华东师范大学计算机科学技术系上机实践报告

课程名称：计算机网络	**年级**：2022	**上机实践成绩**：
指导教师：洪道诚	**姓名**：朱宇笑	**创新实践成绩**：
实验名称：域名系统（DNS）	**学号**：10225001410	**上机实践日期**：2023.11.10
座位编号：F	**组号**：6	**上机实践时间**：2 学时

一、 实验目的

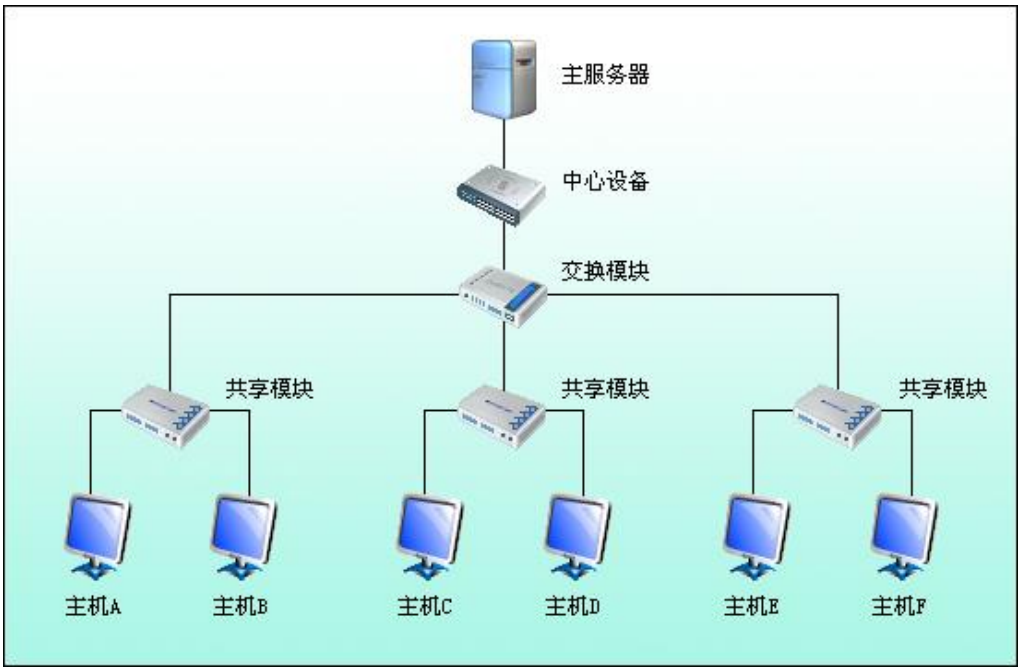
1. 掌握DNS的报文格式
2. 掌握DNS的工作原理
3. 掌握DNS域名空间的分类
4. 理解DNS高速缓存的作用

二、 实验设备

1. PC机
2. 仿真编辑器和协议分析器

三、 实验原理

实验采用网络结构一



（一） 域名空间

在域名空间中，名字被定义在一个根在顶部的树型结构中。这个树结构最多有128 层：第 0 层为根，如下图所示：

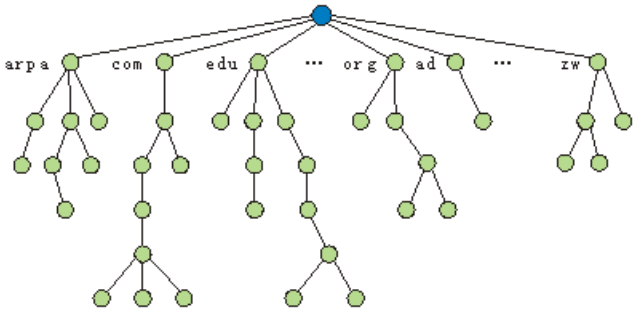


图 2-8 域名空间

1. 标号

树上的每一个节点都有一个标号，标号是一个最多有 63 个字符的字符串。根节点的标号是空字符串。每一个节点的子节点都具有不同的标号，这样就保证了域名是惟一的。

2. 域名

一个完全的域名是用点“.”分隔开的标号序列。域名总是从节点标号向上读到根节点标号的。因为最后一个标号是根节点的标号，所以一个完全的域名总是以空标号结束。因为空字符串表示什么也没有，所以域名的最后一个字符是一个点。下图给出了一个域名示例。

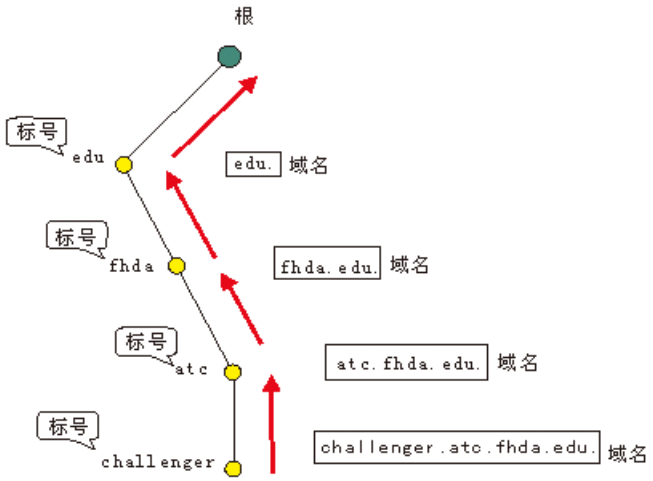


图 2-9 域名和标号

(1)完整域名

若域名以空字符串结束，那么这个域名就叫做完整域名（FQDN）。完整域名是包括主机全名的域名。它包括从最具体的到最一般的所有标号，并惟一地定义了该主机的名字。例如，域名：challenger.atc.fhda.edu 是名为 challenger 的计算机的完整域名。

(2)不完整域名

若一个域名不是以空字符串结束，则它就叫做不完整域名（PQDN）。不完整域名从一个节点开始，它没有到达根节点。它适用于这样一种情况：当要被解析的域名和客户属于同一个场所时，解析程序可以自动加上缺少的部分，以便创建完整域名。例如，如果在场所 atc.fhda.edu 上的用户想得到计算机 challenger 的 IP 地址，用户就可以定义一个不完整域名：challenger。DNS 客户在把地址传递给 DNS 服务器之前，会加上后缀 atc.fhda.edu。

3. 域

域（domain）是域名空间中的子树。域的名字就是这个子树顶部节点的域名。下图给出了一些域。域本身又可划分为若干个域（有时也称它们为子域）。

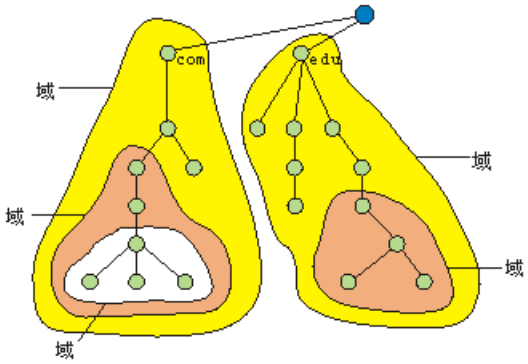


图 2-10 域

（二） DNS 协议简介

DNS（域名服务）是一种能够完成从域名到地址或从地址到域名的映射系统。使用 DNS，计算机用户可以间接的通过域名来完成通信。Internet 中的 DNS 被设计成为一个联机分布式数据库系统，采用客户/服务器方式工作。分布式的结构使 DNS 具有很强的容错性。

（三） DNS 的域名分类

在 Internet 中，域名空间被划分为 3 个部分：类属域、国家域和反向域，如下图所示：

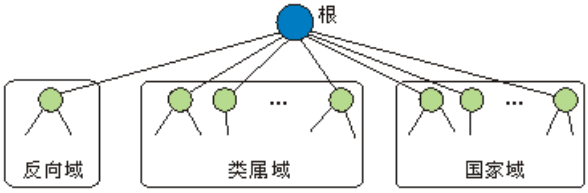


图 2-11Internet 中使用的 DNS

1. 类属域

类属域按照主机的类属行为分类。树中的每一个节点定义一个域，它是到域名空间数据库的一个索引，如下图所示：

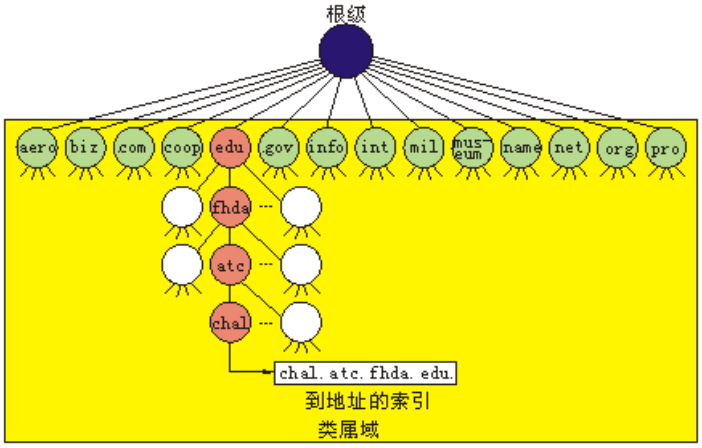


图 2-12 类属域

在类属域的第一级允许有 14 个标号。这些标号描述了不同的机构类型，如下表所示：

表 2-1 第一级类属域

标号	说明	标号	说明
Aero	航空和航天公司	int	国际机构
Biz	企业或商行（与“com”相似）	mil	军事机构

标号	说明	标号	说明
Com	商业机构	museum	博物馆和其它非盈利组织
Coop	协作的企业组织	name	人名字（个人的）
Edu	教育机构	net	网络支持中心
Gov	政府机构	org	非盈利机构
Info	信息服务提供者	pro	专业个体组织

2. 国家域

国家域使用两字符的国家或地区的缩写（例如，用 cn 代表中国）。第二级标号可以是机构的标号，或者是国家指定的标号。

3. 反向域

反向域用来把一个地址映射为域名。例如，有时服务器会收到来自客户的请求，要完成一个任务。但是服务器不能确定这个客户是否在授权的客户列表中，因为只有客户的 IP 地址（从收到的 IP 数据包中提取出来的）被列出。要确定这个客户是否在授权列表中，服务器可以使用它的解析程序向 DNS 发送查询，并请求把地址映射为名字。这种类型的查询叫做反向查询或指针（PTR）查询。要处理反向查询，在域名空间中要增加反向域，且其第一级节点叫做 arpa（由于历史原因）。第二级节点叫做 in-addr（表示反向地址）。域的其余部分为 IP 地址。

处理反向域的服务器也是分级的。这就表示地址的网络号部分要比子网号部分的等级高，而子网号部分要比主机号部分的等级高。在与类属域和国家域相比较时，反向域看起来是反过来的，如 132.34.45.121 的 IP 地址在读出时应为 121.45.34.132.in-addr.arpa。下图是反向域配置的说明。

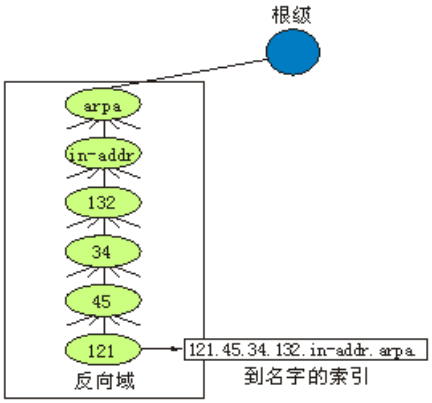


图 2-13 反向域

（四） DNS 报文格式

DNS 报文由 12 字节长的首部和 4 个长度可变的字段组成，如下图所示：

标识（16 位）	标志（16 位）
问题记录数（16 位）	应答记录数（16 位）
授权记录数（16 位）	附加记录数（16 位）
查询问题	
回答（资源记录数可变）	
授权（资源记录数可变）	
额外信息（资源记录数可变）	

图 2-14DNS 报文格式

(1)标识：该字段占两个字节，由客户程序设置并由服务器返回。客户程序通过它来确定响应与查询是否匹配。

(2)标志：16 位的标志字段被划分为若干子字段，如下图所示：

QR	Opcode	AA	TC	RD	RA	保留	AD	CD	rcode
1 位	4 位	1 位	1 位	1 位	1 位	1 位	1 位	1 位	4 位

图 2-15DNS 标志字段

标志字段的各子字段含义如下：

●QR（查询/响应）：该位为 0 时是查询报文；为 1 时是响应报文。

●Opcode：该位为 0 时是标准查询；为 1 时是反向查询；为 2 时是服务器状态请求。

●AA（授权回答）：这是 1 位字段。当它设置为 1 时，表示名字服务器是权限服务器。它只用在响应报文中有效。

●TC（截断的）：该位只在响应报文中有效，它表示响应报文被切割，因为响应报文过大而无法适用于数据包的数据部分。例如，如果响应包含大量名称服务器，数据包可能会超过允许的 MTU。这时，数据包将被切割，并且将 TC 域位设置为 1。

●RD（要求递归）：如果目标名称服务器不包含所请求的信息，该域表示客户端请求递归查询。

●RA（递归可用）：该域在响应中有效，它表示响应名称服务器是否提供递归查询。

●AD（可信数据）：这位用来指定所有的数据已经被服务器认证。

●CD（验证无效）：这位指定了没有被认证的数据对于询问者来说是可以接受的。

●Rcode：该域长度为 4 位，用于 DNS 响应中，表示是否出现错误。

(3)问题记录数：该字段占两个字节，查询问题部分包含的条目数量。

(4)应答记录数：该字段占两个字节，表示回答部分包含的回答记录数。在查询报文中它的值是 0。

(5)授权记录数：该字段占两个字节，包含在响应报文的授权部分的授权记录数。在查询报文中它的值是 0。

(6)附加记录数：该字段占两个字节，包含在响应报文的附加部分的附加记录数。在查询报文中它的值是 0。

(7)查询问题：DNS 查询或响应报文中会有查询部分。查询部分中每个问题的格式如下图所示：

查询名	
查询类型	查询类

图 2-16DNS 查询问题字段

●查询名：表示要查找的名字，它是一个或多个标识符序列。

●查询类型：表示查询问题时的类型。最常用的查询类型是 A 类型，表示期望获得查询名的 IP 地址；而一个 PTR 查询则请求获得一个 IP 地址对应的域名。

●查询类：表示查询的类别。其值通常是 1，表示 Internet 类型。

(8)回答（资源记录数可变）：DNS 响应报文中会有回答部分。回答部分包括从服务器到客户（解析程序）的回答。其资源记录的格式如下图所示：

域名	
类型	类
生存时间	
资源数据长度	资源数据

图 2-17DNS 回答字段

●域名：表示记录中资源数据对应的名字。它的格式和查询名字字段格式相同。

●类型：表示资源记录的类型。它的值和查询类型的值是一样的。

●类：表示资源记录的类别。它的值和查询类的值是一样的。

●生存时间：表示客户程序保留该资源记录的秒数。

●资源数据长度：表示资源数据的数量。该数据的格式依赖于类型字段的值。

●资源数据：表示该资源数据的内容。

(9)授权（资源记录数可变）：DNS 响应报文中会有授权部分。授权部分为该查询给出关于一个或多个授权服务器的信息（域名）。其资源记录的格式如下图所示：

域名	
类型	类
生存时间	
资源数据长度	资源数据

图 2-18DNS 授权字段

●域名：表示记录中资源数据对应的名字。它的格式和查询名字字段格式相同。
●类型：表示资源记录的类型。它的值和查询类型的值是一样的。
●类：表示资源记录的类别。它的值和查询类的值是一样的
●生存时间：表示客户程序保留该资源记录的秒数。
●资源数据长度：表示资源数据的数量。该数据的格式依赖于类型字段的值
●资源数据：表示该资源数据的内容。

(10)额外信息（资源记录数可变）：DNS 响应报文中会有额外信息部分。额外信息部分提供有助于解析程序的附加信息。其资源记录格式如下图所示：

域名	
类型	类
生存时间	
资源数据长度	资源数据

图 2-19DNS 额外信息字段

●域名：表示记录中资源数据对应的名字。它的格式和查询名字段格式相同。
●类型：表示资源记录的类型。它的值和查询类型的值是一样的。
●类：表示资源记录的类别。它的值和查询类的值是一样的。
●生存时间：表示客户程序保留该资源记录的秒数。
●资源数据长度：表示资源数据的数量。该数据的格式依赖于类型字段的值。
●资源数据：表示该资源数据的内容。

（五） 正向解析与反向解析

1. 解析程序

DNS 解析程序是客户/服务器模式的应用程序。需要把地址映射为域名或把域名映射为地址的主机要调用 DNS 解析程序。解析程序用映射请求找到最近的 DNS 服务器。若 DNS 服务器有这个信息，则满足解析程序的要求；否则，或者让解析程序找其它的服务器，或者再请其它服务器提供这个信息。

当解析程序收到响应后，就解释这个响应，看它是正确的解析还是错误的解析，最后把解析结果交给请求映射的进程。

2. 正向解析

通常，解析程序把域名交给服务器，请求服务器给出相应的地址，服务器检查类属域或国家域并查找映射。

如果需要查询的域名是类属域名或国家域名，解析程序就把这个需要查询的域名发送到本地 DNS 服务器进行解析。若本地服务器不能解析这个域名，它就让解析程序再找其它的 DNS 服务器，或者直接询问其它 DNS 服务器。

3. 反向解析

有时客户会要求将 IP 地址映射到相应的域名，客户把 IP 地址发送到 DNS 服务器并请求服务器映射出相应的域名，这种查询叫做反向解析，也叫做 PTR 查询。要回答这类查询，DNS 使用反向域。在请求中，IP 地址需要反过来，同时还要附上两个标号 in-addr 和

arpa，以创建可以被反向域部分所接受的域。例如，若解析程序收到的 IP 地址是 132.34.45.121，解析程序首先把地址反过来，并在发送前加上两个标号。发送出的域名是“121.45.34.132.in-addr.arpa”，它由 DNS 服务器接受和解析。

（六） 递归解析与迭代解析

1. 递归解析

客户（解析程序）可以向域名服务器请求递归回答。这就表示解析程序期望服务器提供最终解答。若服务器是这个域名的权限服务器，就检查它的数据库并作出响应。若服务器不是权限服务器，它就将请求发送给另一个服务器（通常是父服务器）并等待响应。若父服务器是权限服务器，则响应；否则，就将查询再发送给另一个服务器。当查询最终被解析时，响应就返回，直到最后到达发出请求的客户。下图给出了这个过程。

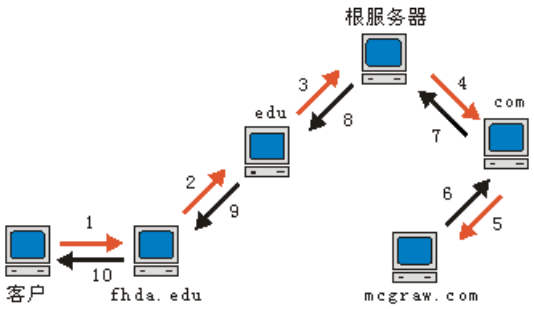


图 2-20 递归解析

2. 迭代解析

客户(解析程序)可以向域名服务器请求迭代回答。若服务器是这个域名的权限服务器，它就发送解答。若不是，就返回它认为可以解析这个查询的服务器的 IP 地址。客户就向第二个服务器重复查询。若新找到的服务器能够解决这个问题，就回答这个查询；否则，就向客户返回一个新的服务器的 IP 地址。现在客户必须向第三个服务器重复查询。这个过程称为迭代，客户向多个服务器重复发送同样的查询。在下图中，客户在从 mcgraw.com 服务器获得解答之前，查询了 4 个服务器。

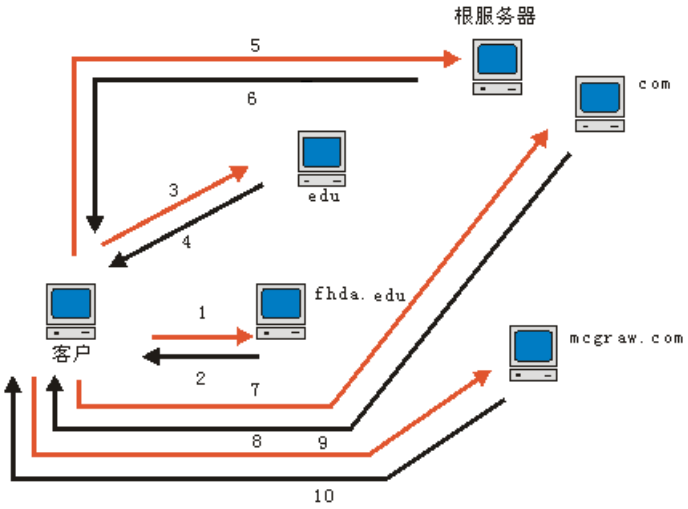


图 2-21 迭代解析

（七） 高速缓存

如果 DNS 服务器收到的需要解析的域名不在它的域中，它就会以递归的或迭代的解析方式请求父服务器。为提高效率，DNS 使用高速缓存机制。当服务器向另一个服务器请求映射并收到它的响应时，在把响应发送给客户之前，DNS 服务器先将这个响应存储在它的高速缓存中。若另一个客户请求同样的映射，它就检查高速缓存并解

析这个域名。这时，DNS 服务器把响应标记为未授权的，用来通知客户这个响应是来自高速缓存而不是来自一个授权的 DNS 服务器。这种高速缓存技术加速了解析过程。

地址与域名的映射关系是会发生变化的，如果 DNS 服务器将一个映射长期保存在高速缓存中，这个映射可能会过期，它可能把过期的映射发送给客户。目前有两种方法解决这个问题。第一种方法是权限服务器把生存时间（TTL）信息添加在映射上，生存时间定义了接收映射的服务器可以在高速缓存中保存本条映射的时间（以秒为单位）。经过这段时间后，这个映射就变成为无效的。第二种方法是 DNS 服务器对每一个高速缓存的映射保留一个 TTL 计数器。当 TTL 计数器到期时就清除这条映射。

（八） 压缩

当域名重复出现时，DNS 就需要用偏移指针来替换。例如，在资源记录中，域名通常是问题记录的域名的重复。为了避免发生这样的重复，DNS 定义了 2 字节的偏移指针，它指向前一次出现的该域或该域的一部分。这个指针的格式如下图所示：

11	开始字节的地址
2 位	14 位

图 2-22 偏移指针

例如，解析程序向本地服务器发送查询报文，要找出主机“chal.fhda.edu”的 IP 地址。这里将分开讨论查询报文和响应报文。

下图给出了解析程序发送出的查询报文。前两个字节是标识符（0x1333），它使响应报文与查询报文关联起来。因为解析程序可以向同一个 DNS 服务器发送多个查询，标识符有助于将不同的响应与查询对应起来。下一个字节是标志，其值为 0x0100。查询报文如下图所示：

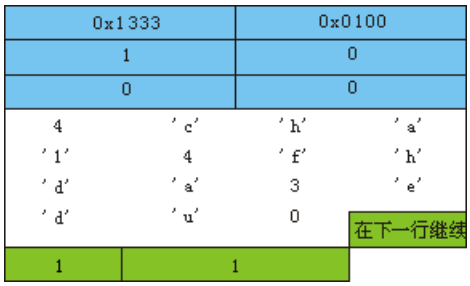


图 2-23 查询报文

QR 位定义报文是查询报文。OpCode 是 0000，表示是标准查询。这个报文只包含一个问题记录。域名是 4chal4fhda3edu0。下一个 2 字节定义查询类型是 IP 地址；最后两个字节定义类是 Internet。

下图给出了服务器的响应报文。

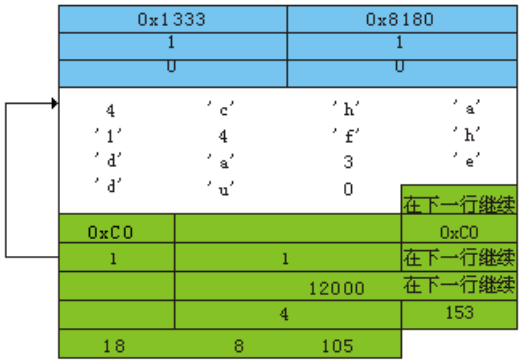


图 2-24 响应报文

除了标志不同的回答记录数是 1，标志的值是 0x8180 以外，响应报文与查询报文相似。标志的值是 0x8180，用二进制表示是 1000000110000000，把它划分为以下的几个字段：

QR	Opcode	AA	TC	RD	RA	保留	AD	CD	rcode
1	0000	0	0	1	1	0	0	0	0000

图 2-25 响应报文的标志字段

QR 位定义报文是响应。OpCode 是 0000，它表示是标准的查询。递归可用（RA）和 RD 位的值设置为 1。报文只包含一个问题记录和一个回答记录。问题记录是与查询报文一致的。回答记录有一个指针 0xC00C（分成两行），它指向问题记录而不是重复这个域名。下一个字段定义域的类型（地址）。再下面一个字段定义类（Internet）。值为 12000 的字段是 TTL（12000s）。再下面的字段是资源数据长度字段，资源数据是 IP 地址（153.18.8.105）。

（九） DNS 封装

DNS 可以使用 UDP 封装，也可以使用 TCP 封装。服务器使用的是熟知端口号 53。当响应报文的长度小于 512 字节时就使用 UDP，因为大多数 UDP 封装受 512 字节的数据包长度限制。若响应报文的长度超过 512 字节，就要使用 TCP 封装。

若解析程序事先知道响应报文的长度超过 512 字节，就要使用 TCP 封装。例如，若次名字服务器（作为客户）需要主服务器传送数据，它就必须使用 TCP 连接，因为要传送的信息的长度通常是超过 512 字节的。

若解析程序不知道响应报文的长度，它可以使用 UDP 封装。若响应报文的长度超过 512 字节，服务器就截断这个报文，并把 TC 位置 1。解析程序之后就打开 TCP 连接，并重复这个请求，以便从服务器得到完整的响应。

四、 实验步骤

练习 1 Internet 域名空间的分类

各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。

本练习一人一组，现仅以主机 A 为例，其它主机的操作参考主机 A。

「说明」本实验要求主机能上广域网。

1. 类属域

将主机 A 的“首选 DNS 服务器”设置为公网 DNS 服务器，目的是能够访问 Internet。

(1)主机 A 启动协议分析器开始捕获数据并设置过滤条件（提取 DNS 协议）。

(2)主机 A 在命令行下运行“nslookup www.python.org”命令，如下图所示。

```
PS C:\Users\zyx99> nslookup www.python.org
服务器:  UnKnown
Address:  fe80::1

非权威应答:
名称:    dualstack.python.map.fastly.net
Addresses:  2a04:4e42:8c::223
          146.75.112.223
Aliases:  www.python.org
```

(3)主机 A 停止捕获数据。分析主机 B 捕获到的数据及主机 A 命令行返回的结果，回答以下问题：

● “www.python.org”对应的 IP 地址是什么？

回答：146.75.112.223。

● “www.python.org”域名的顶级域名的含义是什么？

回答：.org 域名是互联网的通用顶级域之一，英文全称“organization”，意思为“组织”，

适用于各类型组织机构，包括非盈利团体，是组织机构的首选。

2. 国家域

(1)主机 A 启动协议分析器开始捕获数据并设置过滤条件（提取 DNS 协议）。

(2)主机 A 在命令行下运行“nslookup www.jl.gov.cn”命令，如下图所示。

```
PS C:\Users\zyx99> nslookup www.jl.gov.cn
服务器:  UnKnown
Address:  fe80::1

非权威应答:
名称:    451e4e8b7e80208a.qaxcloudwaf.com
Addresses:  2409:8c20:9c73:11e::10c
          223.111.128.84
Aliases:  www.jl.gov.cn
```

(3)主机 A 停止捕获数据。分析主机 B 捕获到的数据及主机 A 命令行返回的结果，回答以下问题：

● “www.jl.gov.cn”对应的 IP 地址是什么？

回答：223.111.128.84。

● “www.jl.gov.cn”域名的顶级、二级、三级域名的含义是什么？

回答：顶级域名.cn 为国家域，是”China”的缩写，代表中国；二级域名.gov.cn 是”government”的缩写，是政府机构的专用域名；三级域名.jl 代表吉林省。

3. 反向域

(1)将主机 A 的“首选 DNS 服务器”设置为服务器的 IP 地址（默认为 172.16.0.253）。

(2)主机 A 启动协议分析器开始捕获数据并设置过滤条件（提取 DNS 协议）。

(3)主机 A 在命令行下运行“nslookup 172.16.0.253”命令。

(4)主机 A 停止捕获数据。分析主机 A 捕获到的数据及主机 A 命令行返回的结果，回答以下问题：

●172.16.0.253 对应的域名是什么？

回答：JServer.NetLab

●反向域的顶级、二级域名分别是什么？

回答：顶级域名：.NetLab；二级域名：.JServer。

练习 2　DNS 正向查询

本练习一人一组，现仅以主机 A 为例，其它主机的操作参考主机 A。

「说明」

本练习中要求每台主机配置 DNS 服务器，（DNS 服务器的 IP 地址即服务器的 IP 地址）其 IP 地址以 172.16.0.253 为例。

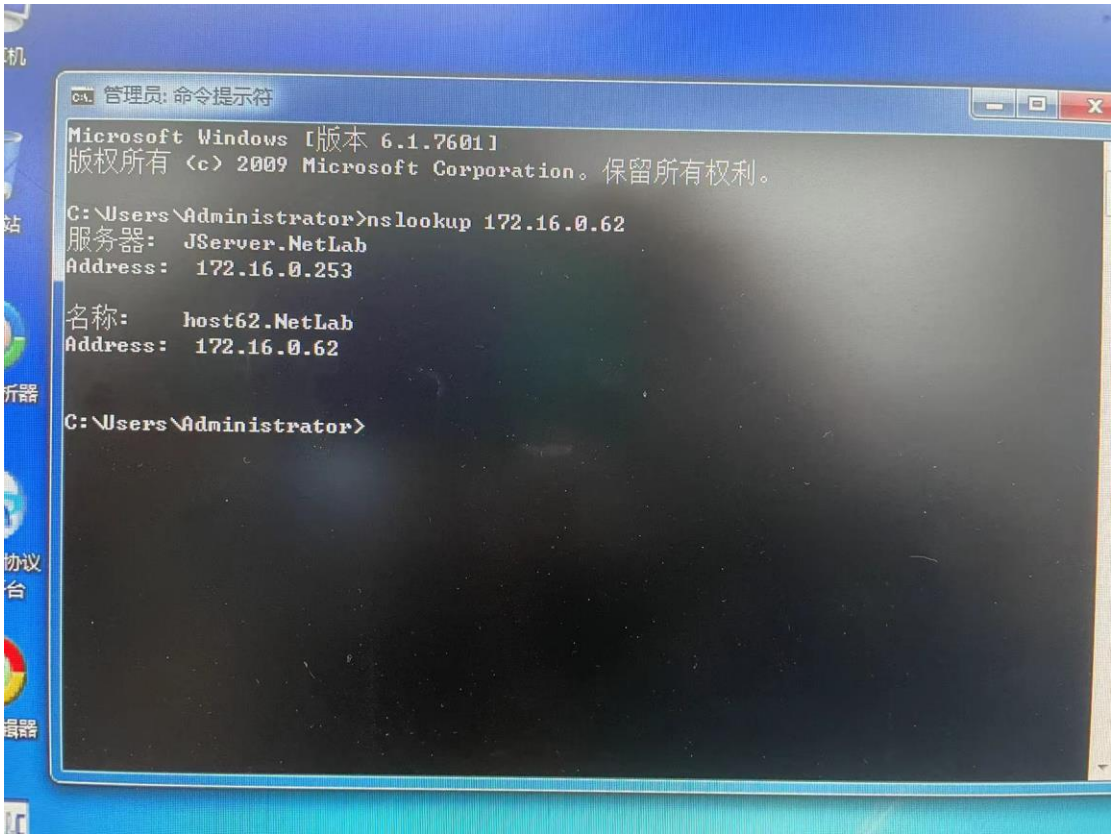
各组主机 IP 地址配置如下：

第一组六台主机 IP 地址依次为 172.16.0.11，172.16.0.12……172.16.0.16；

第二组六台主机 IP 地址依次为 172.16.0.21，172.16.0.22……172.16.0.26；

其它各组以此类推。

1. 在主机 A 执行命令“nslookup 本机的 IP 地址”获取本机的域名，记录下来。



2. 主机 A 启动协议编辑器，编写一个 DNS 正向查询报文。其中：

MAC 层：

源 MAC 地址：本机 MAC 地址

目的 MAC 地址：服务器的 MAC 地址

IP 层：

源 IP 地址：本机 IP 地址

目的 IP 地址：服务器的 IP 地址（默认为 172.16.0.253）

总长度：IP 层及其上层协议总长度

校验和：IP 层字段全部编辑完成后，计算 IP 层校验和

UDP 层：

源端口：大于 1024 的端口

目的端口：53

有效负载长度：UDP 层及其上层协议总长度

校验和：所有字段编辑完成后，计算校验和

DNS 层：

标志：0100

问题记录数：1

域名循环体：选中第一个“域名循环体”项，点击右边按钮[B]来追加域名块。按格式要求填写步骤 1 获取的主机的域名。

例如：设步骤 1 中获取的域名为 host11.Netlab，则追加 2 块。选中“域名循环体”下的“长度”项，修改长度值；出现“域标记”项，选中“域标记”项，点击右边按钮[E]输入相应的值。最后一块“长度”字段为 0。

查询类型：1

查询类别：1

设置如图所示：

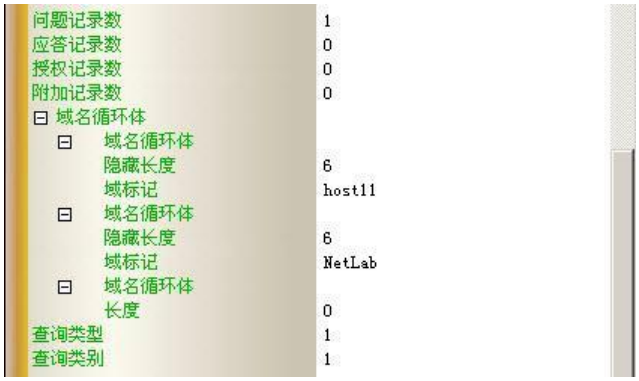
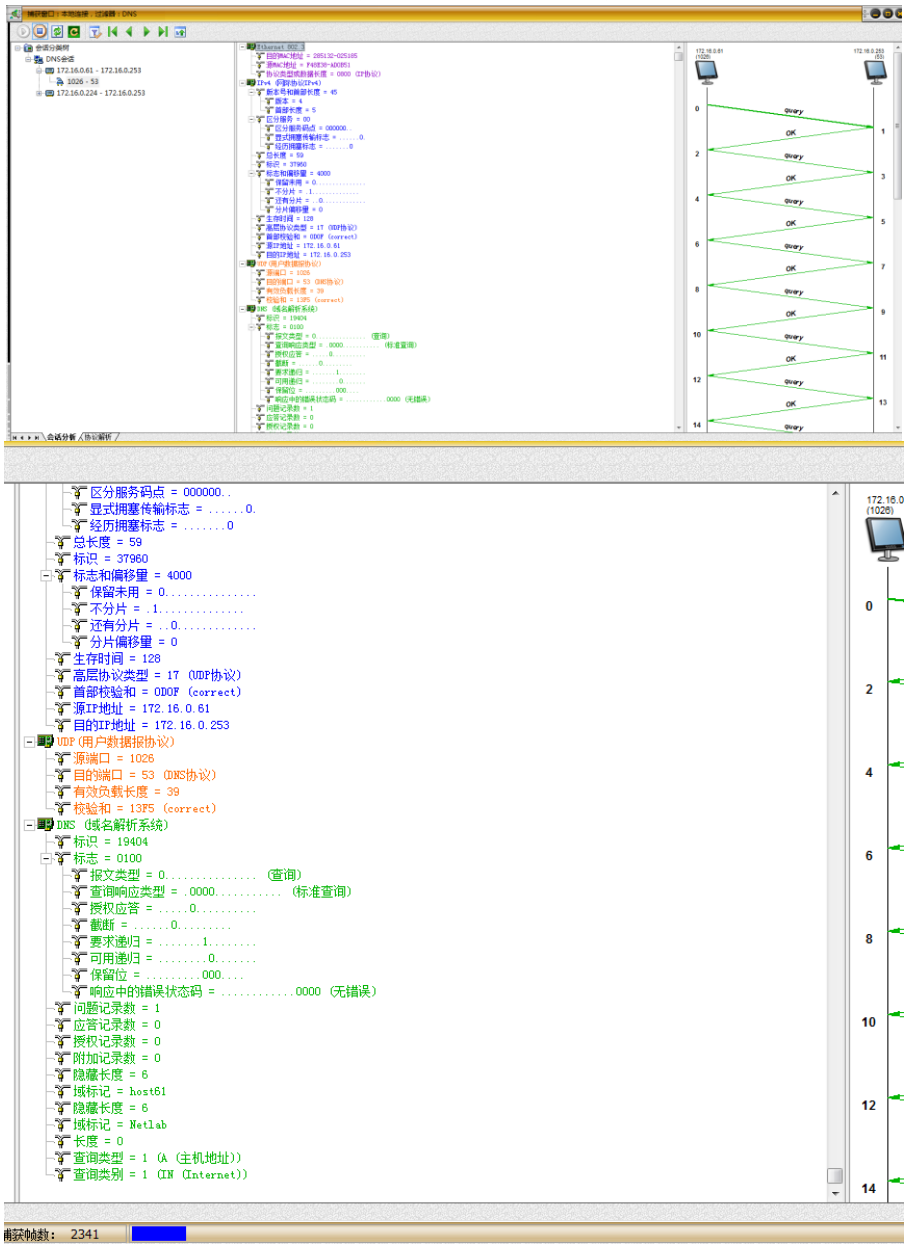


图 11-19DNS 帧的编辑

3. 主机 A 启动协议分析器开始捕获数据，并设置过滤条件（提取 DNS 协议）。
4. 主机 A 发送已编辑好的报文。
5. 主机 A 停止捕获数据。在捕获到的数据中查找 DNS 响应报文。



● 在响应报文中提取对方主机的 IP 地址。

回答：对方主机的 IP 地址为 172.16.0.253。

练习 3 DNS 反向查询

本练习一人一组，现仅以主机 A 为例，其它主机的操作参考主机 A。

1. 该练习中，DNS 服务器及各主机 IP 地址配置同练习二。

2. 主机 A 启动协议编辑器，编写一个 DNS 反向查询报文。其中：

MAC 层：

源 MAC 地址：本机 MAC 地址

目的 MAC 地址：服务器的 MAC 地址

IP 层：

源 IP 地址：本机 IP 地址

目的 IP 地址：服务器的 IP 地址（默认为 172.16.0.253）

总长度：IP 层及其上层协议总长度

校验和：IP 层字段全部编辑完成后，计算 IP 层校验和

UDP 层：

源端口：大于 1024 的合法端口号

目的端口：53

有效负载长度：UDP 层及其上层协议总长度

校验和：所有字段编辑完成后，计算校验和

DNS 层：

标志：0100

问题记录数：1

域名循环体：选中“域名循环体”项，点击右边按钮[B]来追加域名块。按格式要求填写主机反向域域名（反转 IP+.in-addr.arpa）。例如：设主机 A 的 IP 地址为 172.16.0.11，则它的反向域为 11.0.16.172.in-addr.arpa，这需要追加 6 个块，其中最后一个块“长度”字段为 0，如图所示：

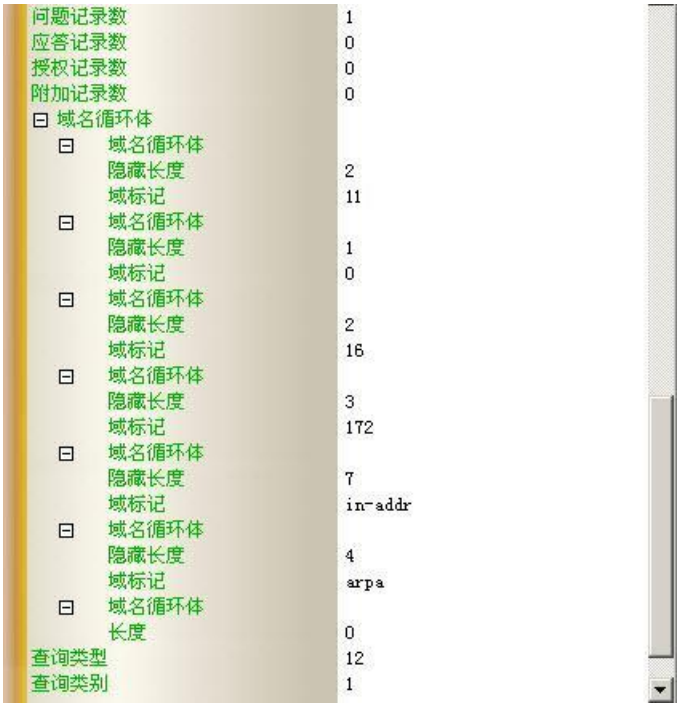


图 11-20DNS 帧的编辑

查询类型：12

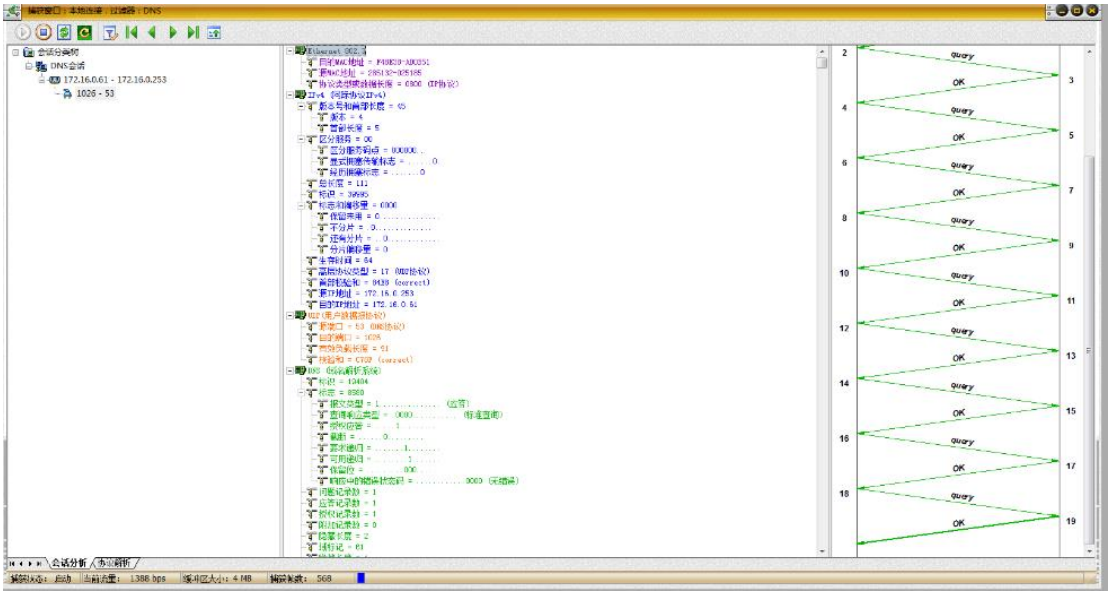
查询类别：1

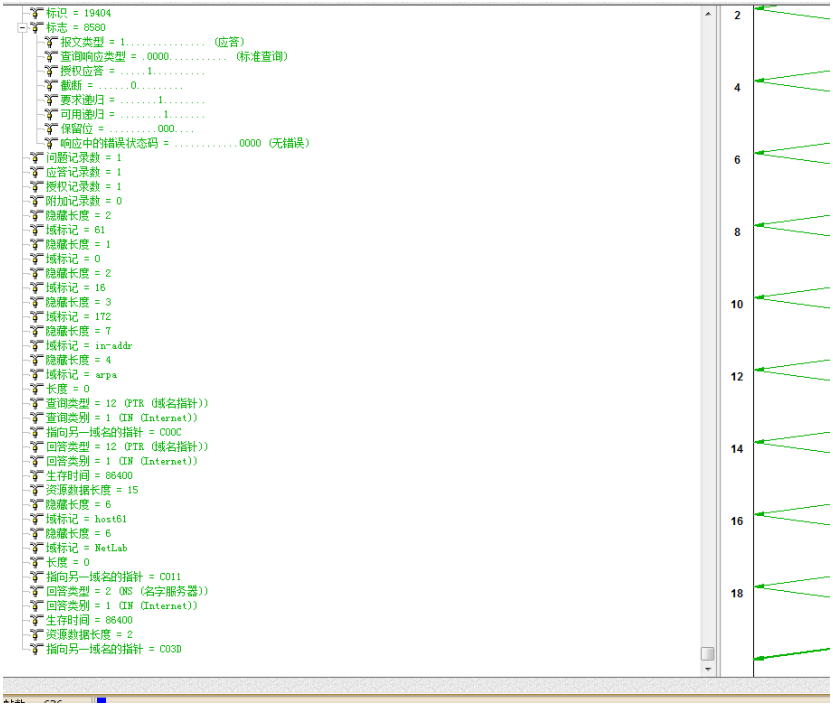
3. 主机 A 启动协议分析器开始数据捕获，设置过滤条件（提取 DNS 协议）。

4. 主机 A 发送已编辑好的报文。

5. 主机 A 停止捕获数据。在捕获到的数据中查找 DNS 响应报文。

●在响应报文中提取主机 A 的域名地址。





回答：域名地址为 172.16.0.61。

练习 4　DNS 的应用及高速缓存

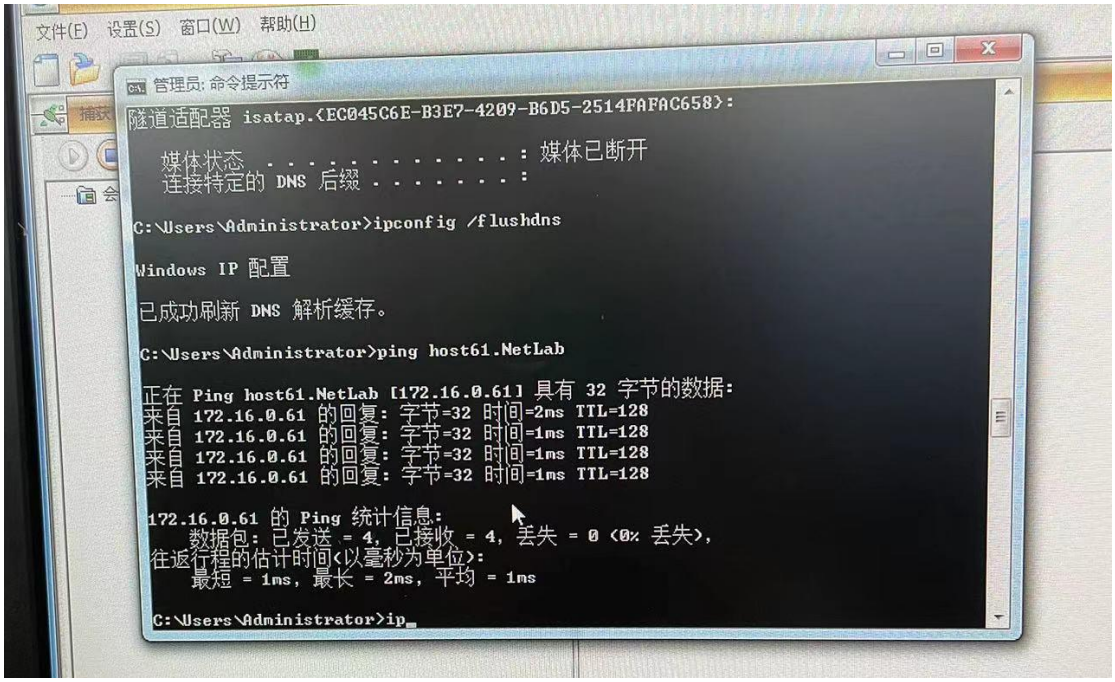
本练习将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

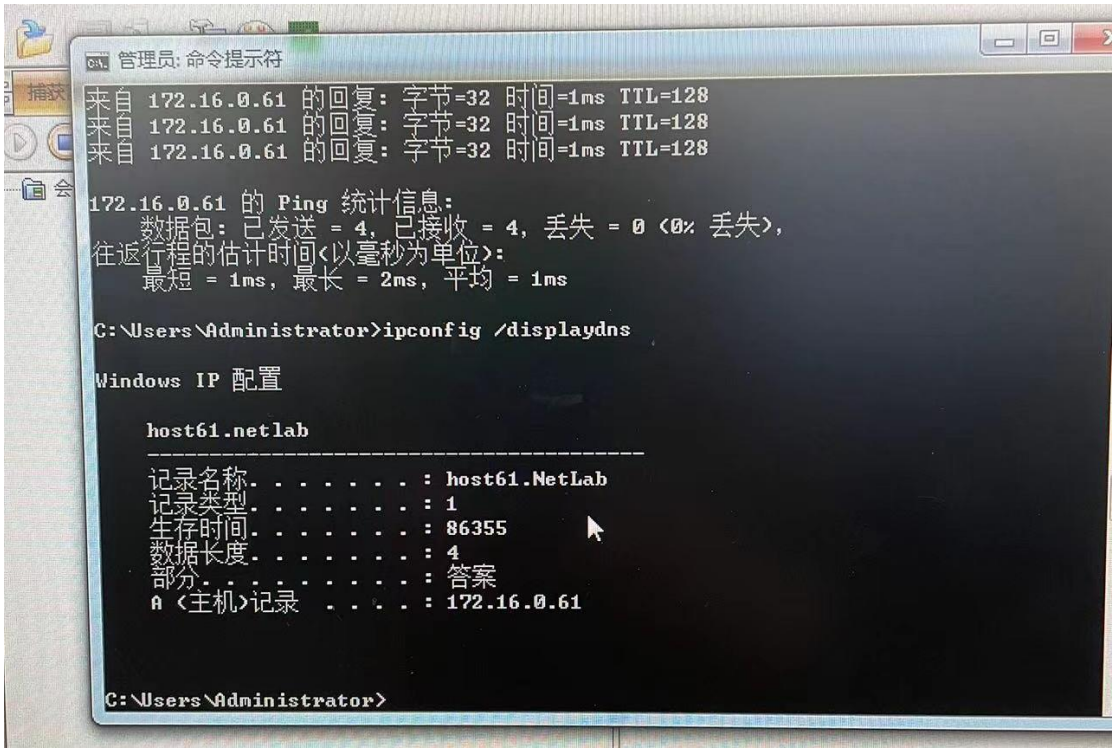
1.该练习中，DNS 服务器及各主机 IP 地址配置同练习二。

2.主机 A、B 分别在命令行下执行“ipconfig/flushdns”命令来清空 DNS 高速缓存。

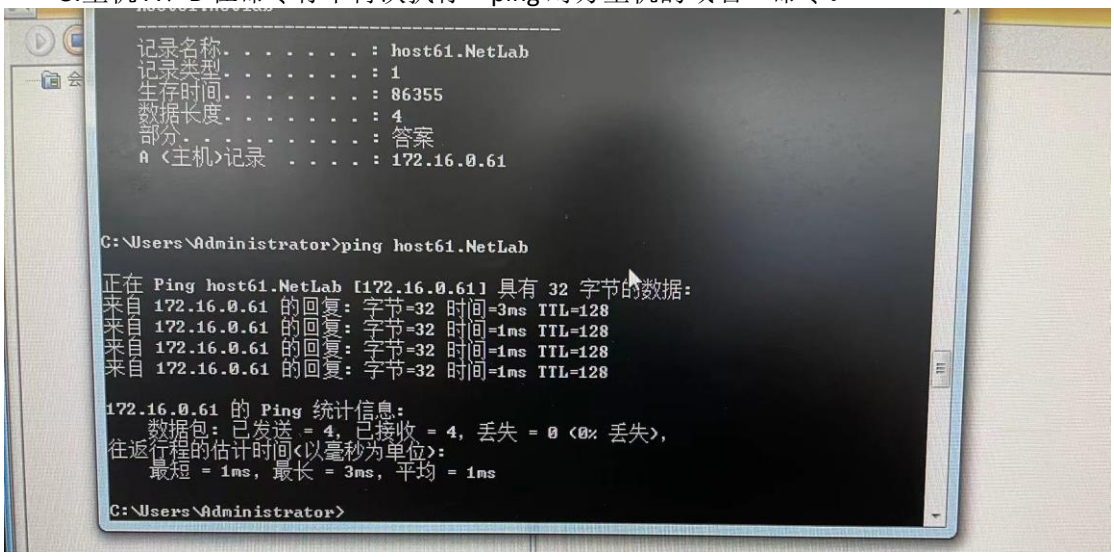
3.主机 A、B 分别启动协议分析器开始捕获数据并设置过滤条件（提取 DNS 协议和 ICMP 协议）。

4.主机 A、B 分别在命令行下执行“ping 对方的域名”命令，然后执行“ipconfig/displaydns”命令来显示 DNS 高速缓存。在缓存中找到对方的域名所对应的记录。

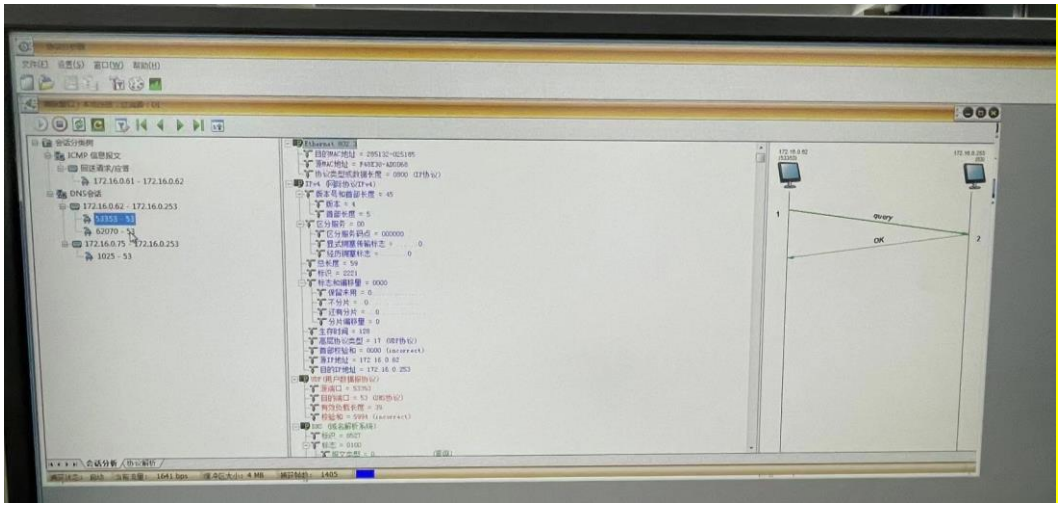


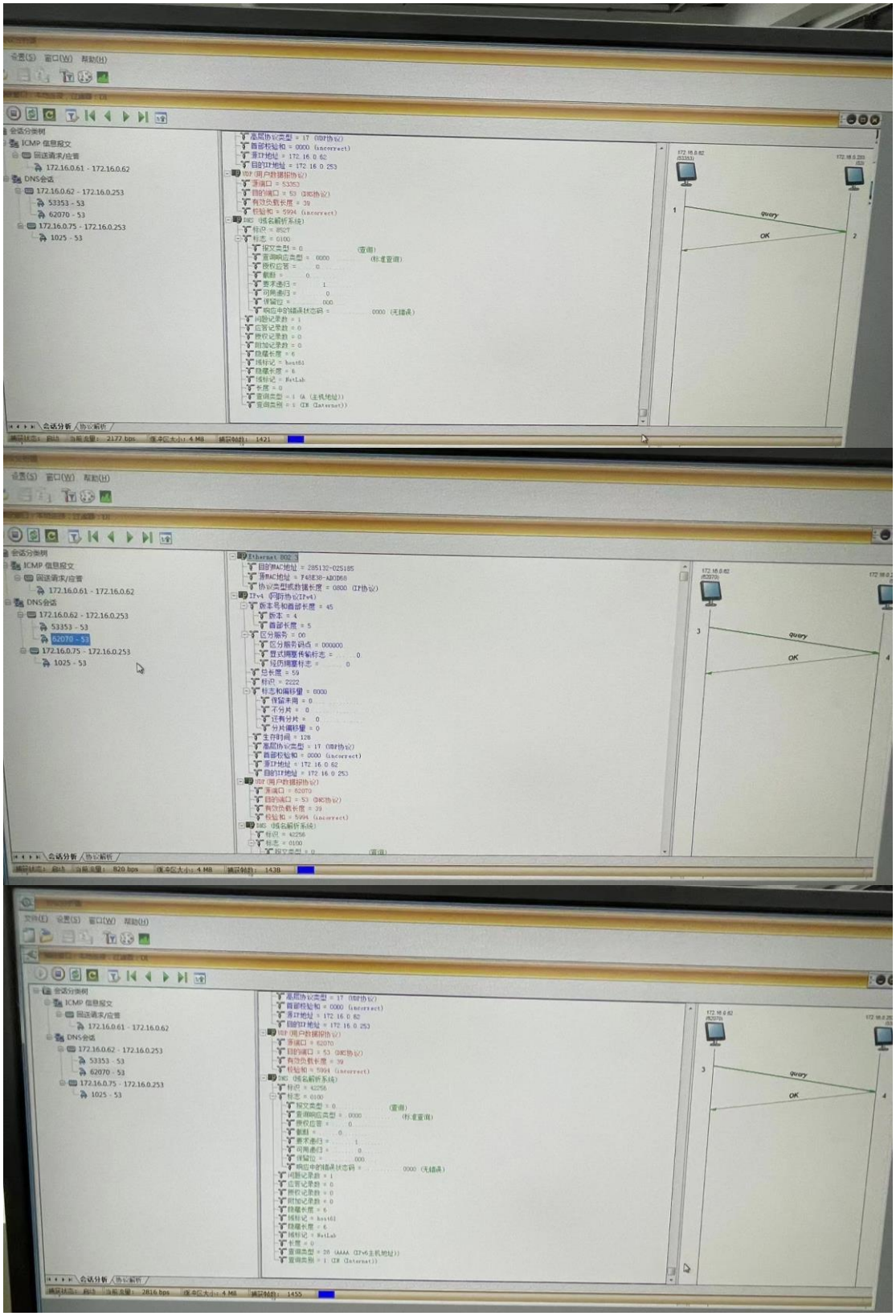


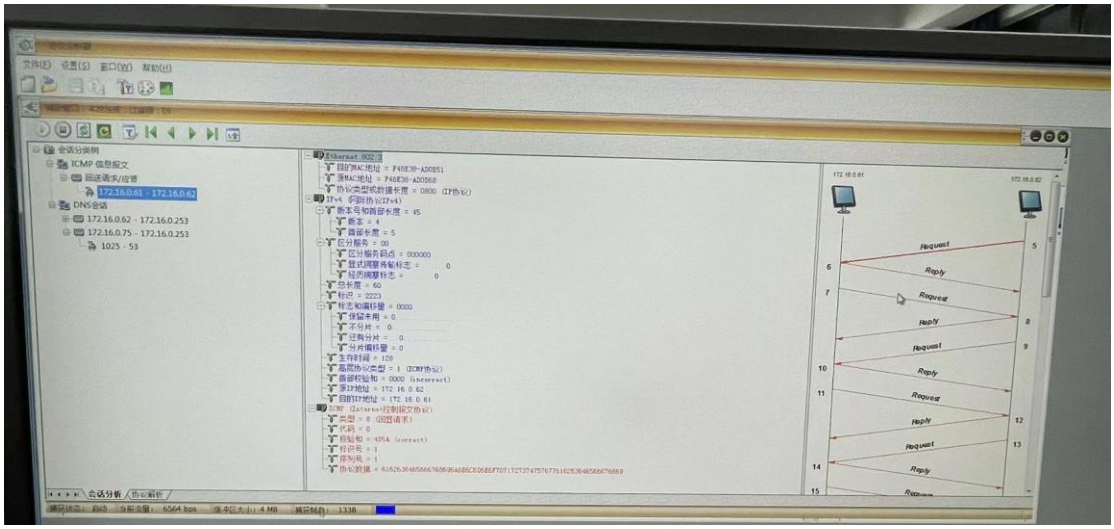
5.主机 A、B 在命令行下再次执行“ping 对方主机的域名”命令。



6.主机 A、B 停止捕获，如下图所示。




query
OK
query
OK
query
OK



分析其捕获的数据及对方的 DNS 高速缓存中的内容，回答问题：

●简述在使用域名完成的通信中，DNS 协议所起到的作用。

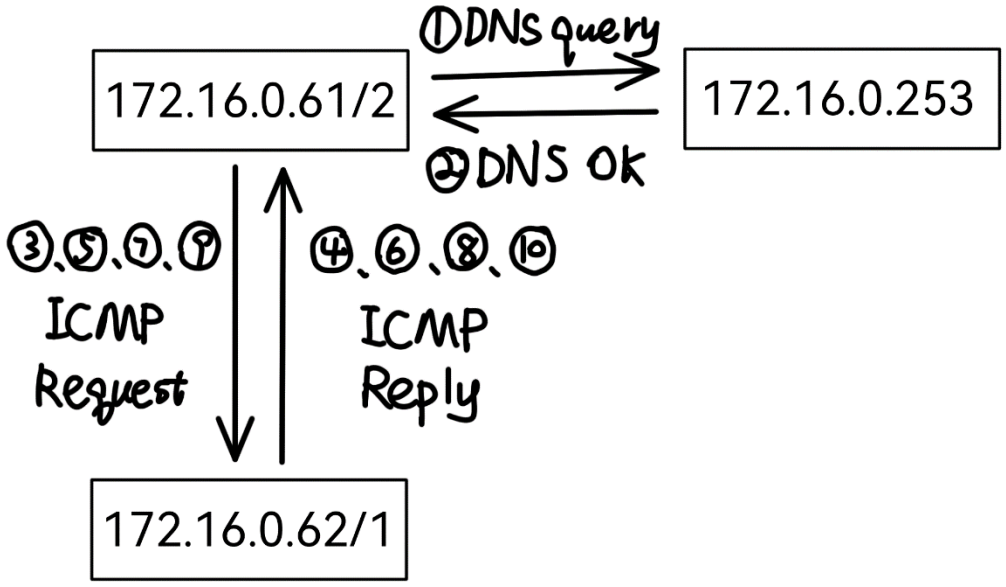
回答：DNS（域名服务）是一种能够完成从域名到地址或从地址到域名的映射系统。当用户在浏览器中输入一个域名，浏览器会向本地的 DNS 服务器发出查询请求，DNS 服务器会根据自身缓存或向上级 DNS 服务器进行查询，最终得到该域名对应的 IP 地址，

●简述 DNS 高速缓存的作用。

回答：当服务器向另一个服务器请求映射并收到它的响应时，在把响应发送给客户之前，DNS 服务器先将这个响应存储在它的高速缓存中。若另一个客户请求同样的映射，它就检查高速缓存并解析这个域名。这种高速缓存技术加速了解析过程。

●参考“会话分析”视图的显示结果，绘制此次访问过程的报文交互图（包括 ICMP 协议）。

回答：如下图所示。



7.恢复网络环境，将“首选 DNS 服务器”清空。

五、 实验结果总结

思考问题:

1. Internet 的域名结构是怎样的？它与目前的电话网的号码结构有何异同之处？
   回答：Internet 采用了层次树状结构的命名方法，其上任意一个主机或路由器都有一个唯一的名字，称为域名。域名从层次上分为顶级域名、二级域名、三级域名等。目前顶级域名有三类：国家顶级域名、国际顶级域名、通用顶级域名。电话网的号码也采用层次树状结构的命名方法，在添加了区号之后也是唯一的，其前数位与运营商、所在地区相关。
2. 域名的 IP 地址是否只有一个？
   回答：一般来说，一个域名在同一时间只能与一个特定的 IP 地址相对应。然而，从理论上讲，一个域名是可以对应到多个 IP 地址的，比如“Baidu.com”就拥有多个不同的 IP 地址。但在实际的用户访问过程中，当用户访问这个域名时，系统会将其导向其中一个特定的 IP 地址，而不是同时访问所有的 IP 地址。
3. 域名服务协议的主要功能是什么？域名服务协议中的根服务器和授权服务器有何区别？授权服务器与管辖区有何关系？
   回答：域名是用来解决用户记忆 IP 地址困难而产生的域名地址。在访问百度时，原本需要记忆一串 IP 地址，但有了域名后就不需要了。计算机只能识别 IP 地址，而域名和 IP 地址之间存在一种对应关系。为了将域名转换为计算机能识别的 IP 地址，我们需要域名服务协议这一工具。
   根服务器是负责管理互联网域名系统的服务器，它并不直接对域名进行解析，而是知道如何找到授权域名服务器，以便将查询传递给正确的授权服务器。授权服务器是负责实际解析域名的服务器，它直接对域名进行解析。
   因特网允许各个单位根据本单位的具体情况将本域名划分为若干个域名服务器管辖区。在各管辖区设置相应的授权域名服务器。