网络安全——

网络攻击—DNS威胁与防范

北京邮电大学
郑康锋
kfzheng@bupt.edu.cn

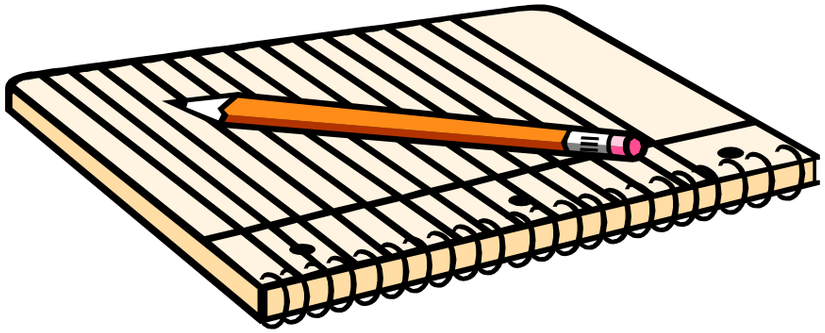
目录

学习完本次课程，您应该能够了解：

- DNS概述
- DNS协议
- DNS工作流程
- DNS安全威胁
- DNS安全防范

DNS安全威胁及防范

- DNS概述
- DNS协议
- DNS工作流程
- DNS安全威胁
- DNS安全防范



DNS 概述

- 域名系统（Domain Name System，DNS）负责在域名和IP地址之间进行转换，是互联网的基础设施。

```
C:\Users\zkf>nslookup
默认服务器:  UnKnown
Address:  10.3.9.4

> www.bupt.edu.cn
服务器:  UnKnown
Address:  10.3.9.4

非权威应答:
名称:    vn46.bupt.edu.cn
Addresses:  2001:da8:215:4038::161
          10.3.9.161
Aliases:  www.bupt.edu.cn

> www.baidu.com
服务器:  UnKnown
Address:  10.3.9.4

非权威应答:
名称:    www.a.shifen.com
Addresses:  220.181.38.150
          220.181.38.149
Aliases:  www.baidu.com
```

解析域名

```
C:\Users\zkf>ping www.bupt.edu.cn
正在 Ping vn46.bupt.edu.cn [2001:da8:215:4038::161] 具有 32 字节的数据:
来自 2001:da8:215:4038::161 的回复: 时间=1ms
来自 2001:da8:215:4038::161 的回复: 时间<1ms
来自 2001:da8:215:4038::161 的回复: 时间=1ms
来自 2001:da8:215:4038::161 的回复: 时间<1ms
2001:da8:215:4038::161 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 1ms，平均 = 0ms

C:\Users\zkf>ping www.baidu.com
正在 Ping www.a.shifen.com [220.181.38.150] 具有 32 字节的数据:
来自 220.181.38.150 的回复: 字节=32 时间=2ms TTL=51
来自 220.181.38.150 的回复: 字节=32 时间=3ms TTL=51
来自 220.181.38.150 的回复: 字节=32 时间=2ms TTL=51
来自 220.181.38.150 的回复: 字节=32 时间=2ms TTL=51

220.181.38.150 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms，最长 = 3ms，平均 = 2ms
```

Ping域名

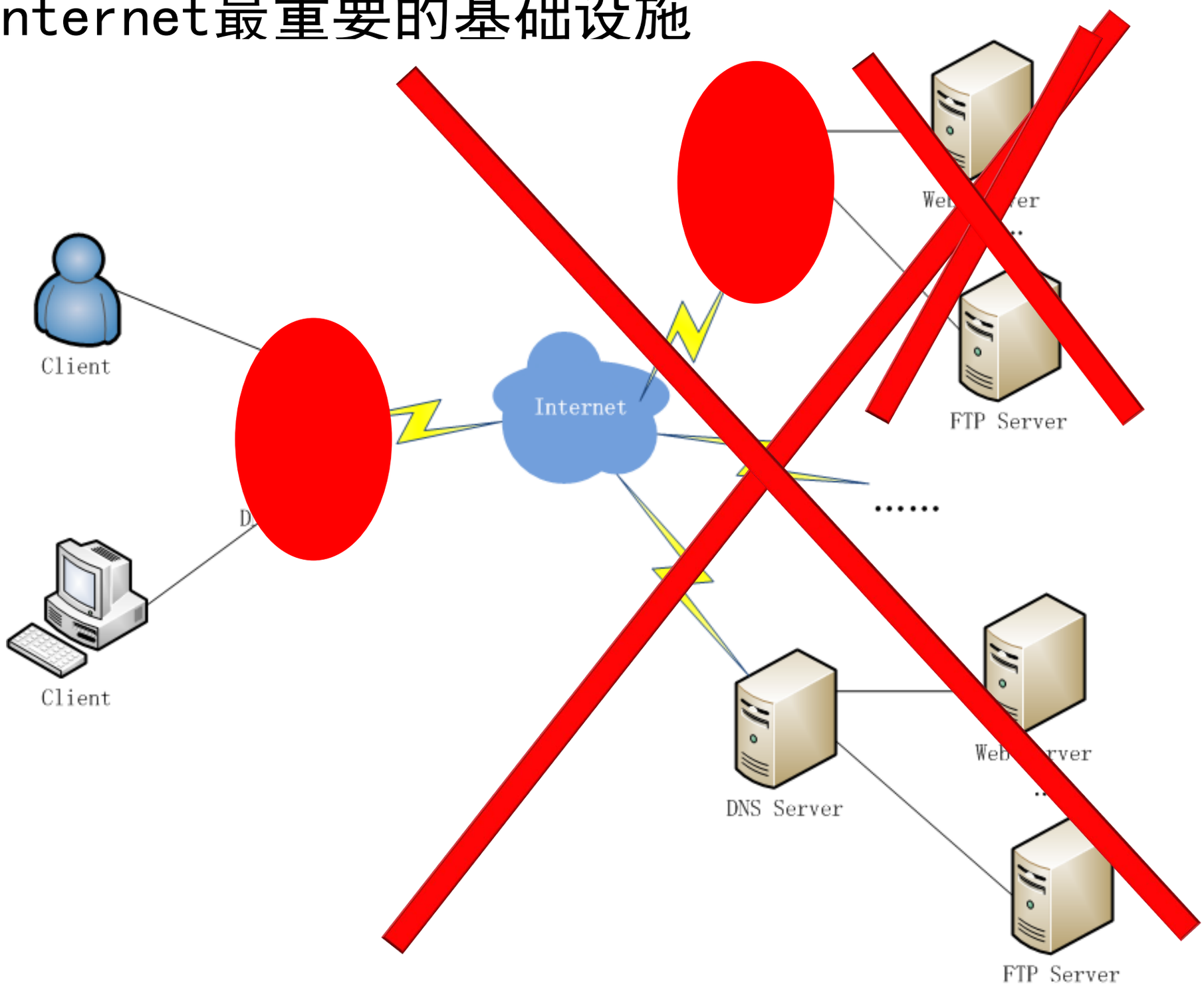
什么是DNS?

- 域名系统（Domain Name System, DNS）
- 负责在域名和IP地址之间进行转换
- 是Internet中最重要的基础设施

- The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.
- It associates various information with domain names assigned to each of the participating entities.
- Most prominently, it translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide.

DNS概述

- Internet最重要的基础设施



DNS概述

- 早在ARPANET时代，整个网络上只有数百台计算机，那时使用一个hosts文件，列出所有主机的名字和相应的IP地址。只要用户输入一个主机的名字，计算机就能很快的将这个主机名字解析成机器能够识别的二进制IP地址。

- 虽然从理论上讲，可以只使用一个名称服务器，使它装入因特网上所有的主机名，并回答所有对IP地址的查询，但是随着网络的扩大，这样的域名服务器肯定会因过负荷而无法正常工作，而且一旦该域名服务器出现故障，整个网络就会瘫痪。

DNS概述

- 1983年因特网开始采用层次结构的命名树作为主机的名字，并使用分布式的域名系统DNS【RFC 1034,1035】，这两个文档已经成为因特网的正式标准。
- 因特网的域名系统被设计成为一个**联机分布式数据库系统**，并采用客户服务器方式运行。
- DNS使用的大多数名字都可在本地解析，仅有少量解析需要在因特网上通信，因此系统效率很高。
- 由于DNS是分布式系统，即使单个计算机出现故障，也不会妨碍整个系统的运行。

DNS概述

- 因特网域名系统采用层次树状结构的命名方法，任何一个连接到因特网的主机或路由器都有一个**唯一的层次结构的名字**，即域名（Domain Name）。这里，“域”是名字空间中的一个可被管理的划分。域还可以继续划分为子域，如：二级域、三级域等。

- 域名结构由若干分量组成，各分量之间用点隔开，如：

  ．．．.三级域名.二级域名.顶级域名

- 各分量代表不同级别的域名，每一级域名都由英文字母和数字组成，不区分大小写。域名系统既不规定一个域名需要包含多少个下级域名，也不规定每一级域名代表什么意思。

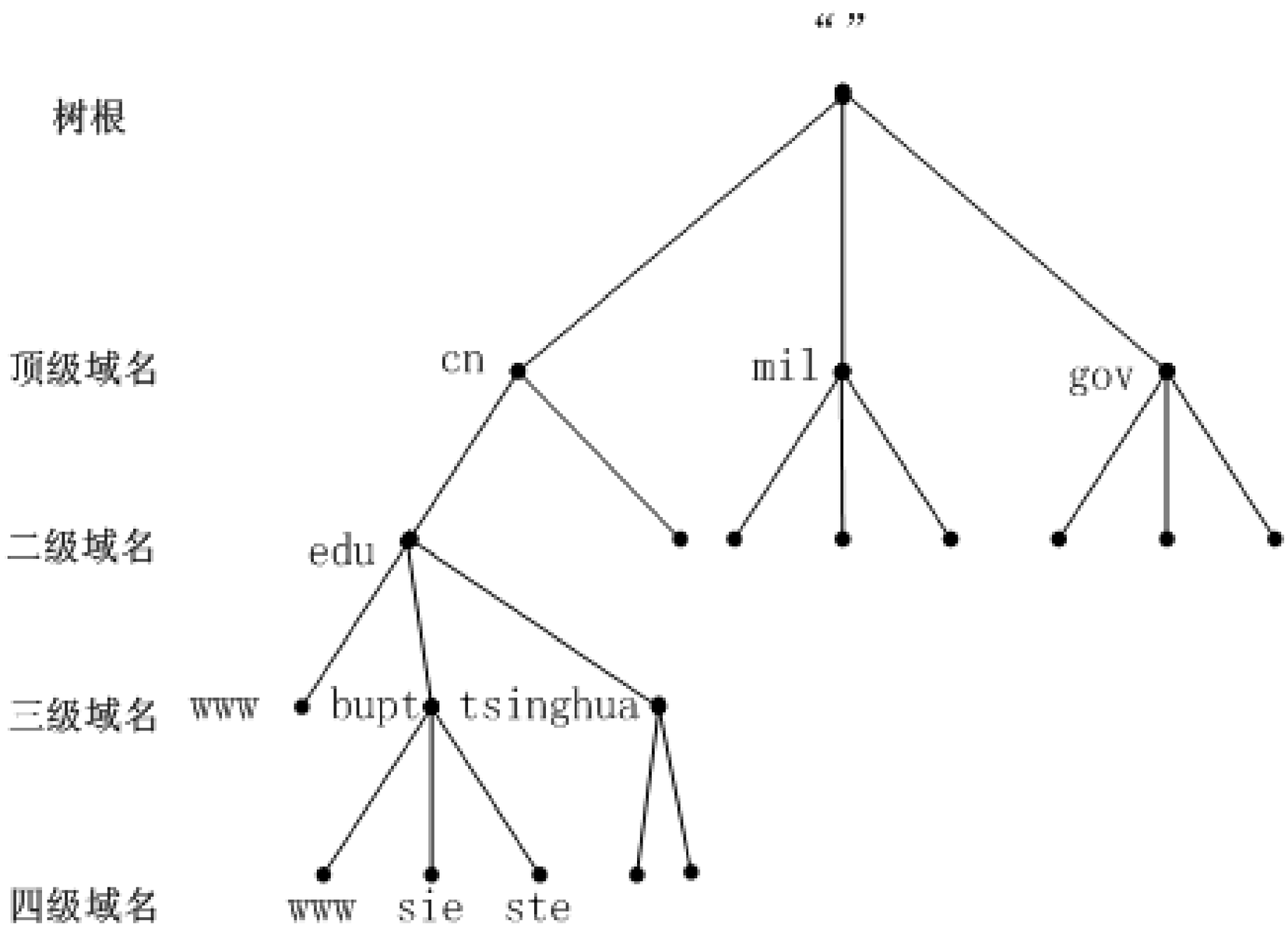
- 各级域名由其上一级域名管理机构管理。这种方法可使每个名字是唯一的，并且也容易设计一种域名查找机制。需要注意的是，域名只是一个逻辑概念，并不代表计算机所在的物理位置。

DNS概述

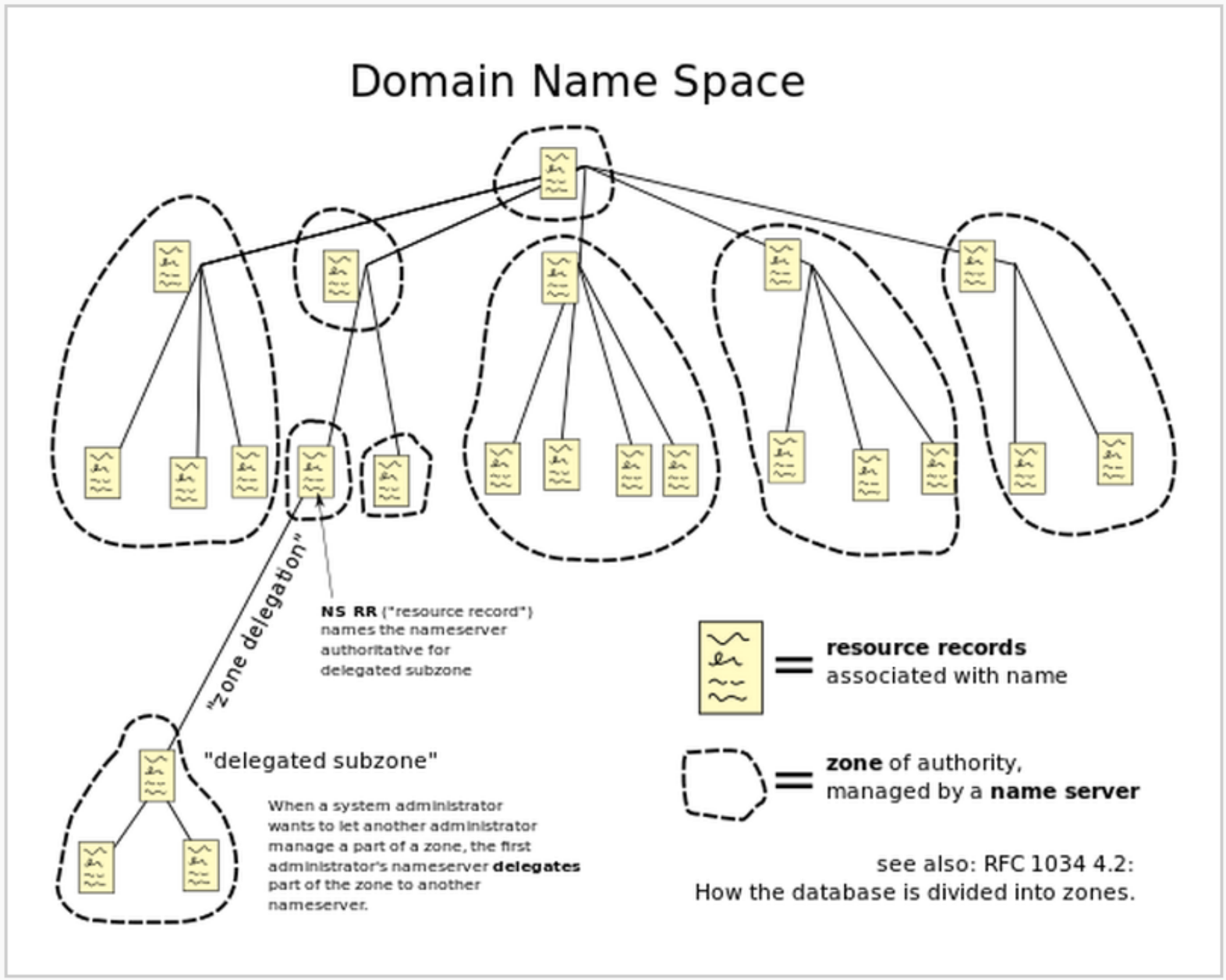
- 通用顶级域名（gTLD）
  - .com/.net/.org/.edu/.gov/.mil/.int
  - .cn
  - .mobi
  - .asia
  - .biz(new)
  - .info(new)
  - .name(new)
  - .cc, .tv, .sh, .hk

DNS概述

- 域名空间，树形结构



Domain Name Space



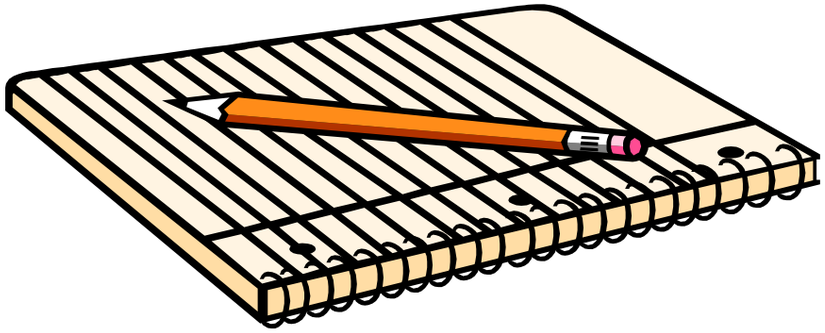
The hierarchical Domain Name System, organized into zones, each served by a name server

DNS常用命令（Windows）

- ipconfig/all
  - 查看网络配置情况，包括DNS服务器IP。
- ipconfig /flushdns
  - 清除DNS缓存
- ipconfig /displaydns
  - 查看DNS缓存
- Nslookup
  - 查看DNS解析结果。

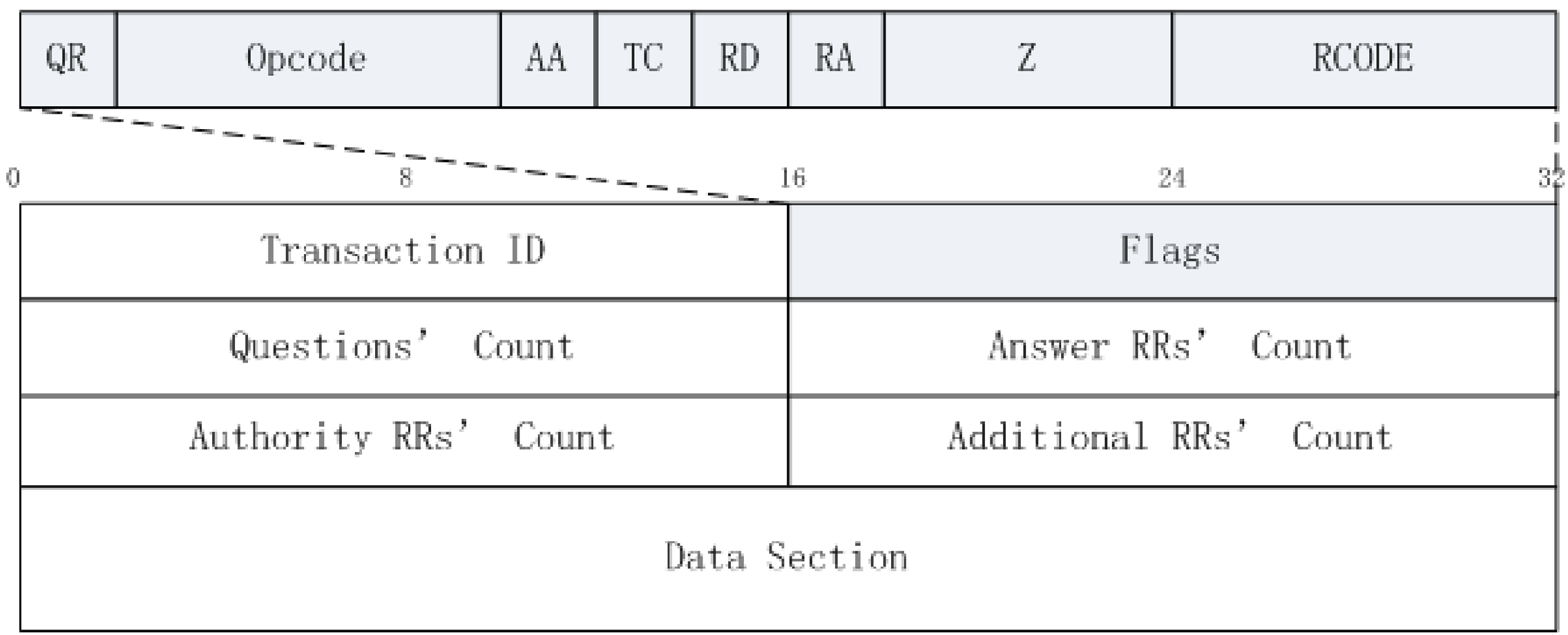
DNS安全威胁及防范

- DNS概述
- DNS协议
- DNS工作流程
- DNS安全威胁
- DNS安全防范



DNS协议

- DNS既可以使用TCP，又可以使用UDP，端口为53.
  - DNS主从服务器之间区传送传输时使用TCP协议
  - 客户端与DNS服务器之间传输时用的是UDP协议
- DNS报文格式如下：



DNS协议

- Transaction ID – 用于连接查询和答复的16bit。
- Question count – 16位字段，用以定义问题的个数。
- Answer count – 16位字段，用以定义回答的资源个数。
- Authority count – 16位字段，用以定义名字服务器的资源个数。
- Additional count – 16位字段，用以定义附加记录部分的资源个数。
- Data Section – 不定长度。

  依次添入问题、应答、名字服务器、附加记录的详细信息。

DNS协议

- Flags
  - QR－ 识别查询和答复消息的1位字段：
    0 查询；
    1 应答；
  - Opcode － 描述消息类型的4位字段：
    0 标准查询（由名字到地址）；
    1 逆向查询；
    2 服务状态请求 ；
  - AA － 命令回答：1位字段。当设置为1时，识别由命令名字服务器作出的答复
  - TC － 切断。1位字段。当设置为1，表明消息已被切断。
  - RD － 1位字段。由名字服务器设置为1请求递归服务。
  - RA －1位字段。由名字服务器设置表示递归服务的可用性。
  - Z －3位字段。备用，设置为0。
  - Rcode － 响应代码，由名字服务器设置的4位字段用以识别查询状态。

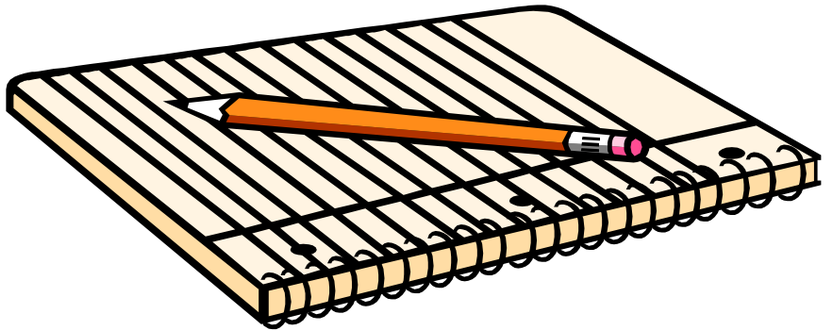
DNS协议

No.	Time	Source	Destination	Protocol	Info
14	6.919898	172.16.0.113	172.16.0.4	DNS	Standard query A hhz.242.net
15	6.920977	172.16.0.4	172.16.0.113	DNS	Standard query response A 222.128.5.182

```
⊞ Frame 15 (87 bytes on wire, 87 bytes captured)
⊞ Ethernet II, Src: 172.16.0.4 (00:0c:29:f8:9e:14), Dst: 172.16.0.113 (00:19:d1:4f:df:4e)
⊞ Internet Protocol, Src: 172.16.0.4 (172.16.0.4), Dst: 172.16.0.113 (172.16.0.113)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 1063 (1063)
⊟ Domain Name System (response)
    Transaction ID: 0x0008
  ⊟ Flags: 0x8180 (Standard query response, No error)
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ hhz.242.net: type A, class IN
        Name: hhz.242.net
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ hhz.242.net: type A, class IN, addr 222.128.5.182
        Name: hhz.242.net
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 12 minutes, 17 seconds
        Data length: 4
        Addr: 222.128.5.182
```

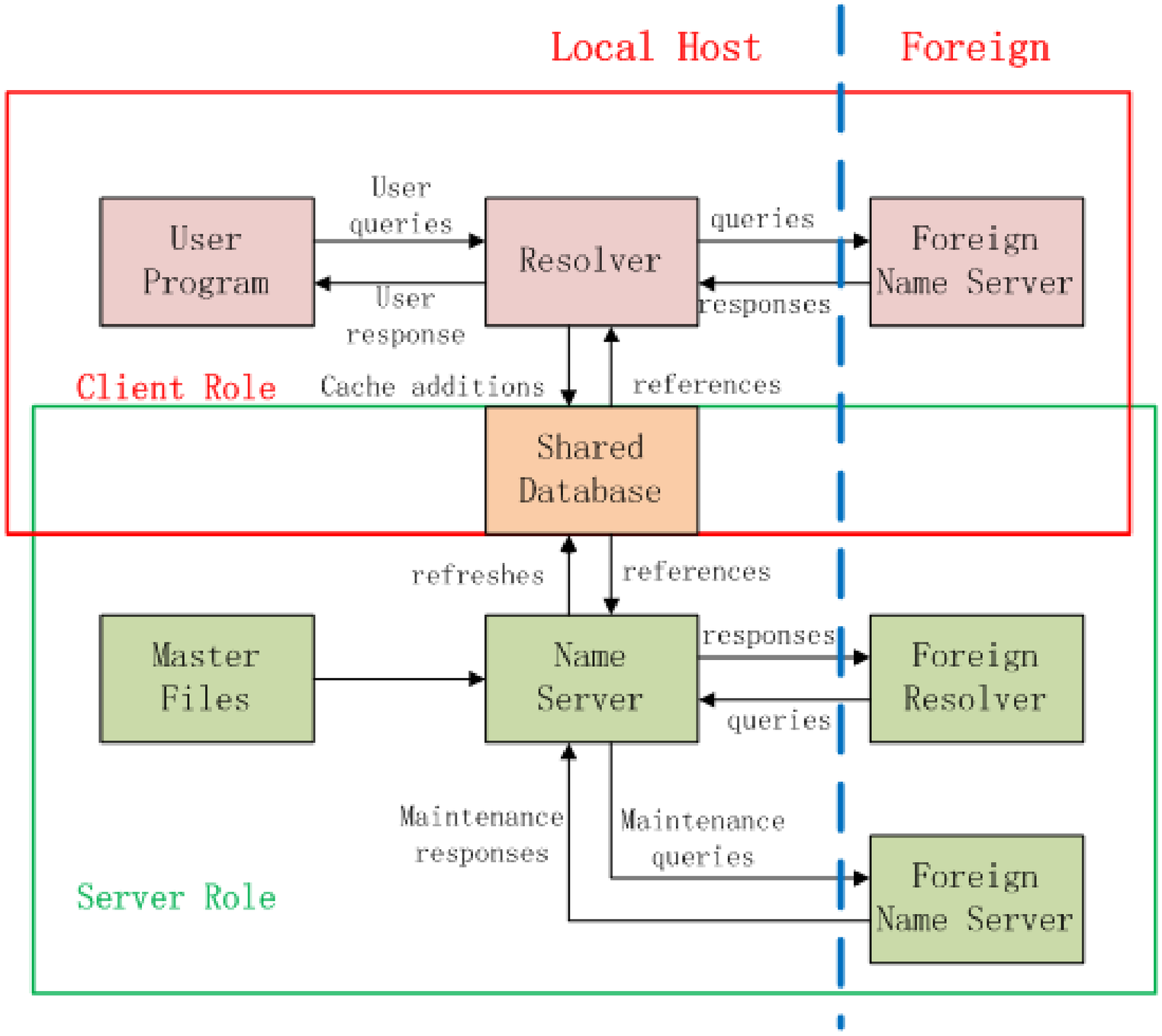
DNS安全威胁及防范

- DNS概述
- DNS协议
- DNS工作流程
- DNS安全威胁
- DNS安全防范



DNS 工作流程

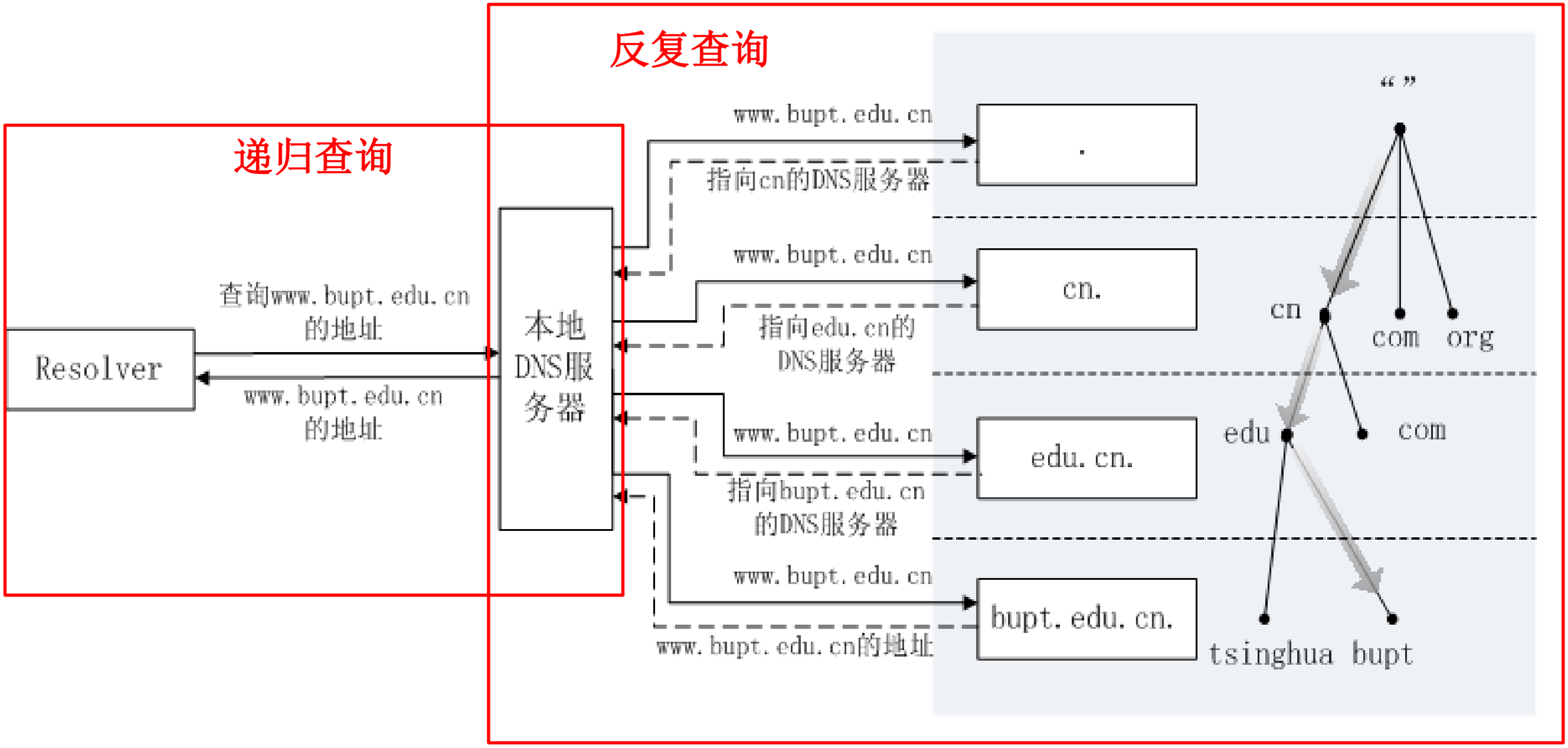
一个兼有客户端和服务器功能的本地主机工作方式。



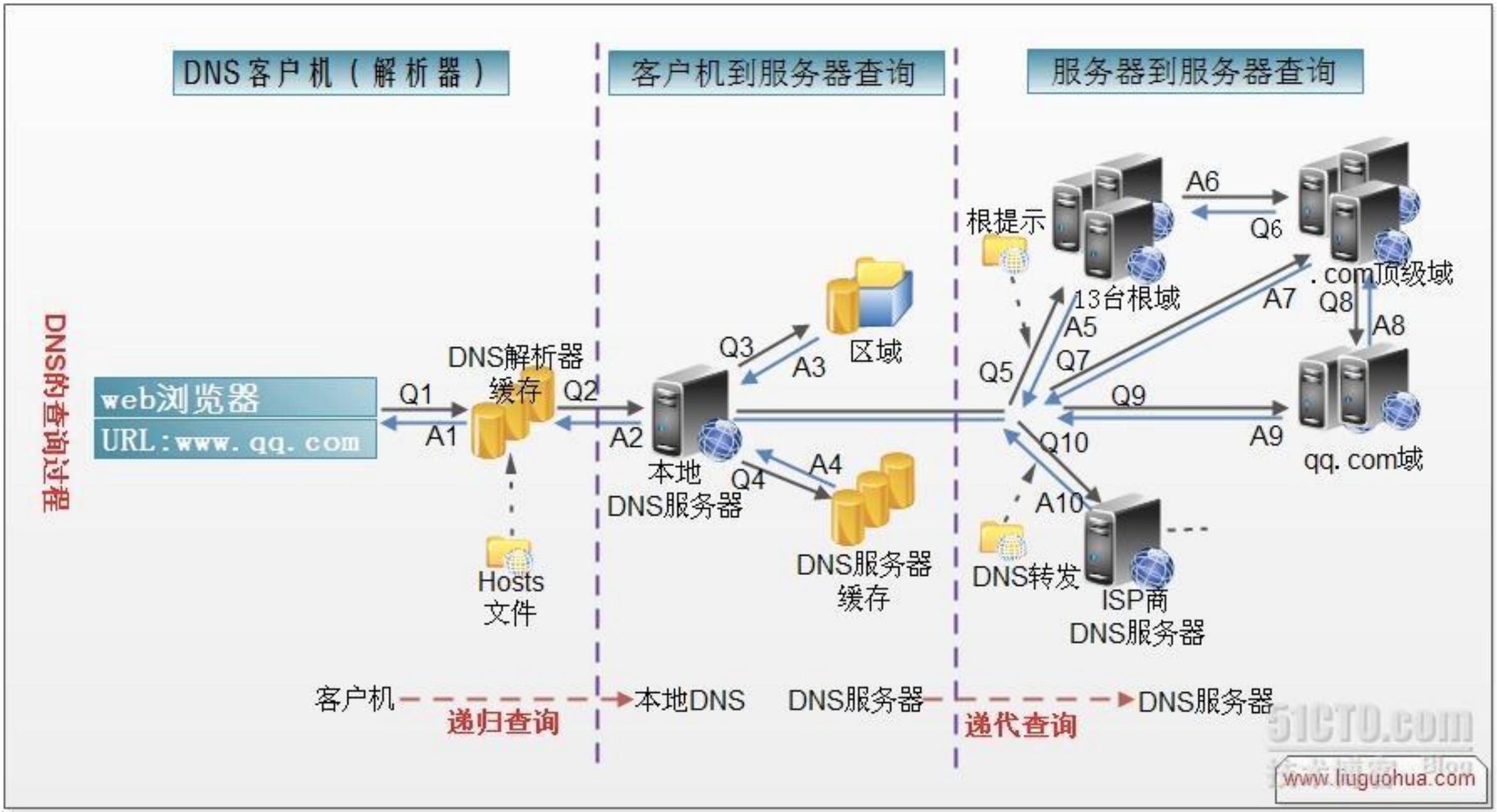
DNS工作流程

- 查询方式
  - **递归查询：**一般客户机和服务器之间是递归查询，DNS服务器如果未能在本地找到相应的信息，就代替用户向其它服务器进行查询，这时它是代替用户扮演了解析器（resolver）的角色，直到最后把结果找到，也可能根本没有结果，那就返回错误，并返回给用户为止。
  - **反复查询（迭代查询）：**一般服务器之间属于反复查询。DNS服务器返回的要么是本地存在的结果信息，要么是一个错误码，告诉查询者你要的信息这里没有，然后再返回一个可能会有查询结果的DNS服务器地址，让查询者到那里去查一查。

DNS工作流程


反复查询
递归查询
Resolver
查询www.bupt.edu.cn
的地址
www.bupt.edu.cn
的地址
本地
DNS服
务器
www.bupt.edu.cn
指向cn的DNS服务器
www.bupt.edu.cn
指向edu.cn的
DNS服务器
www.bupt.edu.cn
指向bupt.edu.cn
的DNS服务器
www.bupt.edu.cn
www.bupt.edu.cn的地址
.
cn.
edu.cn.
bupt.edu.cn.
“ ”
cn
com
org
edu
com
tsinghua
bupt

DNS工作机制

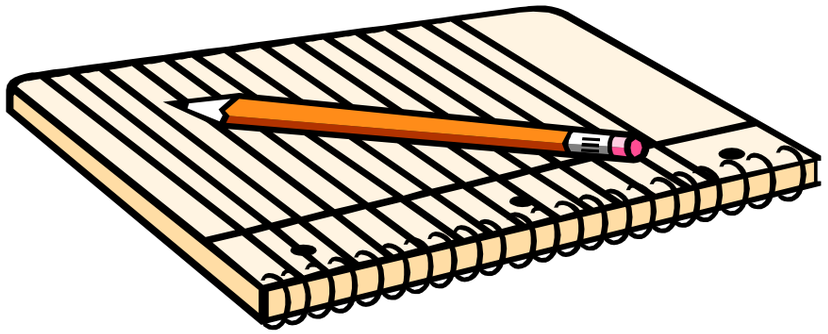

DNS客户机（解析器）
客户机到服务器查询
服务器到服务器查询
DNS的查询过程
web浏览器
URL：www.qq.com
Q1
A1
DNS解析器
缓存
Q2
A2
Hosts
文件
本地
DNS服务器
Q3
A3
区域
Q4
A4
DNS服务器
缓存
根提示
13台根域
A5
Q5
A6
Q6
A7
Q7
.com顶级域
Q8
A8
Q9
A9
qq.com域
Q10
A10
DNS转发
ISP商
DNS服务器
客户机
递归查询
本地DNS
DNS服务器
递代查询
DNS服务器
51CTO.com
www.liuguohua.com

DNS工作机制

DNS的查询模式
(迭代)
Server2
Server1
管理根(root)的DNS服务器
DNS服务器
(迭代)
Server3
(递归)
(迭代)
管理.com的DNS服务器
www.sohu.com的IP地址是？
Server4
管理sohu.com的DNS服务器
DNS客户端

DNS安全威胁及防范

- DNS概述
- DNS协议
- DNS工作流程
- DNS安全威胁
- DNS安全防范



DNS安全威胁

- 安全缺陷
  - 单点故障
  - 软件实现漏洞
    - 缓冲区溢出
    - 拒绝服务
- 恶意攻击
  - 欺骗（ DNS spoofing ）
  - 缓存中毒（cache posioning）
  - 缓冲区溢出漏洞攻击
  - 拒绝服务攻击
  - 信息泄露

DNS安全威胁

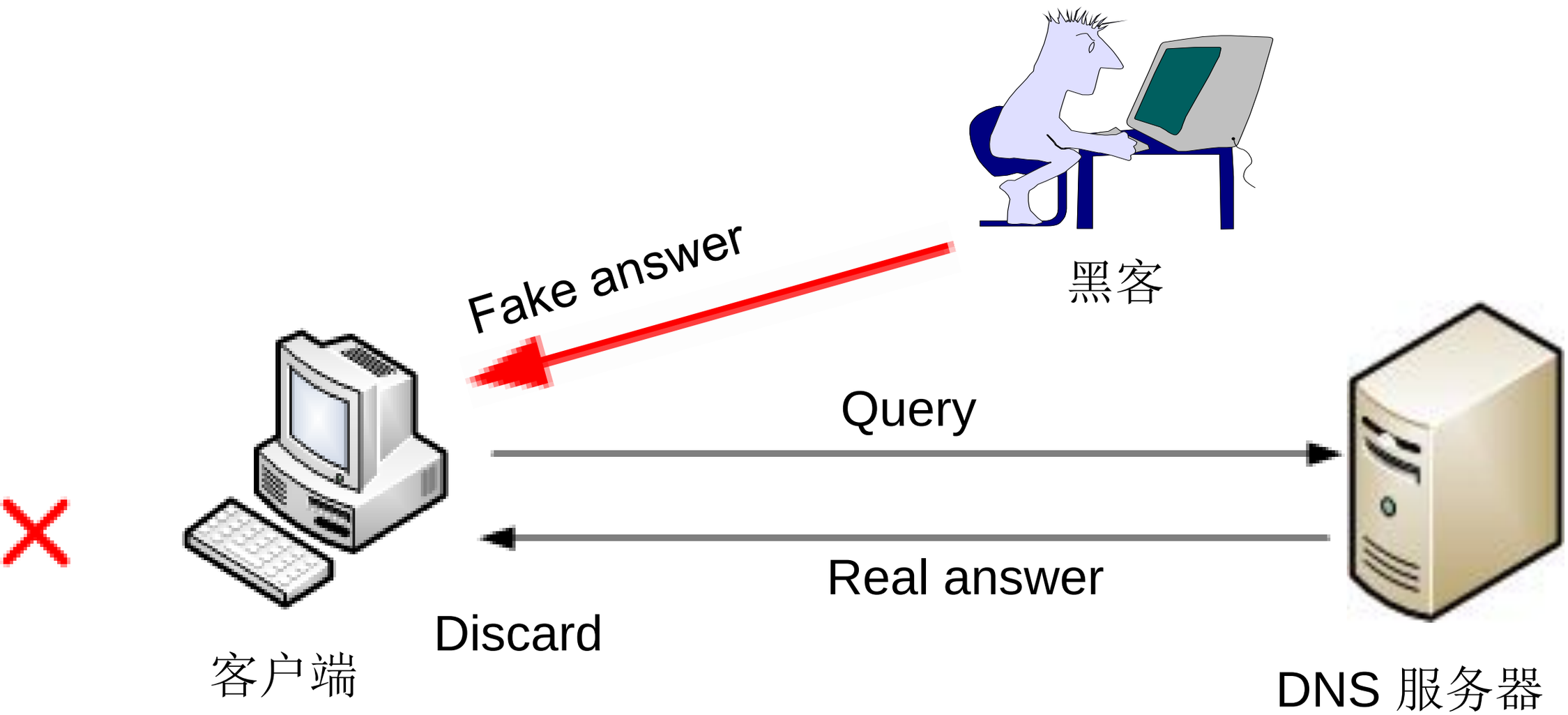
- DNS应答包被客户端接受需要满足以下五个条件
  - 1、应答包question域和请求包question域的域名信息一致。
  - 2、应答包的Transaction ID和请求包中的Transaction ID一致。
  - 3、应答包的源IP地址与请求包的目的IP地址一致。
  - 4、应答包的目的IP地址和端口与请求包的源IP地址和端口一致。
  - 5、第一个到达的符合以上四个条件的应答包。
- 从以上五个条件可以看出，最初设计DNS时没有考虑它的安全问题，这导致DNS协议存在很多漏洞，这使得DNS很容易受到攻击。

DNS安全威胁

- DNS的安全漏洞主要体现在以下三个方面。
  - （1）DNS报文只使用序列号来进行有效性鉴别，序列号由客户程序设置并由服务器返回结果，客户程序通过它来确定响应与查询是否匹配，这就引入了序列号攻击的危险。
  - （2）从协议定义上来看，在DNS应答报文中可以附加信息，该信息可以和所请求的信息没有直接关系，这样，攻击者就可以在应答中随意添加某些信息，如：指示某域的权威域名服务器的域名及IP，导致在被影响的域名服务器上查询该域的请求都会被转向攻击者所指定的域名服务器上去，从而对网络的完整性构成威胁。
  - （3）DNS的缓存机制，当一个客户端/DNS服务器，收到有关域名和IP的映射信息时，它会将该信息存放在缓存中，当再次遇到对此域名的查询请求时就直接使用缓存中的结果而无需重新查询。可以通过ipconfig /displaydns命令查看本地DNS缓存信息。

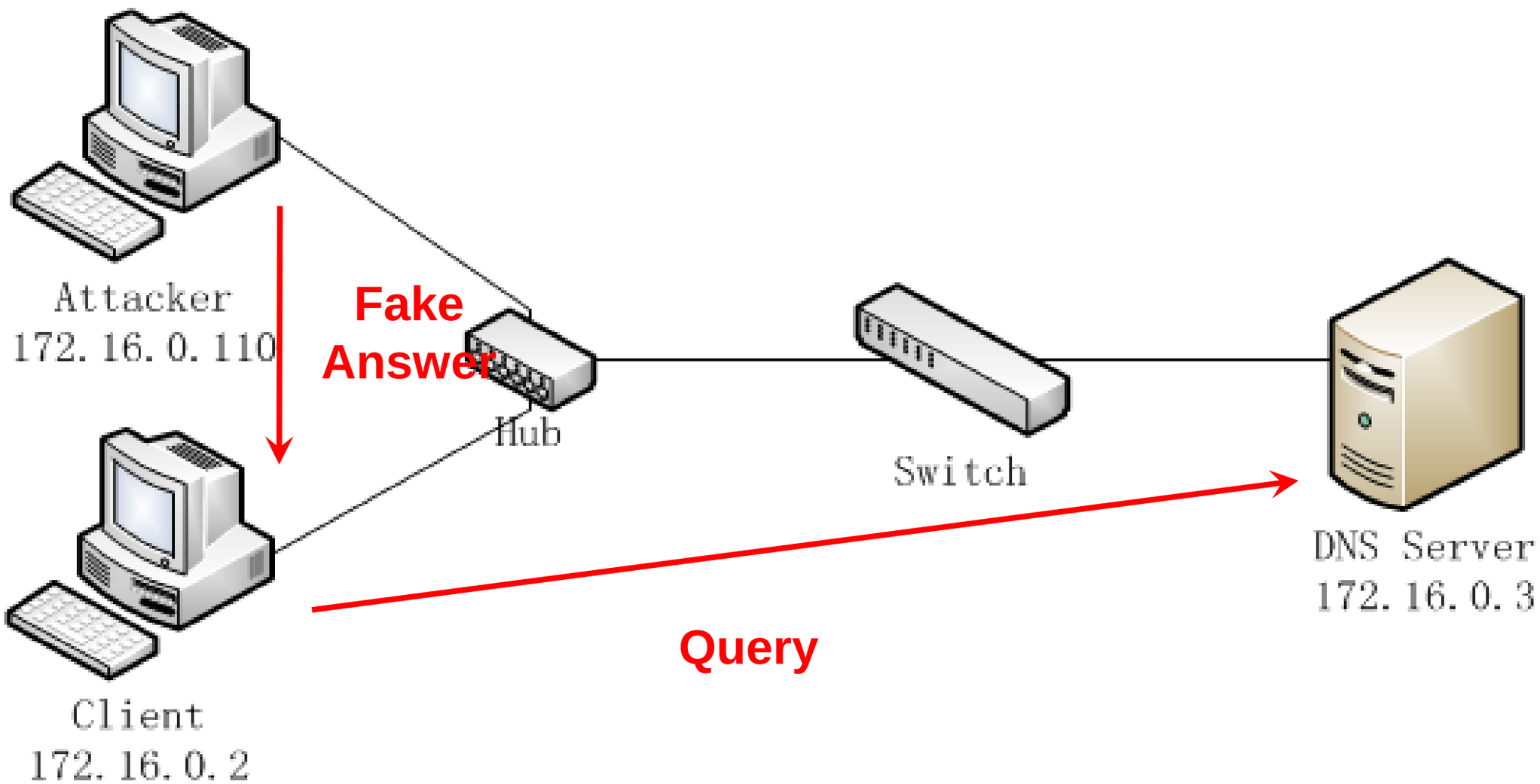
DNS安全威胁

- DNS欺骗攻击流程



DNS安全威胁

- 测试环境:攻击者可以监听到Client与Server之间的通信。



DNS安全威胁

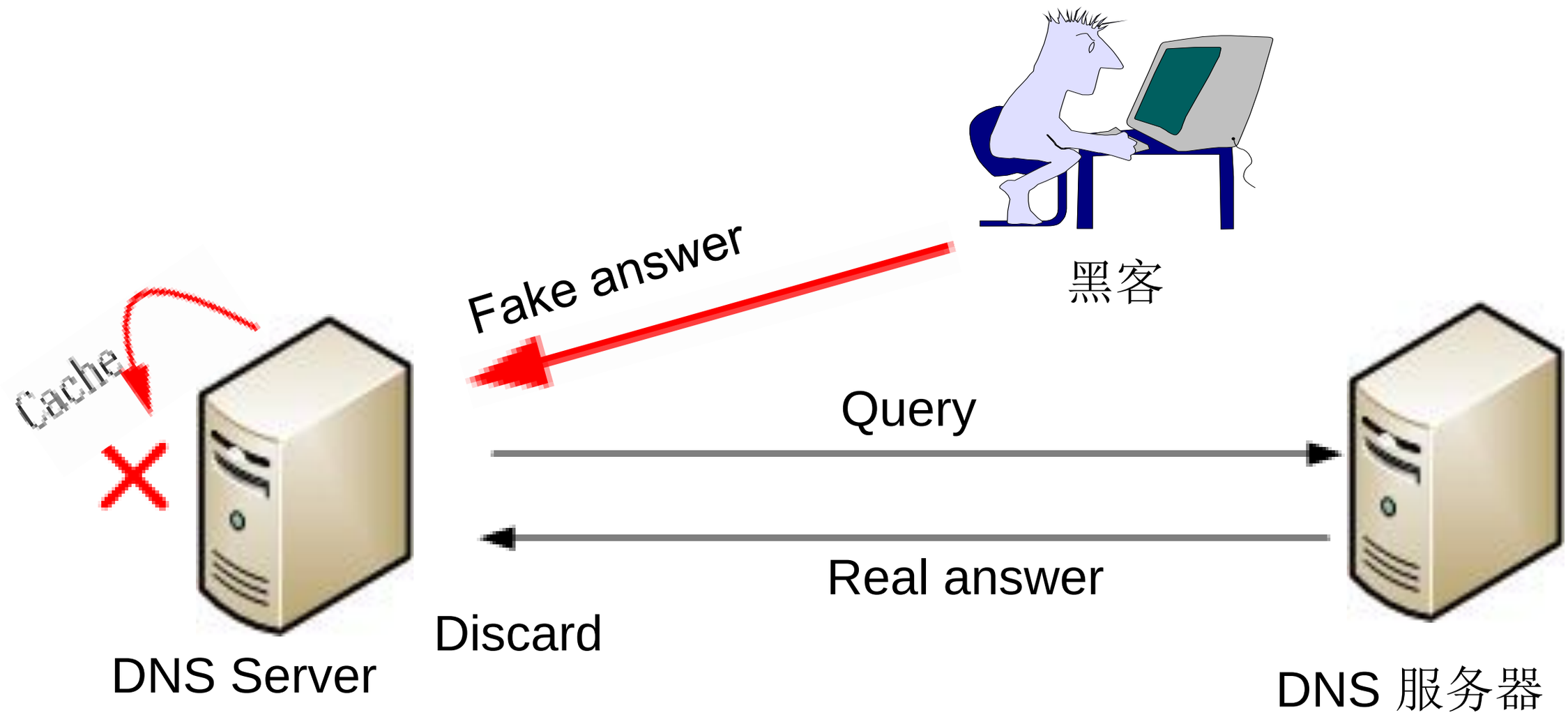
- 如下图所示第二个数据包是攻击者（172.16.0.110）伪装成（172.16.0.3）返回的虚假应答包，由于它是第一个到达的符合条件的数据包，所以会被（172.16.0.2）接受。当（172.16.0.2）通过域名hhz.242.net去访问主机时，会被错误的引导到（172.16.0.110）。
- 同样如果172.16.0.2访问银行或网上交易的网站时，攻击者也可以将其引导到错误的地址，通过虚假网页，进行一些不法行为，如盗取银行帐号及密码等信息。

No.	Time	Source	Destination	Protocol	Info
2	0.000300	172.16.0.2	172.16.0.3	DNS	Standard query A hhz.242.net
3	0.022569	172.16.0.3	172.16.0.2	DNS	Standard query response A 172.16.0.110
4	0.024043	172.16.0.3	172.16.0.2	DNS	Standard query response A 172.16.0.113

```
⊞ Frame 3 (144 bytes on wire, 144 bytes captured)
⊞ Ethernet II, Src: Vmware_f8:9e:14 (00:0c:29:f8:9e:14), Dst: LansTech_6f:32:35 (00:c0:26:6f:32:35)
⊞ Internet Protocol, Src: 172.16.0.3 (172.16.0.3), Dst: 172.16.0.2 (172.16.0.2)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 1031 (1031)
⊞ Domain Name System (response)
```

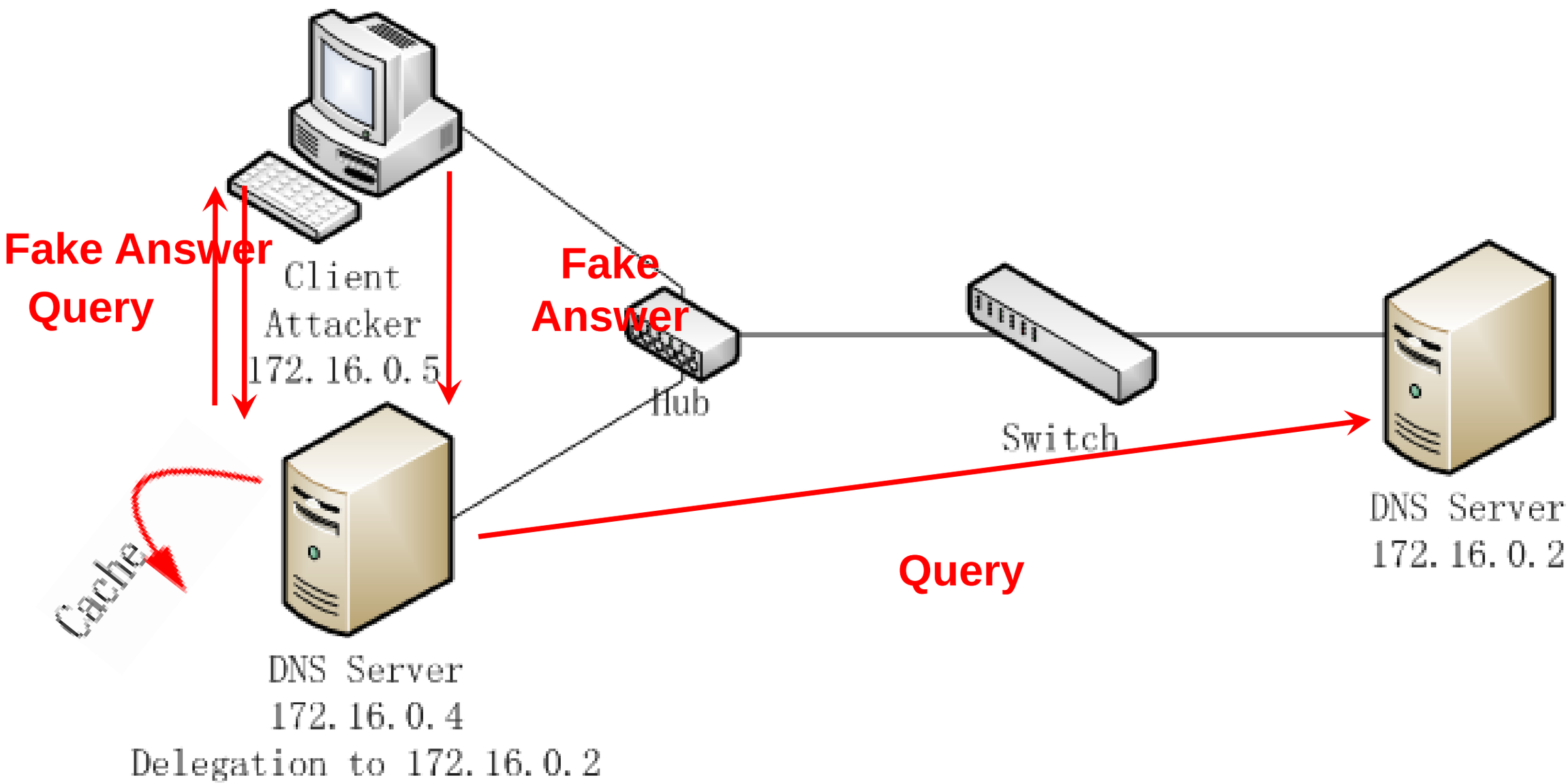
DNS安全威胁

- DNS下毒攻击流程



DNS安全威胁

- 测试环境：攻击者可以能够监听到DNS服务器之间的通信。



DNS安全威胁

- 下图中第三个数据包是攻击者（172.16.0.5）伪装成服务器（172.16.0.2）发送的应答包，这样就可以把虚假信息：1.242.com对应的IP地址为222.128.5.182放入服务器（172.16.0.4）的缓存中。

No.	Time	Source	Destination	Protocol	Info
64	35.880263	172.16.0.5	172.16.0.4	DNS	Standard query A 1.242.com
67	35.882126	172.16.0.4	172.16.0.2	DNS	Standard query A 1.242.com
68	35.905786	172.16.0.2	172.16.0.4	DNS	Standard query response A 222.128.5.182
69	35.907278	172.16.0.4	172.16.0.5	DNS	Standard query response A 222.128.5.182

```
⊞ Frame 69 (103 bytes on wire, 103 bytes captured)
⊞ Ethernet II, Src: 172.16.0.4 (00:0c:29:2c:0b:bb), Dst: 172.16.0.5 (00:0c:29:02:53:f8)
⊞ Internet Protocol, Src: 172.16.0.4 (172.16.0.4), Dst: 172.16.0.5 (172.16.0.5)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 35047 (35047)
⊟ Domain Name System (response)
    Transaction ID: 0x3cc8
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 0
  ⊞ Queries
  ⊟ Answers
    ⊟ 1.242.com: type A, class IN, addr 222.128.5.182
        Name: 1.242.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 15 minutes
        Data length: 4
        Addr: 222.128.5.182
```

DNS安全威胁

- 下毒结果验证：172.16.0.5再次向DNS服务器172.16.0.4查询1.242.com的信息，可以看到DNS服务器没有向172.16.0.2查询，而是直接给出了应答，这说明它的缓存中存在1.242.com的信息，通过抓包分析，下毒攻击是成功的。此类攻击时一般会将TTL值设成较长的时间。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.0.5	172.16.0.4	DNS	Standard query A 1.242.com
2	0.000548	172.16.0.4	172.16.0.5	DNS	Standard query response A 222.128.5.182
5	18.633558	172.16.0.5	172.16.0.4	DNS	Standard query A 1.242.com
6	18.634624	172.16.0.4	172.16.0.5	DNS	Standard query response A 222.128.5.182

```
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 35154 (35154)
⊟ Domain Name System (response)
    Transaction ID: 0xdba0
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 0
  ⊞ Queries
  ⊟ Answers
    ⊟ 1.242.com: type A, class IN, addr 222.128.5.182
        Name: 1.242.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 1 minute, 51 seconds
        Data length: 4
        Addr: 222.128.5.182
```

DNS安全威胁

- 缓冲区溢出攻击
  - BIND 软件的许多版本存在缓冲区溢出漏洞，当攻击者获取了管理员的权限时，就可以入侵BIND所在的主机，并可执行任意指令，这种攻击危害比较严重，攻击者不仅可以获得DNS服务器所在域的数据信息，还可以任意修改该域的数据。针对这种攻击需要及时发现BIND的版本漏洞，并进行升级。
  - 黑客利用DNS服务器软件存在的漏洞实施攻击，比如特定的输入没有进行严格检查，那么就有可能被攻击者利用，攻击者构造特定的畸形数据包来对DNS服务器进行缓冲区溢出攻击。

DNS安全威胁

- 缓冲区溢出攻击的危害主要包括：
  - 1、更改MX记录，造成邮件被截获、修改或删除。
  - 2、更改A记录，将www服务器的域名指向黑客具有的同样www内容的主机，诱使访问者登陆，获取访问者的密码等相关信息
  - 3、利用这台主机作为攻击其他机器的跳板

DNS安全威胁

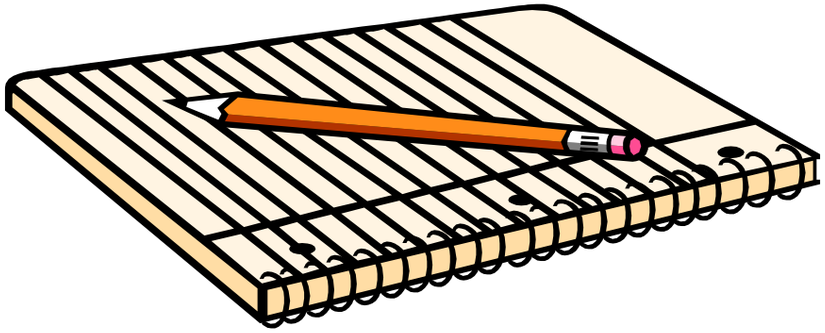
- 拒绝服务攻击
  - 黑客主要利用一些DNS软件的漏洞，如BIND 9版本（版本9.2.0以前的9系列）。如果向运行BIND的设备发送特定的DNS数据包请求，BIND就会自动关闭。攻击者只能是BIND停止提供域名解析服务而不能在服务器上执行任何口令。
  - 造成的危害是：域名无法解析为IP地址，用户无法访问互联网

DNS安全威胁

- 信息泄露
  - BIND软件默认设置是允许主机间进行区传送（ZoneTransfer）。区传送的主要目的是用于主DNS和辅DNS之间的数据同步，使辅DNS可以从主DNS获得新的数据信息。
  - 一旦启用区传送，而不做任何限制，很可能造成信息泄露，黑客可以获得整个授权域内的所有主机信息，判断主机功能及安全性，从中发现目标进行攻击。
  - 一旦这些信息泄露，攻击者就可以根据它推测出主域名服务器的网络结构，为进一步攻击提供参考依据。

DNS安全威胁及防范

- DNS概述
- DNS协议
- DNS工作流程
- DNS安全威胁
- DNS安全防范



DNS安全防范

- DNS攻击的防范：
  - 应对DNS服务器面临的安全隐患主要依据以下两个准则：
    - 选择安全的没有缺陷的BIND版本
    - DNS服务器配置正确可靠

DNS安全防范

- BIND主要有三个版本
  - 1、BIND 4，1998年多数操作系统捆绑的是BIND4，但是现在已经被多数厂商抛弃。
  - 2、BIND 8是曾经使用最广的版本，现在网络中的一部分DNS服务器仍在使用。
  - 3、BIND 9最新版本，全部重新写过，免费（由商业公司资助），BIND9在2000年10份推出。

Blogs | Contact | Donate | Shop | Customer Login

ISC Internet Systems Consortium

DOWNLOADS | Open Source | Support | Community | F Root | About Us

BIND

Versatile, Classic, Complete Name Server Software

Join a Mailing List ›

Report a bug ›

Inquire about BIND Support

- BIND Features
- BIND Significant Features Matrix
- New features in BIND 9.11
- BIND Users Nabble Forum
- BIND Users List Archive
- BIND Issues List
- Test your EDNS compliance
- Dig app for Apple iOS
- Secure DNS Deployment Guide (NIST publication, September, 2013)

BIND is open source software that enables you to publish your Domain Name System (DNS) information on the Internet, and to resolve DNS queries for your users. The name BIND stands for "Berkeley Internet Name Domain", because the software originated in the early 1980s at the University of California at Berkeley.

BIND is by far the most widely used DNS software on the Internet, providing a robust and stable platform on top of which organizations can build distributed computing systems with the knowledge that those systems are fully compliant with published DNS standards.

BIND and DNS

BIND implements the DNS protocols. The DNS protocols are part of the core Internet standards. They specify the process by which one computer can find another computer on the basis of its name. The BIND software distribution contains all of the software necessary for asking and answering name service questions.

The BIND software distribution has three parts:

1. Domain Name Resolver

A **resolver** is a program that resolves questions about names by sending those questions to appropriate servers and responding appropriately to the servers' replies. In the most common application, a web browser uses a local stub resolver library on the same

Featured Downloads

Download "BIND 9.10.6"
bind-9.10.6.tar.gz – Downloaded 65645 times – 9 MB

Download "BIND 9.11.2"
bind-9.11.2.tar.gz – Downloaded 13867 times – 9 MB

Download "BIND 9.9.11"
bind-9.9.11.tar.gz – Downloaded 4223 times – 8 MB

DNS安全防范

- BIND安全配置
  - 1、隔离DNS服务器

    DNS服务器上不应该再运行其他服务，尤其是允许普通用户登录，减小攻击者利用其他服务漏洞攻击DNS服务器的概率。

  - 2、为BIND创建chroot

    chroot是指更改某个进程所能看到的根目录，即将某进程限制在指定的目录中，保证该进程只能对该目录及其子目录有所动作，从而保证整个服务器的安全。BIND9.x系列版本简化了chroot的创建步骤。

DNS安全防范

- BIND安全配置
  - 3、隐藏BIND版本号，通过发送特殊的DNS查询包，DNS服务器会返回DNS的版本信息。如下图所示返回版本为9.2.4。

No.	Time	Source	Destination	Protocol	Info
73	70.380002	192.168.1.110	128.255.64.3	DNS	Standard query TXT version.bind
74	70.888402	128.255.64.3	192.168.1.110	DNS	Standard query response TXT

```
⊞ Frame 74 (104 bytes on wire, 104 bytes captured)
⊞ Ethernet II, Src: 00:1d:0f:54:fe:4c (00:1d:0f:54:fe:4c), Dst: LansTech_6f:26:57 (00:c0:26:6f:26:57)
⊞ Internet Protocol, Src: 128.255.64.3 (128.255.64.3), Dst: 192.168.1.110 (192.168.1.110)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 32770 (32770)
⊟ Domain Name System (response)
    Transaction ID: 0x7777
  ⊞ Flags: 0x8500 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 0
  ⊞ Queries
  ⊟ Answers
    ⊟ version.bind: type TXT, class CH
        Name: version.bind
        Type: TXT (Text strings)
        Class: CH (0x0003)
        Time to live: 0 time
        Data length: 6
        Text: 9.2.4
  ⊞ Authoritative nameservers
```

DNS安全防范

- 通常软件的Bug信息是和特定版本相关的，因此版本号是黑客寻求的最有价值的信息。黑客获得版本号，就可以知道这个软件存在了哪里漏洞。隐藏BIND版本配置比较简单，只需修改配置文件/etc/name.conf，在options部分添加version声明，将BIND版本号信息覆盖。如下所示，当有人请求BIND版本信息时，返回内容将是“I will not tell you”。

```
options{
  version  “I will not tell you”;
};
```

DNS安全防范

- BIND安全配置

  - 4、请求限制

    DNS服务器响应任何人的任何请求这是不能接受的。限制DNS服务器的服务范围很重要，可以把许多入侵者拒之门外。修改BIND的配置文件/etc/named.conf,添加相应内容即可。

  - 5、限制区传送

    默认情况下BIND的区传送是全部开放的，如果没有限制，DNS服务器允许任何人进行区传送，那么网络架构中的主机名、主机ip地址表、路由器名及路由IP表，甚至包括各主机所在的位置和硬件配置信息等情况很容易被入侵者得到。因此需要对区传送进行必要的限制。

DNS安全防范

- BIND安全配置

  - 6、关闭动态更新

最早设计DNS时，所有运行TCP/IP的计算机都是手工配置的。用特定的IP地址手工配置一台计算机时，它的A记录、PTR记录也要手工配置。随着DHCP的出现，IP地址动态分配，使手工更新A记录、PTR记录变得很难管理。

因此，在RFC2136中提出DNS动态更新，使得DNS客户端ip地址或名称出现更改时，可以利用DNS服务器注册和动态更新其资源记录。虽然DNS动态更新规定了怎样的系统才允许更新一台DNS服务器中的记录，但是DNS仍然可能受到威胁，比如攻击者利用IP欺骗，伪装成DNS服务器信任的主机对系统进行更新 或者损害，删减、增加、修改资源记录。

DNS安全防范

- DNS其他加固措施
  - 事务签名（TSIG）技术
  - DNSSEC
  - 配置DNS Flood Detector

DNS安全防范

- 事务签名（TSIG）技术
- DNS事务签名分为TSIG（Transaction Signature）与SIG0（SIGnature）。用户可以根据客户端与服务器端的信任关系选择TSIG或SIG0。对称式TSIG只有一组客户端和服务器端共享密码；非对称式SIG0，采用非对称密码算法，既有公钥又有私钥。如果客户端和服务器端是完全信任的，可以采用TSIG，若是非完全信任，应采用SIG0。采用事务签名主要目的是防止黑客利用IP欺骗对DNS服务器进行攻击，迫使其进行非法区传送。

DNS安全防范

- DNSSEC
  - DNS欺骗是对目前网络应用的最大冲击，攻击者伪装成服务器提供假的域名和IP地址对应信息，将用户引导到错误的网站、或电子邮件丢失。
  - 目前较新的BIND版本针对这一问题已经加入了许多改进方法：如发包源端口和事务ID的随机化。不过真正的解决方案，则有赖于数据包认证机制的建立和推广。
  - DNSSEC就是试图解决这一类问题，BIND9已经加以设计和完成。DNSSEC引入了两个全新的资源记录类型：KEY和SIG，它们允许客户端和域名服务器对任何DNS数据的来源进行验证。

DNS安全防范

- DNSSEC主要依靠公钥技术对包含在DNS中的信息创建密码签名。密码签名通过计算一个哈希值来提供DNS中数据的完整性，并将该哈希值封装进行保护。私钥用来封装哈希值，公钥把哈希值解密出来，通过解密出的哈希值就可以判断数据的完整性。

- 当然DNSSEC也有一些缺点：产生和校验签名需要占用很多的CPU时间，这些额外开销会影响服务器的性能；签名后的数据量很大，加重了互联网的负担。

DNS安全防范

- DNS Flood Detector
- DNS Flood Detector是针对DNS服务器的SYN Flood攻击的检测工具，用于侦测恶意的使用DNS的查询功能。它会监控向服务器查询名称解析的数量，分成守护进程（daemon）和后台（bindsnap）模式。守护进程模式会发出警示（/var/log/message)。Bindsnap模式可以得到接近实时的查询状态。

DNS over TLS

- RFC 7858,8310
- 端口： 853
- DoT 就是基于 TLS 隧道之上的域名协议，由于 TLS 本身已经实现了保密性与完整性，因此 DoT 自然也就具有这两项特性。DoT通过TLS协议及SSL/TLS证书（如:沃通SSL证书）实现安全加密和身份验证，实现保密性和完整性。
- 使用TCP作为基本的连接协议

DNS over HTTPS

- DoH :defines a protocol for sending DNS queries and getting DNS responses over HTTPS. Each DNS query-response pair is mapped into an HTTP exchange.
- 使用HTTPS和HTTP/2进行连接
- RFC8484
- 端口443

问题和讨论