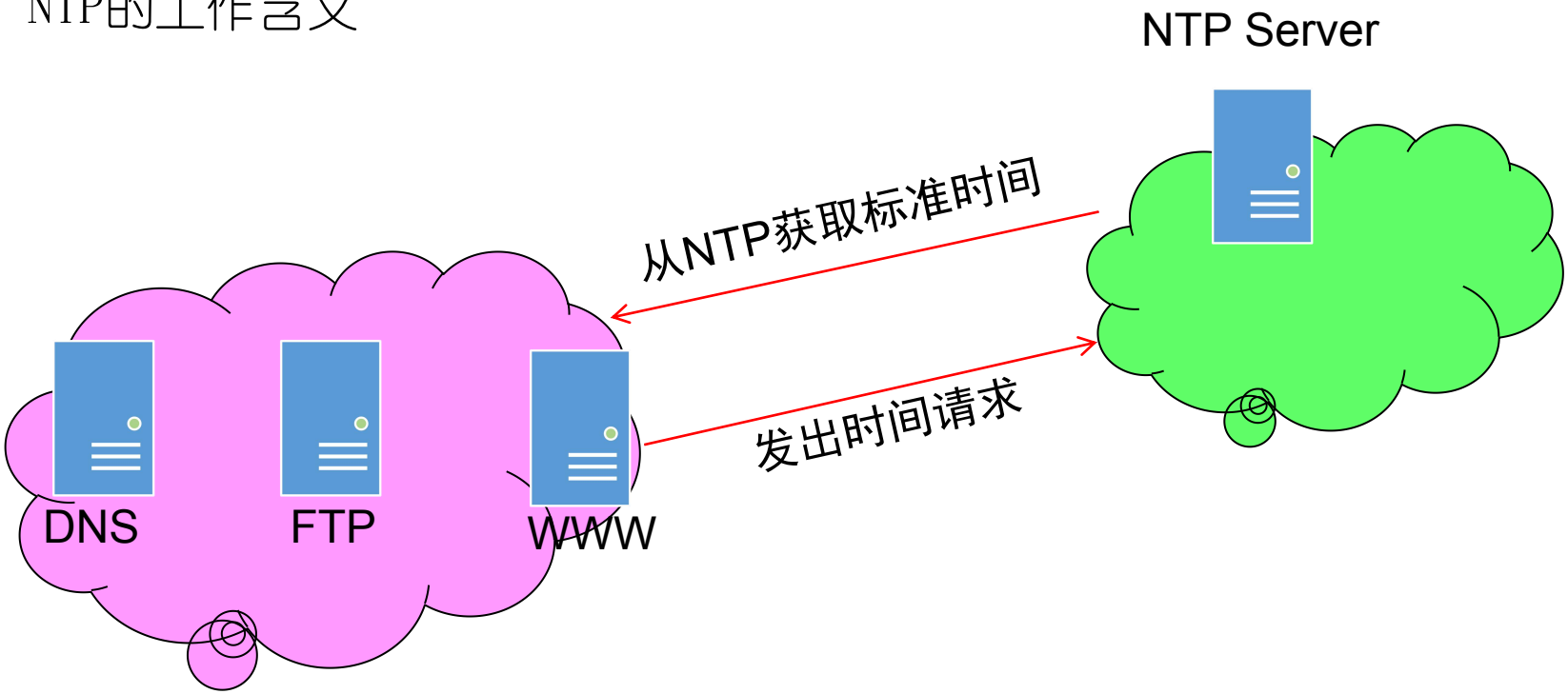
- 计算机网络内如何同步这个标准时间？
  - 最简单的方式就是：客户端向时间服务器端请求获取标准时间，服务端响应时间数据，客户端修改本机时间即可。
  - 问题：但事情没这么简单，因为数据在网络传输过程中，也是需要时间的，这个时间也会影响到时间的准确性。这怎么办呢？。
  - 使用NTP！
    - 当计算机在做时间校准时，也需要把网络延迟计算进去，最后修正这个同步过来的时间，降低误差。这个服务就是 NTP（Network Time Protocol），它可以保证每台机器的时间与时间服务器保持同步。

# NTP - 网络内的时间同步方式

- 网络时间协议NTP (Network Time Protocol)
  - 是TCP/IP协议族里面的一个应用层协议。
  - NTP用于在一系列分布式时间服务器与客户端之间同步时钟。NTP的实现基于IP和UDP。
  - NTP报文通过UDP传输，端口号是123。

# NTP - 网络内的时间同步方式

- NTP的工作含义



# NTP - 网络内的时间同步方式

- NTP的主要应用场景
  - 网络管理：对从不同路由器采集来的日志信息、调试信息进行分析时，需要以时间作为参照依据。
  - 计费系统：要求所有设备的时钟保持一致。
  - 多个系统协同处理同一个复杂事件：为保证正确的执行顺序，多个系统必须参考同一时钟。
  - 备份服务器和客户机之间进行增量备份：要求备份服务器和所有客户机之间的时钟同步。
  - 系统时间：某些应用程序需要知道用户登录系统的时间以及文件修改的时间。

# NTP - 网络内的时间同步方式

| 版本 | 时间 | 协议号 | 描述 |
| --- | --- | --- | --- |
| NTPv1 | 1988年6月 | RFC 1059 | NTPv1首次提出了完整的NTP规则以及算法，但是NTPv1不支持认证和控制消息。 |
| NTPv2 | 1989年9月 | RFC 1119 | NTPv2在NTPv1的基础上支持认证和控制消息。 |
| NTPv3 | 1992年3月 | RFC 1305 | NTPv3正式引入了校正原则，并改进了时钟选择和时钟过滤算法。NTPv3目前应用较为广泛。 |
| NTPv4 | 2010年6月 | RFC 5905 | •NTPv3仅支持IPv4网络，但是随着IPv6的发展和对网络安全性的要求不断提高，NTPv4产生。NTPv4是对NTPv3的扩展，并兼容NTPv3。 NTPv4同时支持IPv4和IPv6网络。<br>•NTPv4提供了一套完整的加密认证体系，安全性上相对NTPv3有了很大的提高。 |

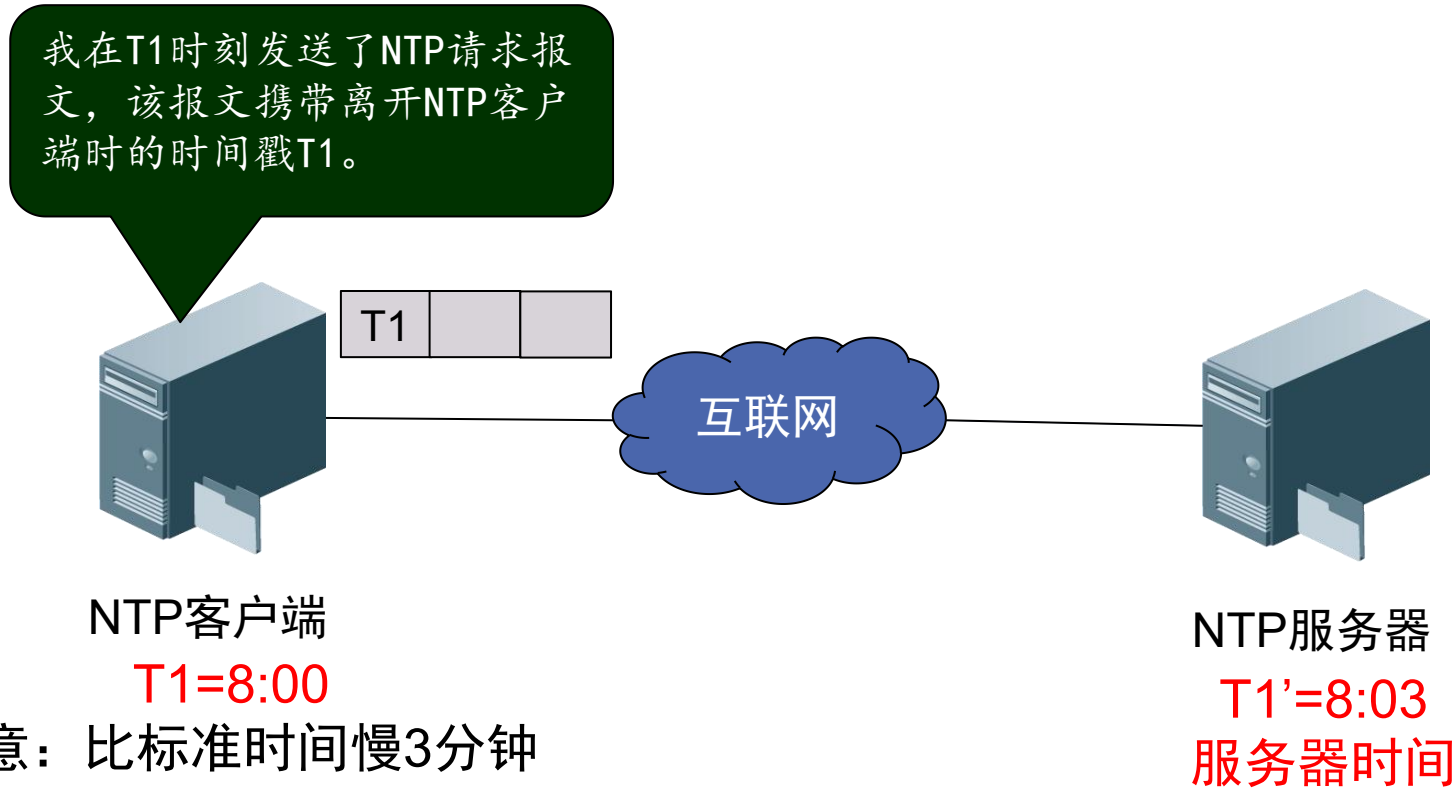
# 三、NTP

## 3.4 NTP的工作原理

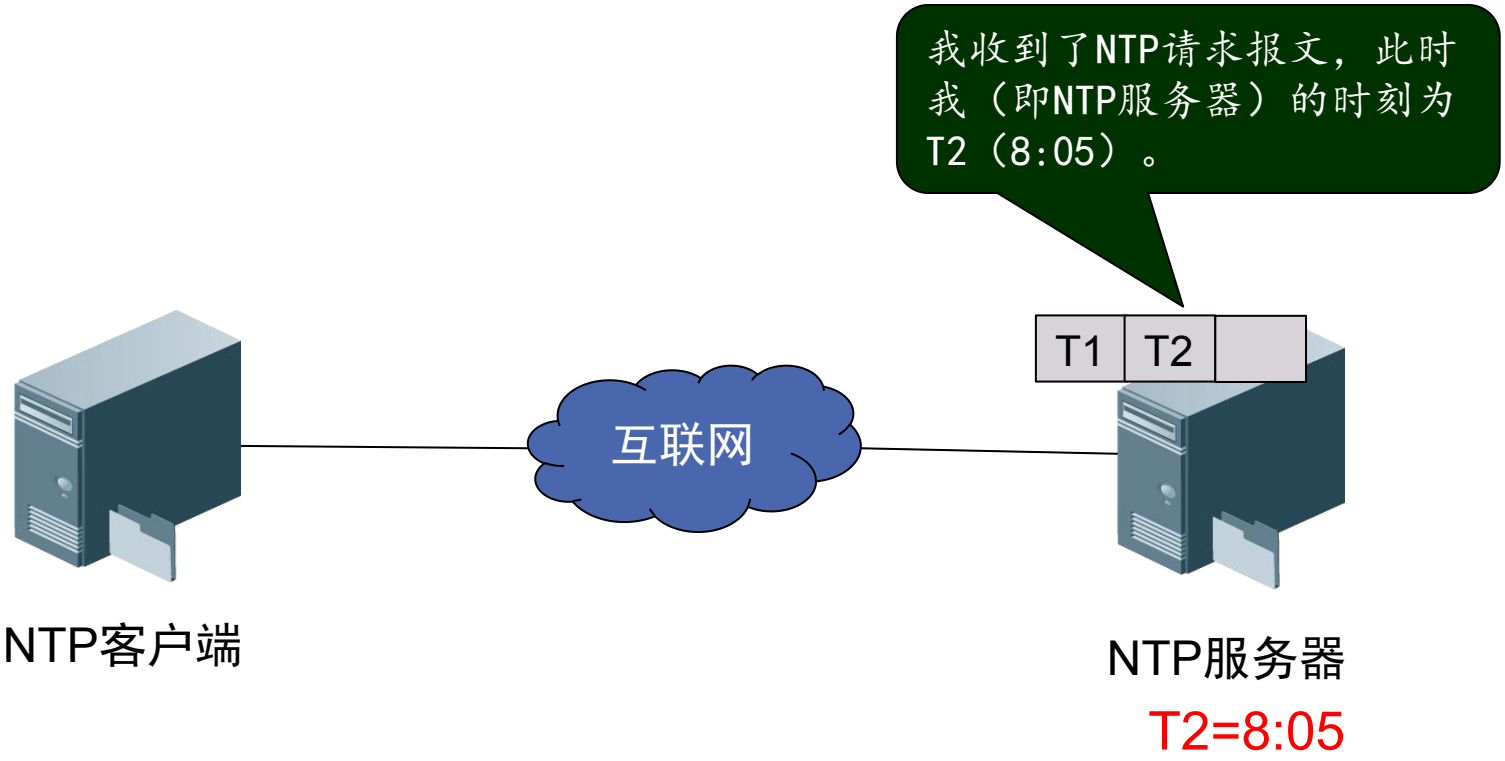
# NTP - NTP工作原理

- NTP客户端和NTP服务器相连，它们都有自己独立的系统时钟，现在通过NTP实现系统时钟自动同步
- NTP客户端的时钟设定为Ta，NTP服务器的时钟设定为Tb。假设Ta比Tb慢3分钟

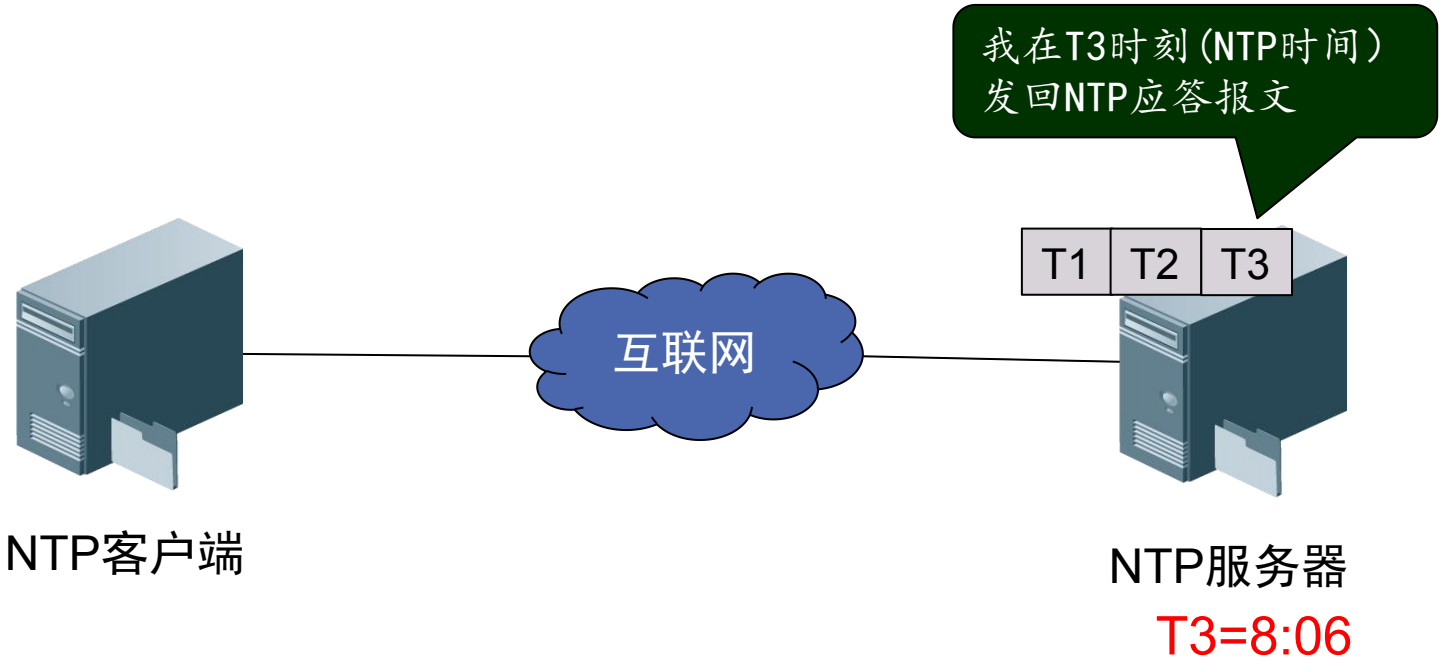
① NTP客户端在T1时刻（客户端的时间，假设8:00）发送一个NTP请求报文给NTP服务器，该请求报文携带离开NTP客户端时的时间戳T1。



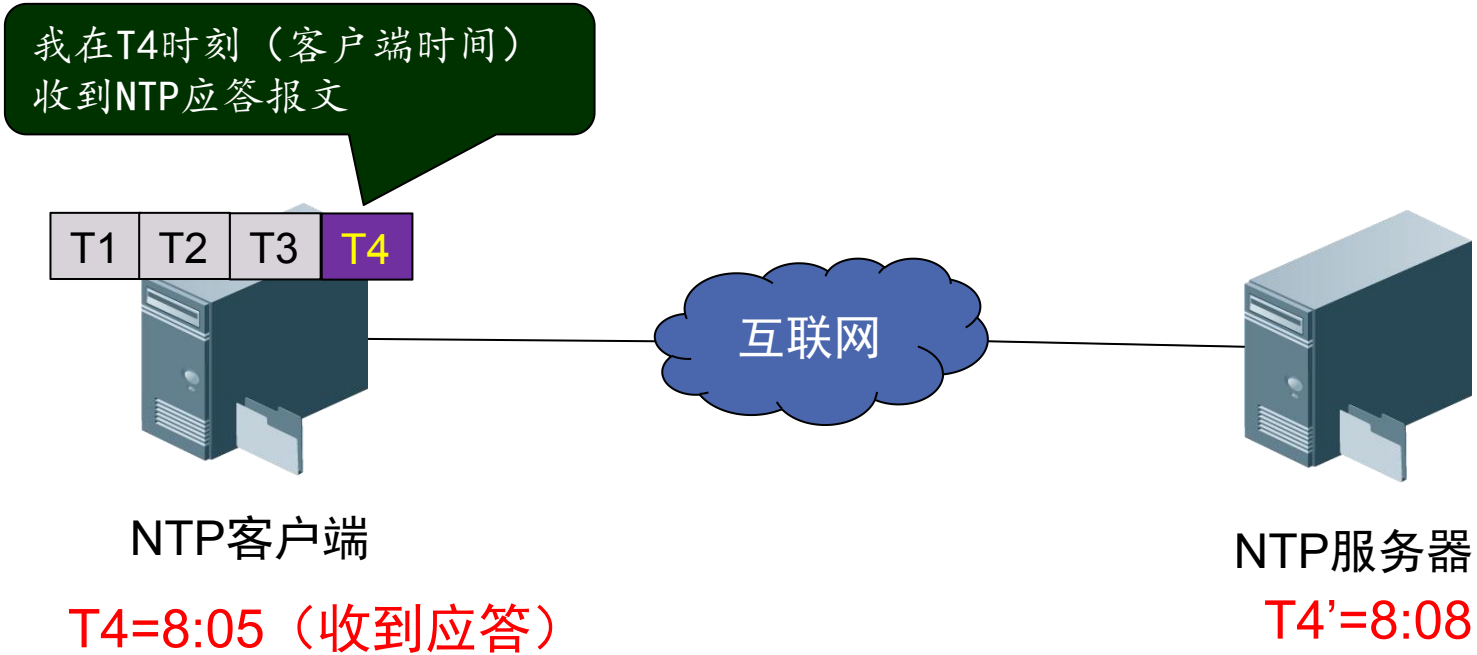
② NTP请求报文到达NTP服务器，此时NTP服务器的时刻为T2（服务器的时间，假设8:05）。



③ NTP服务器处理之后，于T3时刻（服务器的时间，假设8:06）发出NTP应答报文。该应答报文中携带离开NTP客户端时的时间戳T1、到达NTP服务器时的时间戳T2、离开NTP服务器时的时间戳T3



④ NTP客户端在T4时刻（客户端的时间，假设8:05）接收到该应答报文。

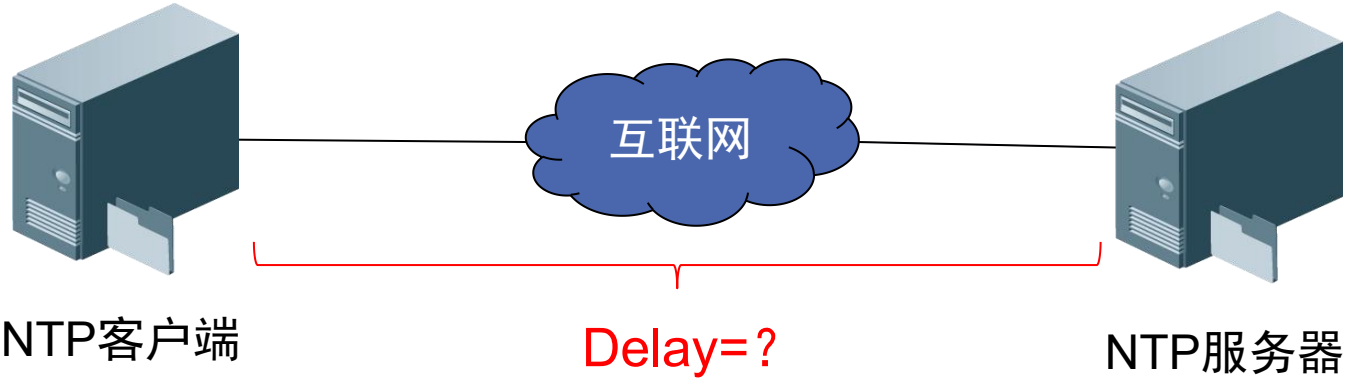


求：NTP报文从NTP客户端发送到NTP服务器所需要的平均时间Delay。

客：T1=8:00（发出请求）
服：T2=8:05（收到请求）
服：T3=8:06（发出应答）
客：T4=8:05（收到应答）

Delay = [ ( T4 - T1 ) - ( T3 – T2 ) ] / 2

代入T1～T4的假设值，得出Delay=2



求：设NTP客户端与NTP服务器之间的时间差为Offset。

以T4时刻为例，在这个时刻点（即NTP服务器发送过来的报文被客户端收到时），服务器的时刻已经为T3 + Delay。那么时间差Offset可由以下公式获得：

T4 + Offset = T3 + Delay

Offset = T3 + Delay-T4

=8:06+2-8:05=3

# NTP客户端根据Offset来调整自己的时钟，实现与NTP服务器的时钟同步

NTP客户：Ta+Offset

例如此处：Ta+3

Delay = [ ( T4 - T1 ) - ( T3 – T2 ) ] / 2=2

T4 + Offset = T3 + Delay

Offset = T3 + Delay-T4=3

假设客户端比标准时间快3分钟

例如T1=8:00，T2=7:59，T3=8:00，T4=8:05

Ta'=Ta+（-3）
相当于客户端将自身时间减慢3分钟，变为标准时间

Delay = [ ( T4 - T1 ) - ( T3 – T2 ) ] / 2=2

T4 + Offset = T3 + Delay

Offset = T3 + Delay-T4= - 3


NTP客户端　　NTP服务器

注意：比标准时间快3分钟

# 三、NTP

## 3.5 公共的NTP服务器

# NTP - 公共的NTP服务器

- 中国科学院国家授时中心： http://www.ntsc.ac.cn/
  - NTP服务器
    - ntp.ntsc.ac.cn

# NTP - 公共的NTP服务器

- 中国公共NTP服务器： https://www.pool.ntp.org/zone/cn
  - NTP服务器
    - 0.cn.pool.ntp.org
    - 1.cn.pool.ntp.org
    - 2.cn.pool.ntp.org
    - 3.cn.pool.ntp.org

# NTP - 公共的NTP服务器

- 阿里云公共NTP
  - NTP服务器
    - ntp.aliyun.com
    - ntp1.aliyun.com
    - ntp2.aliyun.com
    - ntp3.aliyun.com
    - ntp4.aliyun.com
    - ntp5.aliyun.com
    - ntp6.aliyun.com
    - ntp7.aliyun.com

# NTP - 公共的NTP服务器

- 腾讯公共NTP
- https://cloud.tencent.com/document/product/213/30392
  - NTP服务器：
    - ntp.aliyun.com
    - ntp1.aliyun.com
    - ntp2.aliyun.com
    - ntp3.aliyun.com
    - ntp4.aliyun.com
    - ntp5.aliyun.com
    - ntp6.aliyun.com
    - ntp7.aliyun.com

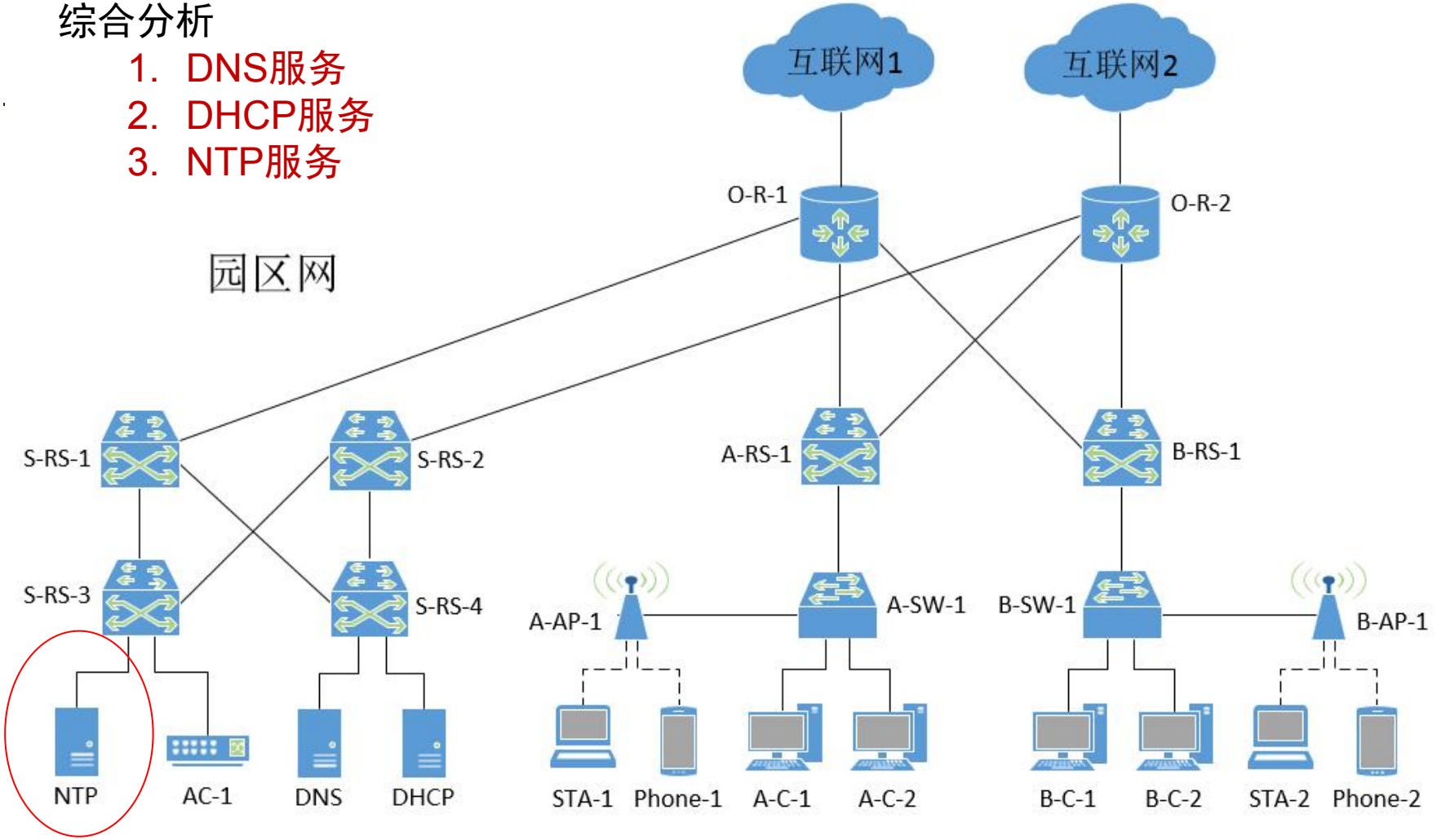
【结合实验自主学习】

# 三、NTP

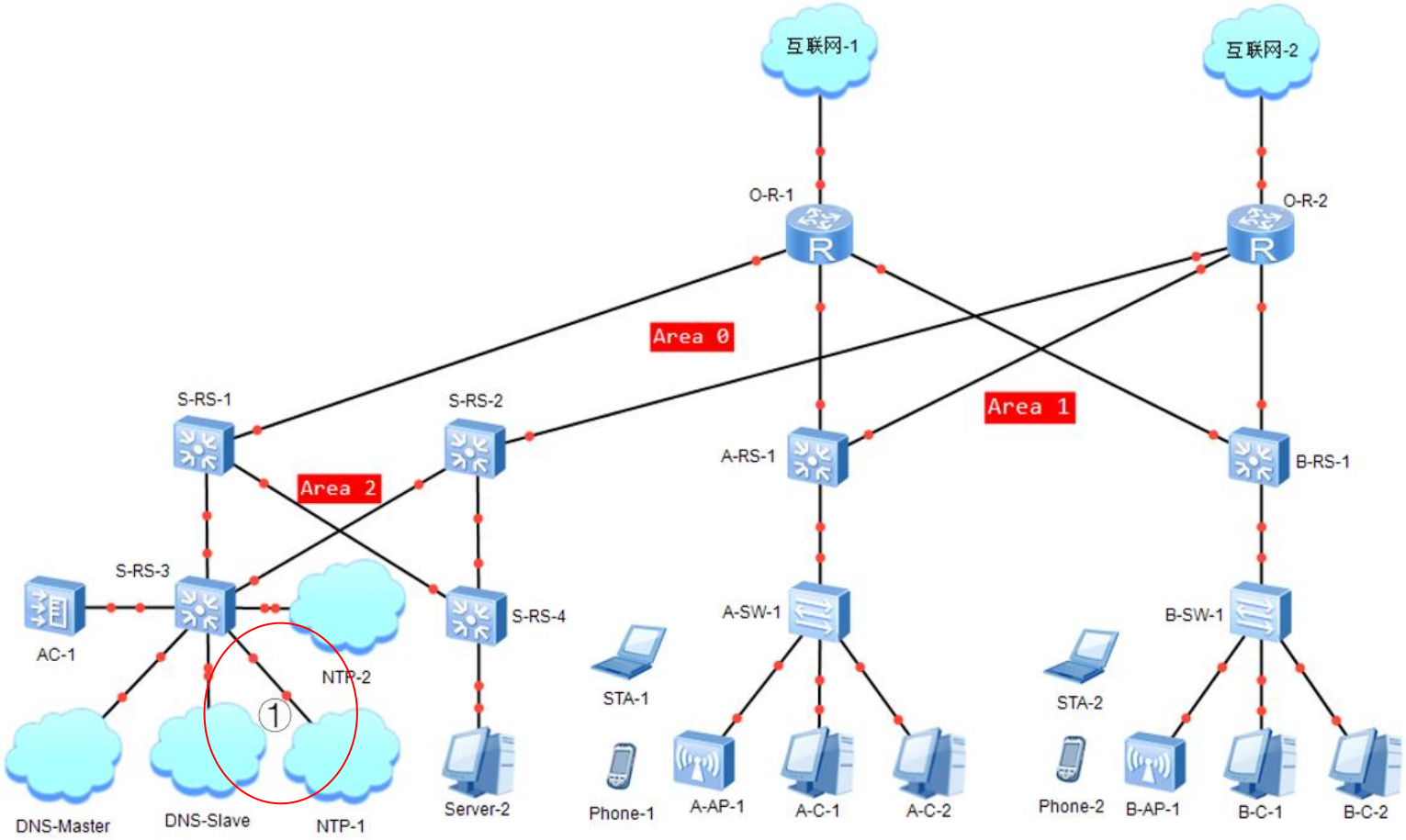
## 3.6 抓包分析NTP报文

## 综合分析

1. DNS服务
2. DHCP服务
3. NTP服务

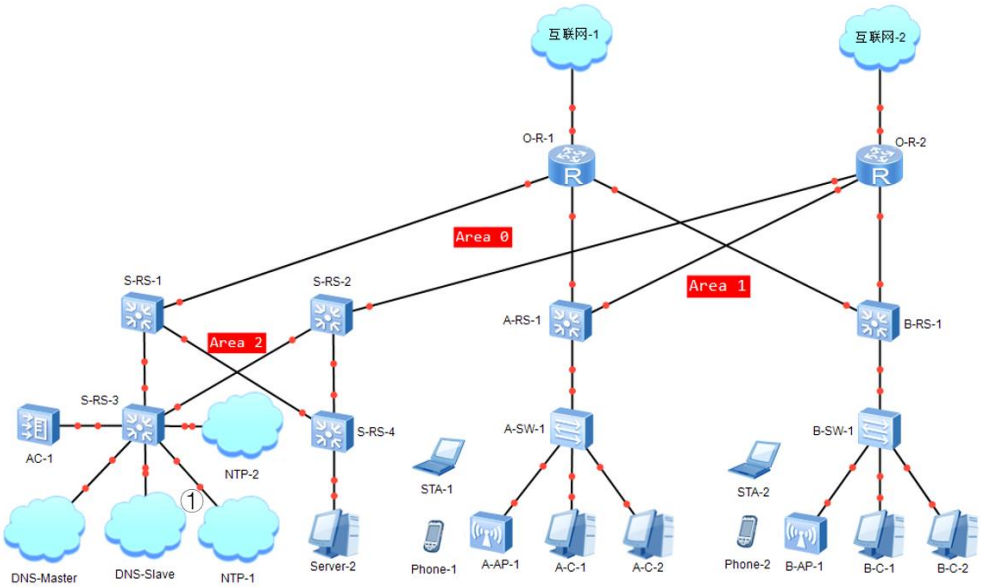


# ➢ 设置抓包点


互联网-1
互联网-2
O-R-1
O-R-2
Area 0
Area 1
Area 2
S-RS-1
S-RS-2
S-RS-3
S-RS-4
A-RS-1
B-RS-1
AC-1
NTP-2
NTP-1
DNS-Master
DNS-Slave
①
Server-2
STA-1
Phone-1
A-SW-1
A-AP-1
A-C-1
A-C-2
STA-2
Phone-2
B-SW-1
B-AP-1
B-C-1
B-C-2

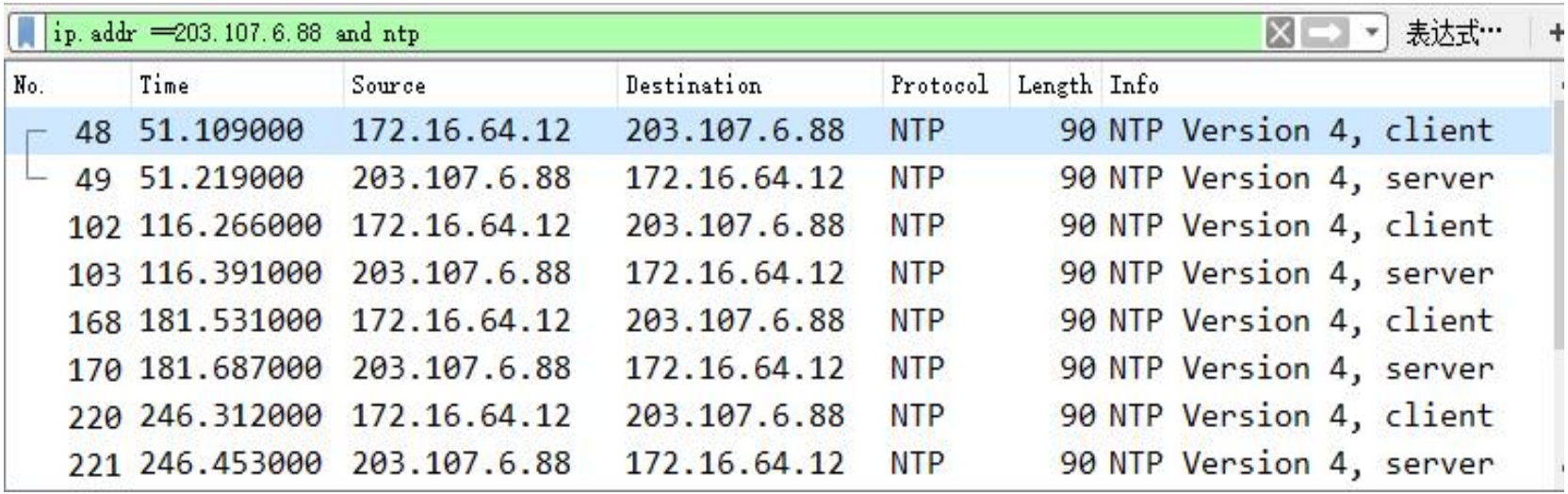
# ➢ 设置抓包点

- 园区网内部的DNS服务器和网络设备自动向园区网内的NTP服务器发出时间同步请求，并获取时间同步；而园区网内的NTP服务器除了要响应园区网内部其他设备发来的时间同步请求之外，其自身还要和互联网上的公共NTP服务器之间进行时间同步操作。




- 因此，在Cloud设备NTP-1的Ethernet 0/0/1接口处启动抓包程序，既可抓取NTP-1和园区网内的其他服务器以及网络设备之间的NTP报文，也可以抓取NTP-1和其chrony配置文件中设置的公共NTP服务器（即ntp.aliyun.com）之间的NTP报文。

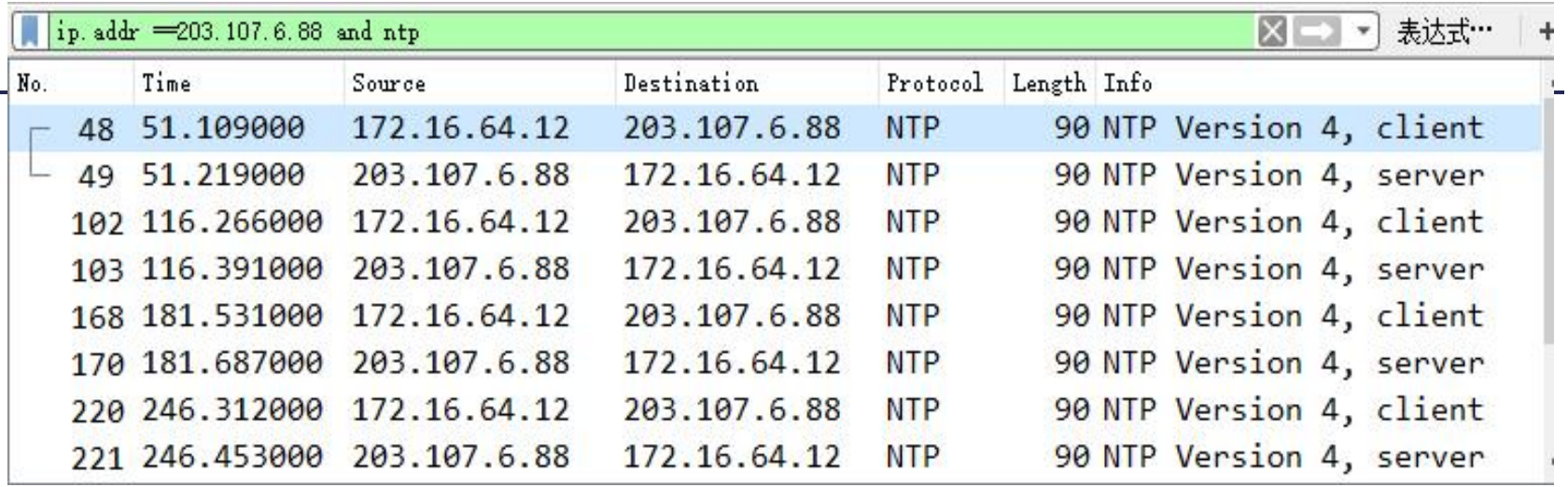
## ➢ NTP报文列表



ip.addr ==203.107.6.88 and ntp　　表达式…

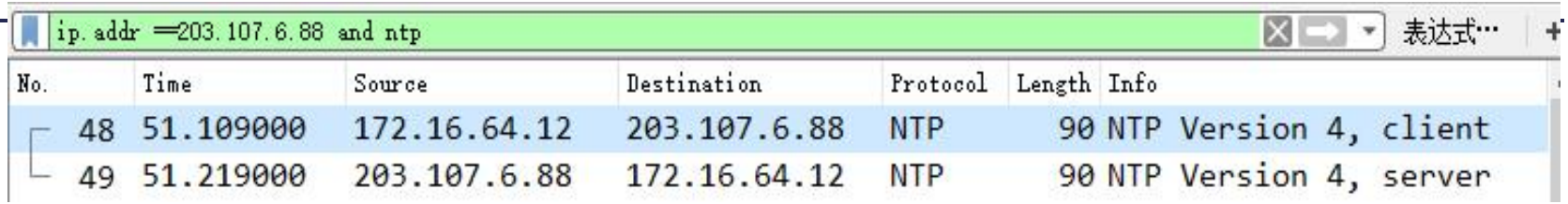
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 48 | 51.109000 | 172.16.64.12 | 203.107.6.88 | NTP | 90 | NTP Version 4, client |
| 49 | 51.219000 | 203.107.6.88 | 172.16.64.12 | NTP | 90 | NTP Version 4, server |
| 102 | 116.266000 | 172.16.64.12 | 203.107.6.88 | NTP | 90 | NTP Version 4, client |
| 103 | 116.391000 | 203.107.6.88 | 172.16.64.12 | NTP | 90 | NTP Version 4, server |
| 168 | 181.531000 | 172.16.64.12 | 203.107.6.88 | NTP | 90 | NTP Version 4, client |
| 170 | 181.687000 | 203.107.6.88 | 172.16.64.12 | NTP | 90 | NTP Version 4, server |
| 220 | 246.312000 | 172.16.64.12 | 203.107.6.88 | NTP | 90 | NTP Version 4, client |
| 221 | 246.453000 | 203.107.6.88 | 172.16.64.12 | NTP | 90 | NTP Version 4, server |

园区网内部的NTP服务器NTP-1（172.16.64.12）与公共NTP服务器（203.107.6.88）之间的时间同步报文

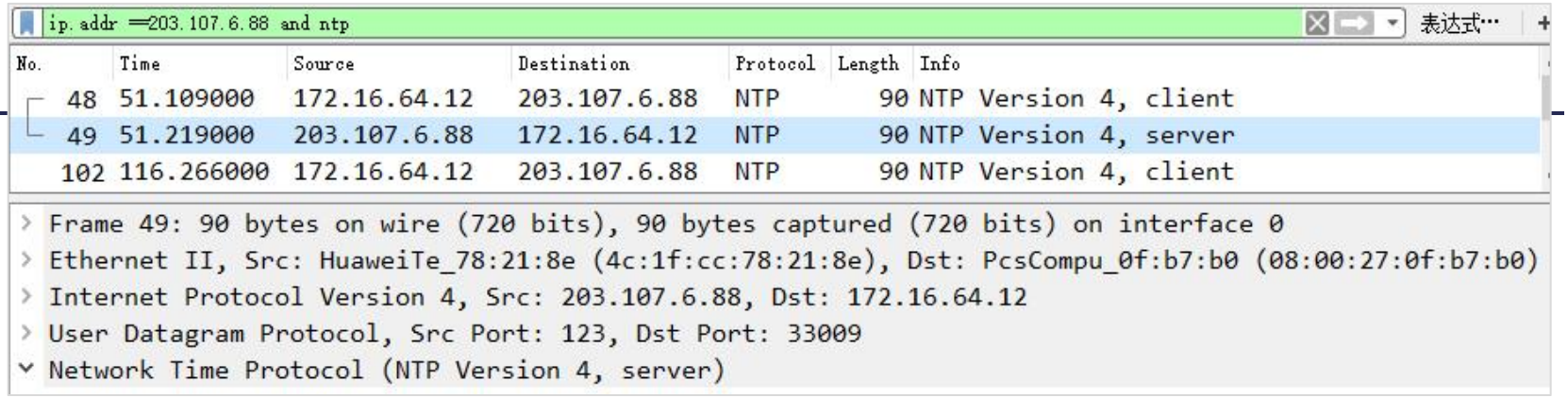



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 48 | 51.109000 | 172.16.64.12 | 203.107.6.88 | NTP | 90 | NTP Version 4, client |
| 49 | 51.219000 | 203.107.6.88 | 172.16.64.12 | NTP | 90 | NTP Version 4, server |
| 102 | 116.266000 | 172.16.64.12 | 203.107.6.88 | NTP | 90 | NTP Version 4, client |
| 103 | 116.391000 | 203.107.6.88 | 172.16.64.12 | NTP | 90 | NTP Version 4, server |
| 168 | 181.531000 | 172.16.64.12 | 203.107.6.88 | NTP | 90 | NTP Version 4, client |
| 170 | 181.687000 | 203.107.6.88 | 172.16.64.12 | NTP | 90 | NTP Version 4, server |
| 220 | 246.312000 | 172.16.64.12 | 203.107.6.88 | NTP | 90 | NTP Version 4, client |
| 221 | 246.453000 | 203.107.6.88 | 172.16.64.12 | NTP | 90 | NTP Version 4, server |

- 此处的NTP时间同步方式是Client/Server方式，其中，NTP-1属于NTP客户端（client），而互联网上的公共NTP服务器（203.107.6.88）则作为NTP服务器端（server），向NTP-1提供时间同步服务；
- 通过48、102、168和220号报文的“Time”字段的值可知，默认情况下，NTP客户端（此处为NTP-1）大约每64秒与其上级NTP服务器（此处是公共NTP服务器203.107.6.88）进行一次时间同步。




- 以49号报文为例，分析NTP报文的内容。
- 这是从互联网上的公共NTP服务器（203.107.6.88）发往NTP-1（172.16.64.12）的NTP响应报文，即NTP服务器端发往NTP客户端的报文。




- 分析报文首部基本信息

| 序号 | 名称 | 内容 / 值 | 备注 |
|---|---|---|---|
| 数据链路层首部 | 源MAC地址 | 4c-1f-cc-78-21-8e | S-RS-3的MAC地址，即NTP-1所在网络的默认网关的MAC地址 |
| | 目的MAC地址 | 08:00:27:0f:b7:b0 | NTP-1的MAC地址 |
| 网络层首部 | 源IP地址 | 203.107.6.88 | 阿里云公共NTP服务器IP地址 |
| | 目的IP地址 | 172.16.64.12 | NTP-1的IP地址 |
| 运输层首部 | 运输层协议 | UDP | User Datagram Protocol- |
| | 源端口 | 123 | NTP服务器端 |
| | 目的端口 | 33009 | NTP客户端 |

## ➢ 分析报文NTP内容

```
Network Time Protocol (NTP Version 4, server)
  Flags: 0x24, Leap Indicator: no warning, Version number: NTP Version 4, Mode: server
  Peer Clock Stratum: secondary reference (2)
  Peer Polling Interval: 6 (64 sec)
  Peer Clock Precision: 0.000000 sec
  Root Delay: 0.011871337890625 seconds
  Root Dispersion: 0.000579833984375 seconds
  Reference ID: 10.137.38.86
  Reference Timestamp: Mar 14, 2021 09:27:47.952487823 UTC
  Origin Timestamp: Apr  5, 2007 10:22:48.440507649 UTC
  Receive Timestamp: Mar 14, 2021 09:28:41.284131190 UTC
  Transmit Timestamp: Mar 14, 2021 09:28:41.284145160 UTC
```

## ➢ 分析报文NTP内容

| 序号 | 名称 | 内容 / 值 | 备注 |
|---|---|---|---|
| 1 | Leap Indicator | no warning | 无闰秒提示 |
| 2 | Version number | NTP Version 4 | 当前版本是NTPv4 |
| 3 | Mode | Server | 以服务器模式工作 |
| 4 | Peer Clock Stratum | Secondary reference (2) | 对等时钟的层数为第2级 |
| 5 | Peer poll Interval | 6 (64 sconds) | 对等轮询间隔时间为64秒 |
| 6 | Peer Clock Precision | 0.000000 seconds | 对等时钟精度 |
| 7 | Root Delay | 0.01187133789… seconds | 到主参考时钟的总往返延迟时间 |
| 8 | Root Dispersion | 0.00057983398… seconds | 本地时钟相对于主参考时钟的最大误差 |
| 9 | Reference ID | 10.137.38.86 | 参考时钟的ID |
| 10 | Reference Timestamp | Mar 14, 2021 09:27:47.952487823 UTC | 本地时钟最近一次同步的时间 |
| 11 | Origin Timestamp | Apr 5, 2007 10:22:48.440507649 UTC | NTP报文离开源端（即NTP-1）的时间 |
| 12 | Receive Timestamp | Mar 14, 2021 09:28:41.284131190 UTC | 本端（即公共NTP）收到NTP报文时间 |
| 13 | Transmit Timestamp | Mar 14, 2021 09:28:41.284145160 UTC | 本端（即公共NTP）应答报文发出时间 |

# 第5讲 网络基础服务

完