



1

DSN实验

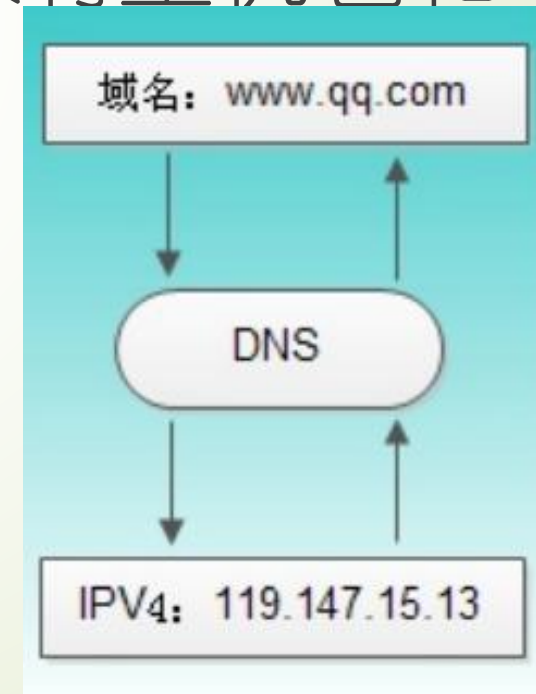
冯巾松

fengjinsong@tongji.edu.cn

DNS

2

- DNS(Domain Name System)是“域名系统”的英文缩写
- 是一种组织成域层次结构的计算机和网络服务命名系统，它用于TCP/IP网络
- 它所提供的服务是用来将主机名和域名转换为IP地址的工作。



为什么需要DNS？

- 网络通讯大部分是基于TCP/IP的，而TCP/IP是基于IP地址的，所以计算机在网络上进行通讯时只能识别如“202.96.134.133”之类的IP地址，而不能认识域名。
- 一般无法记住10个以上IP地址的网站，所以人们访问网站时，更多的是在浏览器地址栏中输入域名，就能看到所需要的页面，这是因为有一个叫“DNS服务器”的计算机，自动把域名“翻译”成了相应的IP地址，然后调出IP地址所对应的网页
- DNS是应用层协议，事实上它是为其他应用层协议工作的，包括并不限于HTTP、SMTP以及FTP，用于将用户提供的主机名解析为IP地址。

DNS的工作过程

- ➡ ①用户主机上运行着DNS的客户端，就是PC机或者手机客户端运行着DNS客户端了
- ➡ ②浏览器将接收到的URL中抽取出域名字段，即要访问的主机名(如http://www.baidu.com/) 并将这个主机名传送给DNS应用的客户端
- ➡ ③DNS客户机端向DNS服务器端发送一份查询报文，其中包含着要访问的主机名字段（中间包括一些列缓存查询以及分布式DNS集群的工作）。
- ➡ ④该DNS客户机最终会收到一份回答报文，其中包含有该主机名对应的IP地址。
- ➡ ⑤一旦该浏览器收到来自DNS的IP地址，就可以向该IP地址定位的HTTP服务器发起TCP连接

DNS服务的体系架构

- ➡ DNS主要作用就是将主机域名转换为ip地址。假设运行在用户主机上的某些应用程序（如Web浏览器或者邮件阅读器）需要将主机名转换为IP地址。这些应用程序将调用DNS的客户端，并指明需要被转换的主机名。用户主机的DNS客户端接收到后，向网络中发送一个DNS查询报文。
- ➡ 所有DNS请求和回答报文使用的UDP数据报经过端口53发送

DNS服务的体系架构

6

➡ 经过若干ms到若干s的延时后，用户主机上的DNS客户端接收到一个提供所希望映射的DNS回答报文。这个查询结果则被传递到调用DNS的应用程序。因此，从用户主机上调用应用程序的角度看，DNS是一个提供简单、直接的转换服务的黑盒子。但事实上，实现这个服务的黑盒子非常复杂，它由分布于全球的大量DNS服务器以及定义了DNS服务器与查询主机通信方式的应用层协议组成。

DNS分布式集群工作方式

- ➡ DNS的一种简单的设计模式就是在因特网上只使用一个DNS服务器，该服务器包含所有的映射，在这种集中式的设计中，客户机直接将所有查询请求发往单一的DNS服务器，同时该DNS服务器直接对所有查询客户机做出响应，
- ➡ 尽管这种设计方式非常诱人，但不适用当前的互联网，因为当今的因特网有着数量巨大并且在持续增长的主机，这种集中式设计会有单点故障问题（故障一个，全球着急）、
- ➡ 使用分布式的层次数据库模式以及缓存方法来解决单点集中式的问题。

DNS分布式集群工作方式

- ➡ 通信容量（上亿台主机发送的查询DNS报文请求，包括但不限于所有的HTTP请求，电子邮件报文服务器，TCP长连接服务），远距离的时间延迟（澳大利亚到纽约的举例），维护开销大（因为所有的主机名-ip映射都要在一个服务站点更新）等问题。
- ➡ DNS服务器一般分三种：根DNS服务器、顶级DNS服务器、权威DNS服务器。

DNS服务器的部分层次结构



DNS域名称

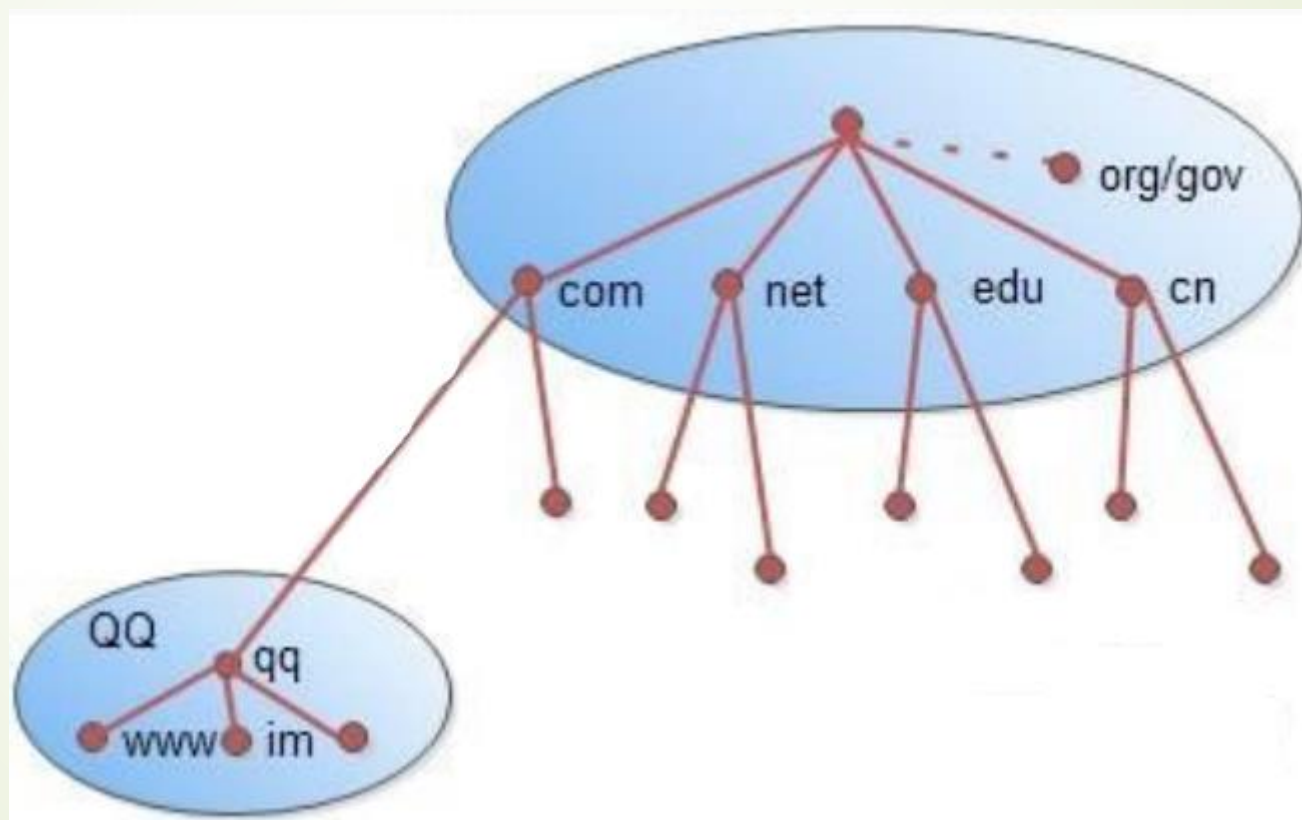
10

- ➡ 域名系统作为一个层次结构和分布式数据库，包含各种类型的数据，包括主机名和域名。
- ➡ DNS数据库中的名称形成一个分层树状结构称为域命名空间。域名包含单个标签分隔点，例如：im.qq.com完全限定域名 (FQDN) 唯一地标识在 DNS 分层树中的主机的位置，通过指定的路径中点分隔从根引用的主机的名称列表。

DNS域名称

11

主机的 FQDN 是 im.qq.com DNS 域的名称层次结构



DNS域名称空间的组织方式

➡ 按其功能命名空间中用来描述 DNS 域名称的五个类别，以及与每个名称类型的示例

名称类型	说 明	示 例
根域	DNS域名中使用时，规定由尾部句点(.)来指定名称位于根或更高级别的域层次结构	单个句点(.)或句点用于末尾的名称
顶级域	用来指示某个国家/地区或组织使用的名称的类型名称	.com
第二层域	个人或组织在 Internet 上使用的注册名称	qq.com
子域	已注册的二级域名派生的域名，通俗的讲就是网站名	www.qq.com
主机名	通常情况下，DNS 域名的最左侧的标签标识网络上的特定计算机，如hl	hl.www.qq.com Blog

DNS

13

➡ 互联网域名系统由名称注册机构负责维护分配由组织和国家/地区的顶级域在 Internet 上进行管理。这些域名有很多缩写，两个字母和三个字母的国家/地区使用的缩写使用。

➡ 一些常见的DNS域名称

DSN域名称	组织机构
Com	商业公司
Edu	教育机构
Net	网络公司
Gov	非军事政府机构
mil	军事政府机构

DNS域名资源记录

➡ DNS数据库中包含的资源记录 (RR)。每个RR 标识数据库中的特定资源。在建立DNS服务器时，经常会用到SOA,NS,A之类的记录，在维护DNS服务器时，会用到MX，CNAME记录。

➡ 常见的RR

说 明	类	时间(ttl)	类型	数 据
起始授权机构	互联网 (IN)	默认值为60分钟	SOA	所有者名称 主名称服务器 DNS 名称、 序列号 刷新间隔 重试间隔 过期时间 最小 TTL
主机	互联网 (IN)	记录特定 TTL (如果存在)，否则区域 (SOA) TTL	A	所有者名称 (主机的 DNS 名称) 主机 IP 地址
名称服务器	互联网 (IN)	记录特定 TTL (如果存在)，否则区域 (SOA) TTL	NS	所有者名称 名称服务器 DNS 名称
邮件交换器	互联网 (IN)	记录特定 TTL (如果存在)，否则区域 (SOA) TTL	MX	所有者名称 邮件 Exchange Server DNS 名称的首选项值
别名	互联网 (IN)	记录特定 TTL (如果存在)，否则区域 (SOA) TTL	CNAME	所有者名称 (别名) 主机的 DNS 名称

DNS服务的工作过程

- 当 DNS 客户机需要查询程序中使用的名称时，它会查询本地DNS服务器来解析该名称
- 客户机发送的每条查询消息都包括3条信息，以指定服务器应回答的问题。
 - 1) 指定的 DNS 域名，表示为完全合格的域名(FQDN)；
 - 2) 指定的查询类型，它可根据类型指定资源记录，或作为查询操作的专门类型；
 - 3) DNS域名的指定类别。

DNS服务的工作过程

16

- 对于DNS 服务器，它始终应指定为 Internet 类别。例如，指定的名称可以是计算机的完全合格的域名，如im.qq.com，并且指定的查询类型用于通过该名称搜索地址资源记录。
- DNS 查询以各种不同的方式进行解析。客户机有时也可通过使用从以前查询获得的缓存信息就地应答查询。DNS 服务器可使用其自身的资源记录信息缓存来应答查询，也可代表请求客户机来查询或联系其他DNS服务器，以完全解析该名称，并随后将应答返回至客户机。这个过程称为**递归**

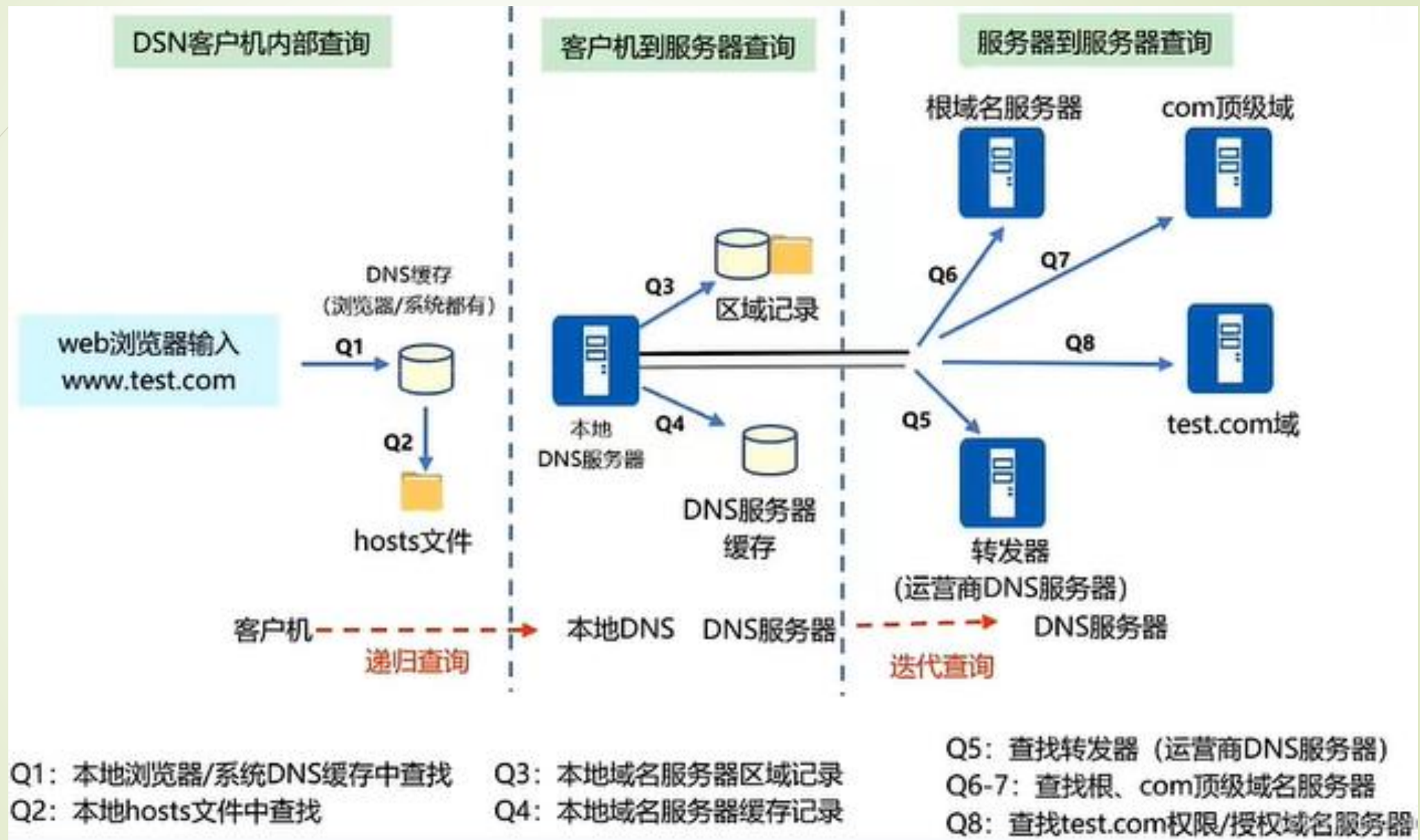
DNS服务的工作过程

17

■ 另外，客户机自己也可尝试联系其他的DNS服务器来解析名称。如果客户机这么做，它会使用基于服务器应答的独立和附加的查询，该过程称作**迭代**，即DNS服务器之间的交互查询就是迭代查询。

DNS域名解析过程

18



DNS域名解析过程

19

- ➡ 0) 当用户通过浏览器访问某域名时，浏览器首先会在**浏览器缓存**中查找是否有该域名对应的IP地址（若曾经访问过该域名且没有清空缓存便存在）；
- ➡ 1) 当浏览器缓存中无域名对应IP，操作系统会先检查自己的**系统缓存(本地的hosts文件)**是否有这个网址映射关系，如果有，就先调用这个IP地址映射，完成域名解析。
- ➡ 2) 如果hosts里没有这个域名的映射，则查找**本地DNS解析器**缓存，是否有这个网址映射关系，如果有，直接返回，完成域名解析。

以上三步均为客户端的DNS缓存

DNS域名解析过程

20

- ➡ 3) 如果hosts与本地DNS解析器缓存都没有相应的网址映射关系，首先会找TCP/IP参数中设置的首选**DNS服务器**，在此叫它本地DNS服务器，此服务器收到查询时，如果要查询的域名，包含在本地配置区域资源中，则返回解析结果给客户机，完成域名解析，此解析具有权威性。
- ➡ 4) 如果要查询的域名，不由本地DNS服务器区域解析，但该服务器已**缓存**了此网址映射关系，则调用这个IP地址映射，完成域名解析，此解析不具有权威性。

从客户端到本地DNS服务器是属于**递归**查询

DNS域名解析过程

21

- ➡ 5) 如果本地DNS服务器本地区域文件与缓存解析都失效，则根据本地DNS服务器的设置（是否设置**转发器**）进行查询。
- ➡ 6) 如果未用转发模式，本地DNS就把请求发至13台根DNS，**根DNS服务器**收到请求后会判断这个域名(.com)是谁来授权管理，并会返回一个负责该顶级域名服务器的一个IP。
- ➡ 7) 本地DNS服务器收到IP信息后，将会联系负责.com域的这台服务器。这台负责.com域的服务器收到请求后，如果自己无法解析，它就会找一个管理.com域的下一级DNS服务器地址(<http://test.com>)给本地DNS服务器，重复该步骤直至找到正确纪录

DNS域名解析过程

➡ 8) 本地域名服务器把返回的结果保存到缓存，以备下一次使用，同时将该结果反馈给客户端，客户端通过这个IP地址与web服务器建立链接

DNS服务器之间的交互查询就是迭代查询

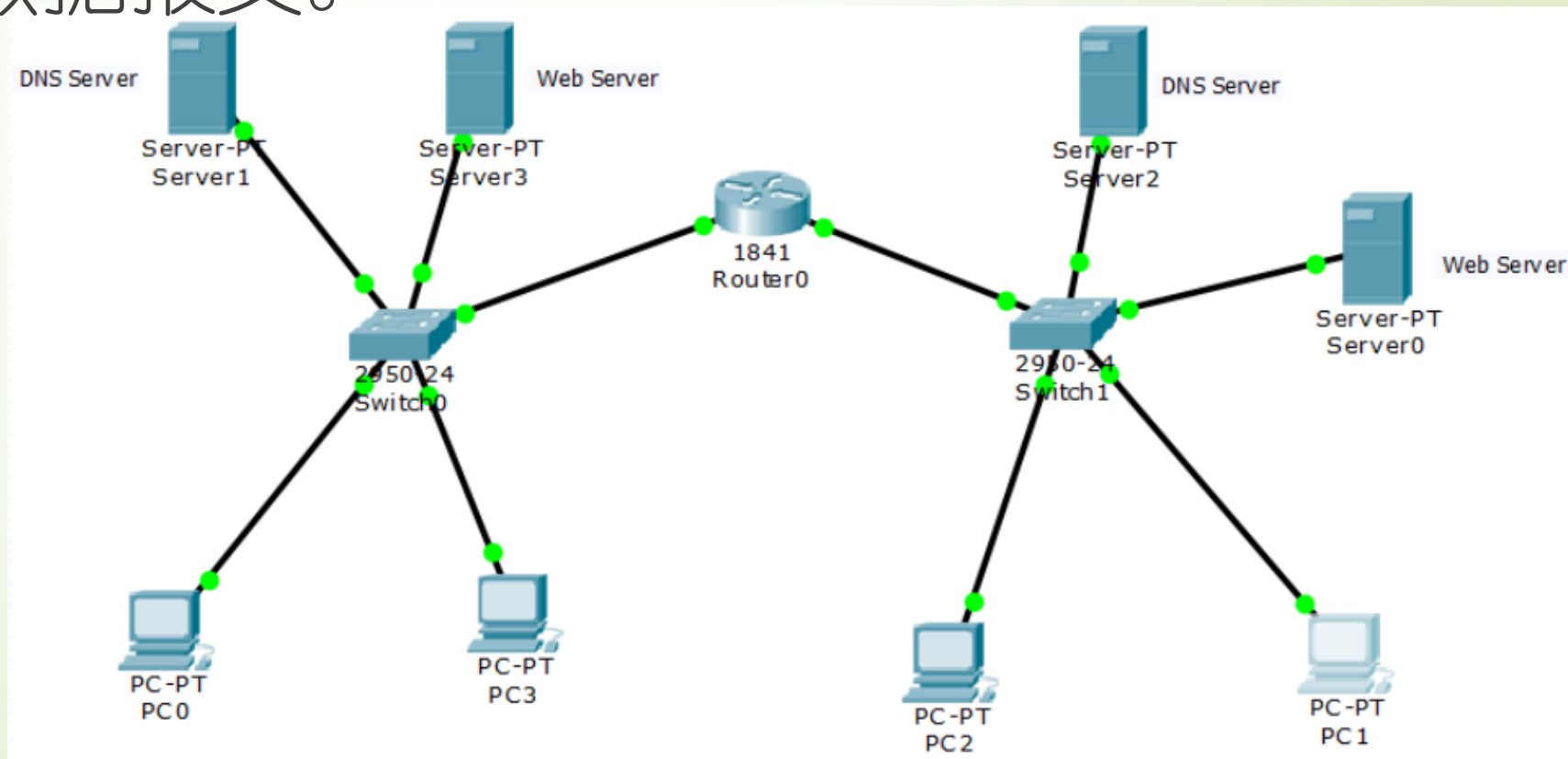
IPv4根域名服务器

➡ IPv4根域名服务器共有13套设备，构成13组域名服务器

域名	IP 地址	运营商
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod(瑞典)
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC(英国)
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project(日本)

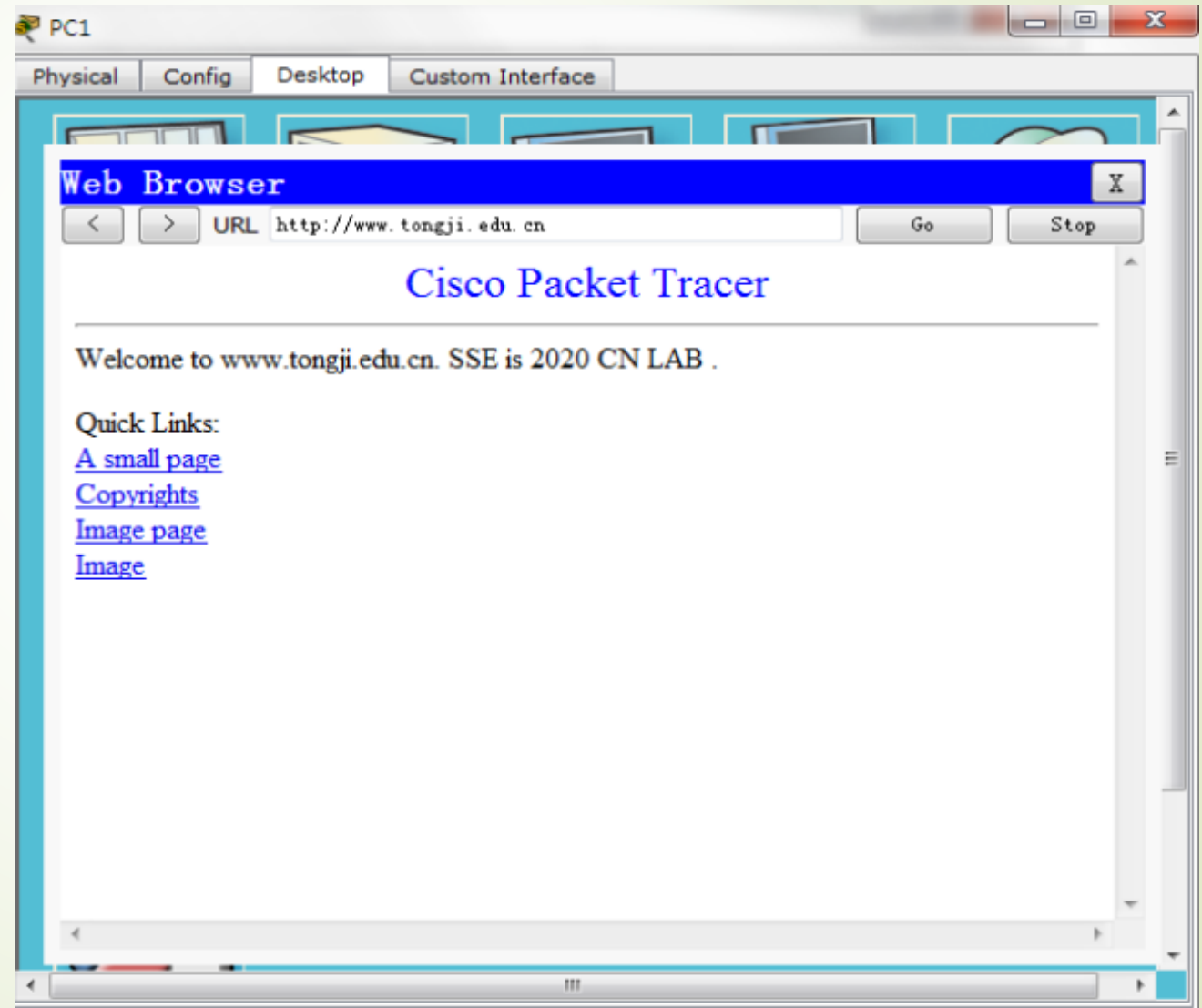
Packet Tracer 分析UDP报文

- ➡ 1) 设置WEB服务器和简单的DNS服务器；
- ➡ 2) 打开PC0浏览器，输入配置Web服务器的Web 地址，如www.tongji.edu.cn,产生UDP数据报文。



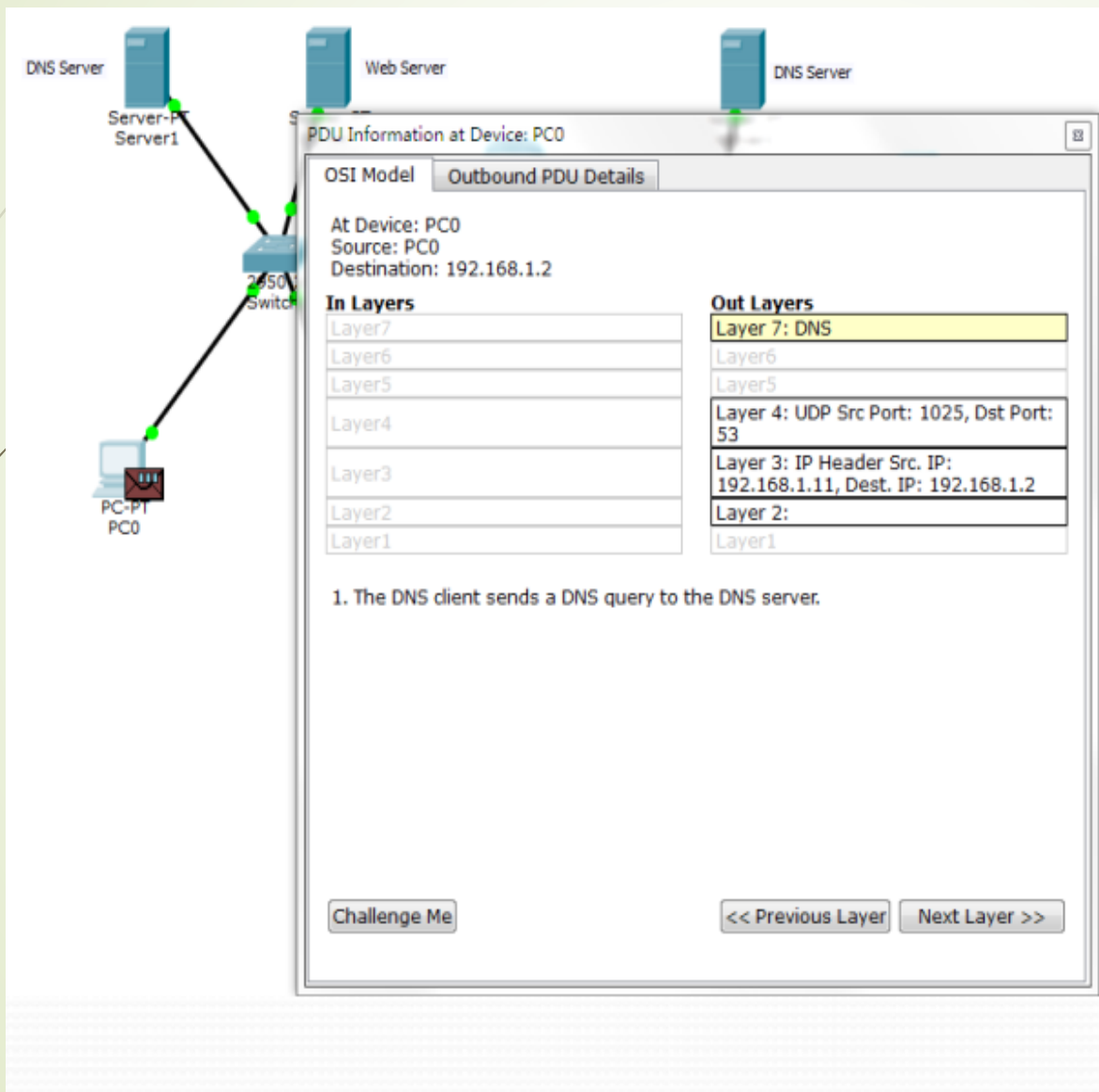
Packet Tracer 分析UDP报文

PC1 WEB Browser



Packet Tracer 分析DNS

26



The network diagram shows a PC-PT PC0 connected to a 2950 Switch. The switch is connected to two DNS Servers (Server-P-Server1 and Server-P-Server2) and a Web Server.

PDU Information at Device: PC0

At Device: PC0
Source: PC0
Destination: 192.168.1.2

OSI Model | **Outbound PDU Details**

In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

Layer 7: DNS
Layer6
Layer5
Layer 4: UDP Src Port: 1025, Dst Port: 53
Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.1.2
Layer 2:
Layer1

1. The DNS client sends a DNS query to the DNS server.

PDU Information at Device: PC0

OSI Model | **Outbound PDU Details**

PDU Formats

0 1 5 8 9 12 15 Bits

ID															
OPCODE		A	T	R	R	Z	RCODE								
A		C		D		A									
QDCOUNT: 1															
ANCOUNT: 0															
NSCOUNT: 0															
ARCOUNT: 0															

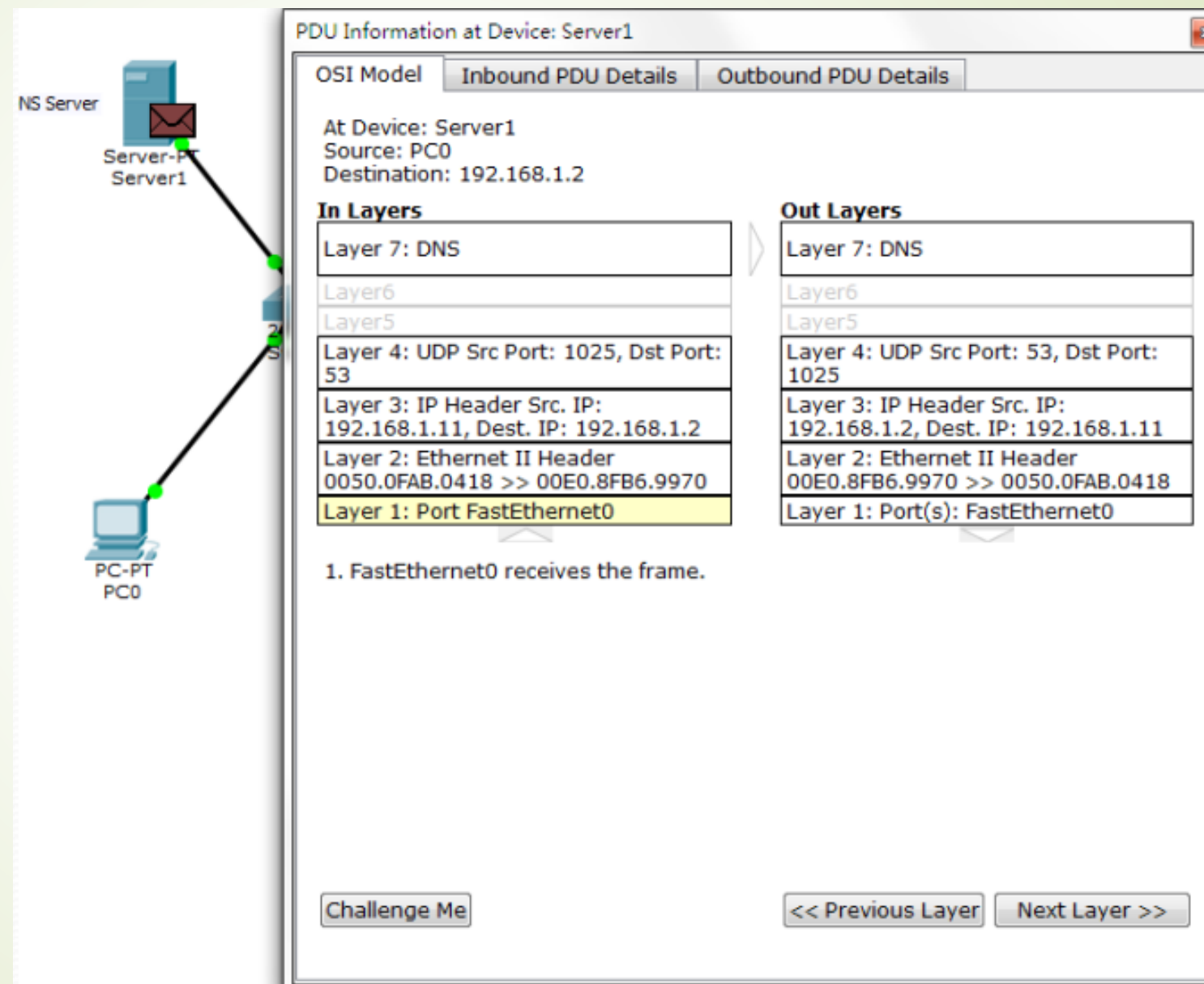
DNS Answer

0 16 31 Bits

NAME: www.tongji.edu.cn																															
TYPE: 0x0001																CLASS: 0x0001															
TTL: 86400																															
LENGTH: 0																															

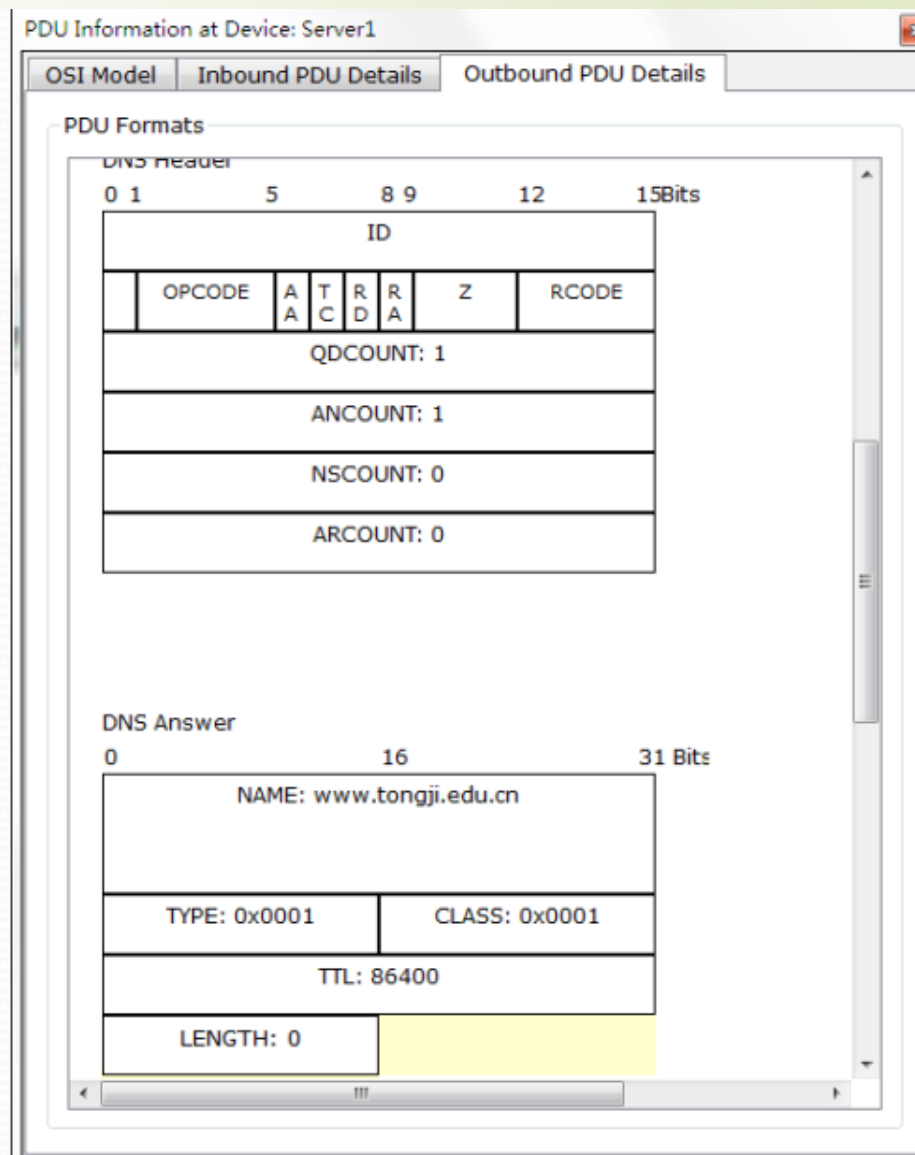
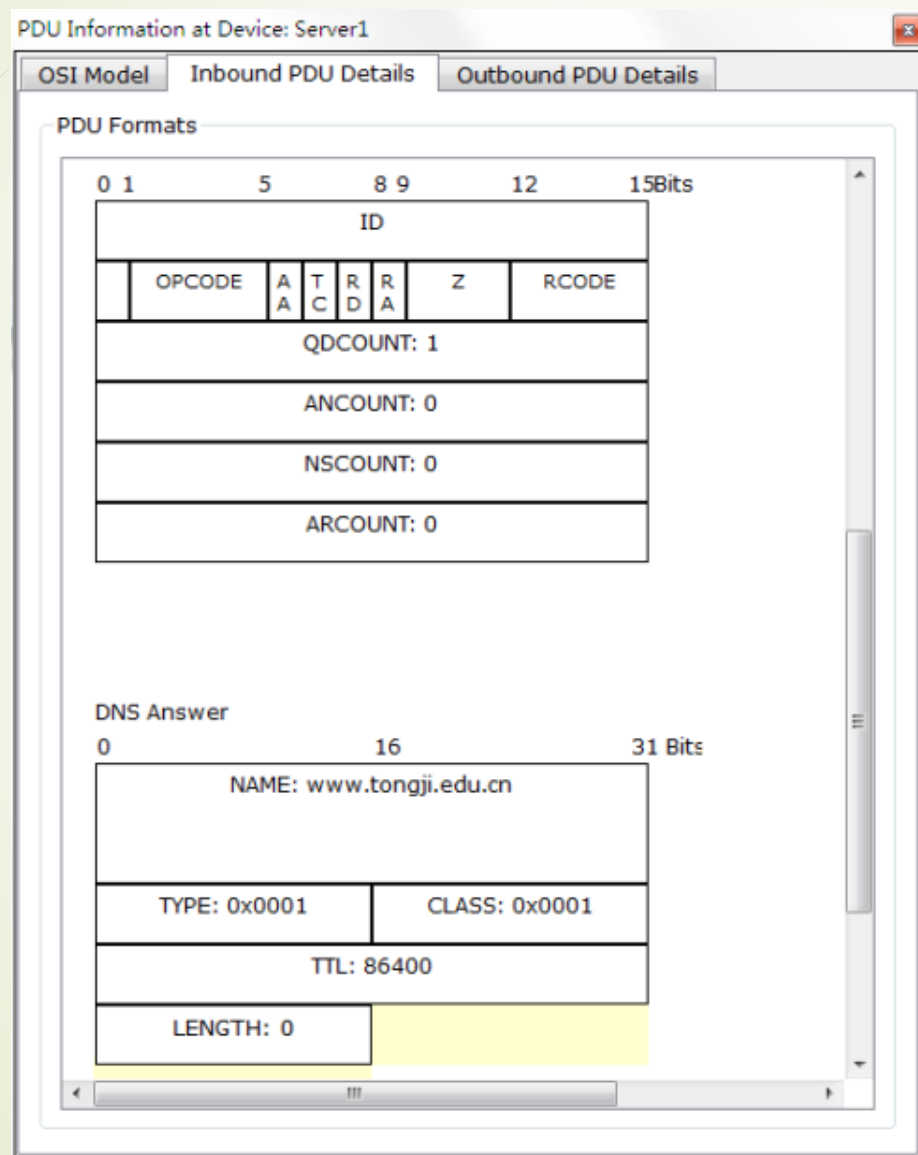
Packet Tracer 分析DNS

27



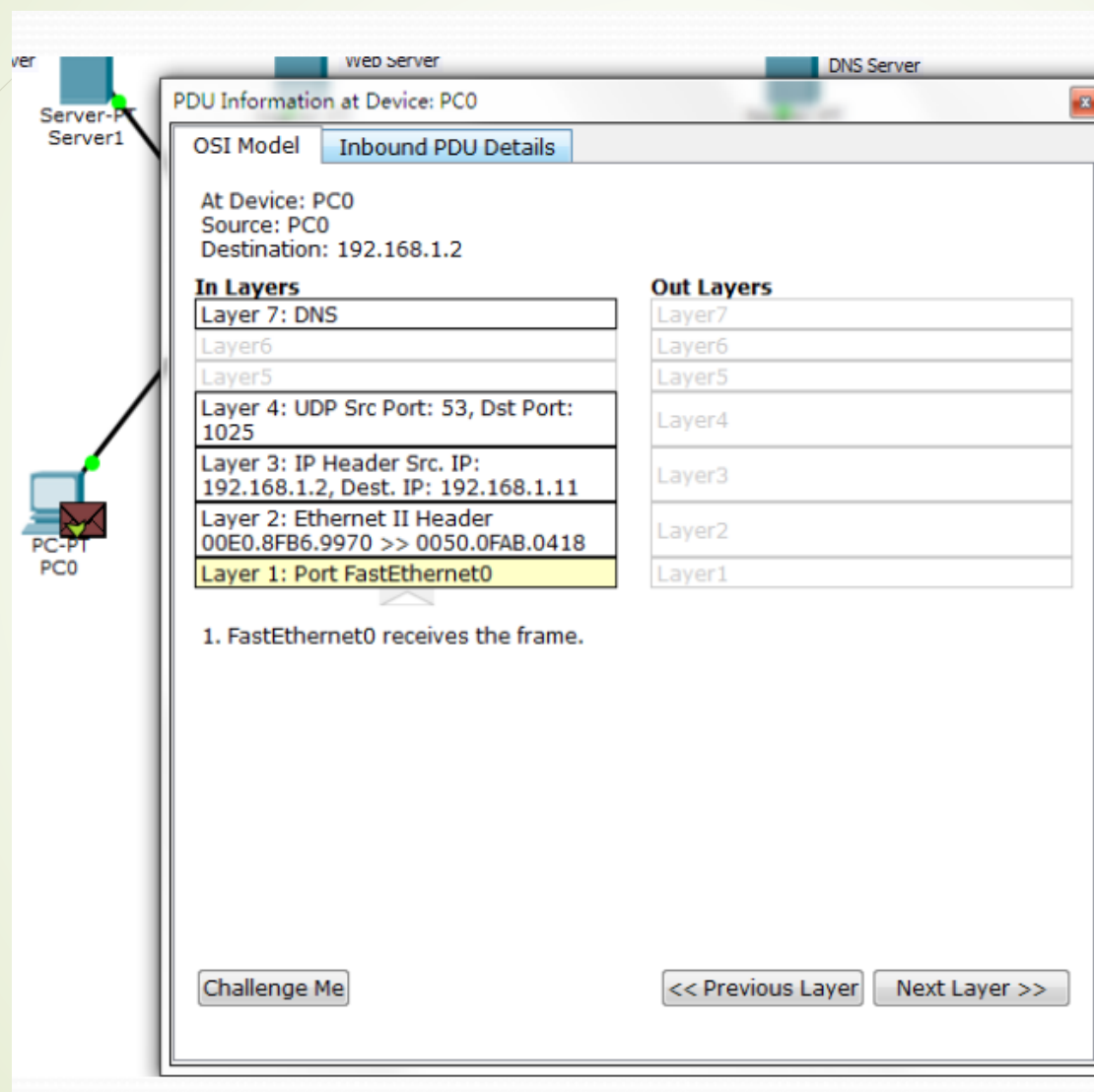
Packet Tracer 分析DNS

28



Packet Tracer 分析DNS

29



PDU Information at Device: PC0

At Device: PC0
Source: PC0
Destination: 192.168.1.2

In Layers

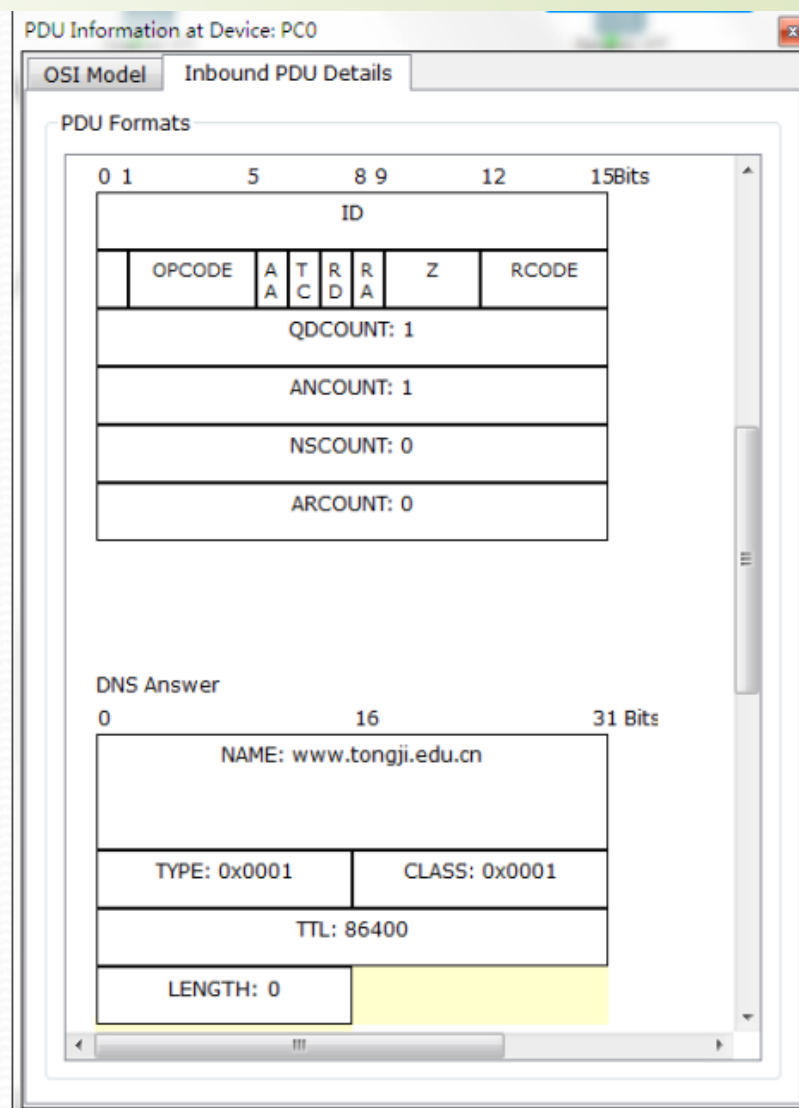
- Layer 7: DNS
- Layer 6
- Layer 5
- Layer 4: UDP Src Port: 53, Dst Port: 1025
- Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.11
- Layer 2: Ethernet II Header 00E0.8FB6.9970 >> 0050.0FAB.0418
- Layer 1: Port FastEthernet0

Out Layers

- Layer 7
- Layer 6
- Layer 5
- Layer 4
- Layer 3
- Layer 2
- Layer 1

1. FastEthernet0 receives the frame.

Challenge Me << Previous Layer Next Layer >>



PDU Information at Device: PC0

OSI Model Inbound PDU Details

PDU Formats

0 1 5 8 9 12 15Bits

ID														
OPCODE		A	T	R	R	Z	RCODE							
A		C		D		A								
QDCOUNT: 1														
ANCOUNT: 1														
NSCOUNT: 0														
ARCOUNT: 0														

DNS Answer

0 16 31 Bits

NAME: www.tongji.edu.cn																														
TYPE: 0x0001																CLASS: 0x0001														
TTL: 86400																														
LENGTH: 0																														

Packet Tracer 分析DNS

➡ 1) 报文头DNS Message

问题数QDCOUNT 表示报文请求段中的问题记录数

资源记录数ANCOUNT 表示报文回答段中的回答记录数

授权资源记录数NSCOUNT 表示报文授权段中的授权记录数

额外资源记录数ARCOUNT 表示报文附加段中的附加记录数

➡ 2) 查询报文 DNS Query

NAME表示查询名，一般表示为需要查询的域名

TYPE表示查询类型

CLASS表示查询类

TTL表示生存时间，表示的是资源记录可以缓存的时间

LENGTH表示资源数据长度

Packet Tracer 分析DNS

31

- ➡ 3) 应答报文 DNS Answer
 - NAME表示资源记录包含的域名
 - TYPE表示资源记录的类型
 - CLASS表示资源记录的类
 - TTL表示资源记录可以缓存的时间
 - LENGTH表示资源数据长度
 - IP表示域名解析的结果

Wireshark DNS报文抓取分析

32

Wireshark interface showing a DNS query and response. The packet list shows a query from 192.168.1.6 to 192.168.1.1 for www.baidu.com. The packet details pane shows the query structure, including the 'Recursion desired' flag. The packet bytes pane shows the raw data. A command prompt window is open, showing the IP configuration for the WLAN adapter, with the IPv4 address 192.168.1.6 highlighted. The command prompt also shows the ping command being executed.

过滤 DNS

递归

本机IP

```
> Frame 10: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface wlan0
> Ethernet II, Src: IntelCor_a7:24:8e (f0:d5:bf:a7:24:8e), Dst: TaicangT_9a:7
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 65104, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x0d04
  Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    0... .. = Truncated: Message is not truncated
    ... ..1... .. = Recursion desired: Do query recursively
    .... ..0... .. = Z: reserved (0)
    .... ..0... .. = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    [Response In: 11]
```

命令提示符

```
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 本地连接* 12:

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . :
本地连接 IPv6 地址 . . . . . : fe80::d617:a8da:5a61:23f4%12
IPv4 地址 . . . . . : 192.168.1.6
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 192.168.1.1

C:\Users\user>ping www.baidu.com

正在 Ping www.a.shifen.com [180.101.51.73] 具有 32 字节的数据:
来自 180.101.51.73 的回复: 字节=32 时间=16ms TTL=53
来自 180.101.51.73 的回复: 字节=32 时间=12ms TTL=53
来自 180.101.51.73 的回复: 字节=32 时间=11ms TTL=53
来自 180.101.51.73 的回复: 字节=32 时间=14ms TTL=53
```


Wireshark DNS报文抓取分析

33

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File (F), Edit (E), View (V), Go (G), Capture (C), Analyze (A), Statistics (S), Tools (T), and Help (H). The toolbar contains icons for various functions like opening files, saving, and zooming. The packet list pane on the left shows two packets: packet 10 is a DNS Standard query from 192.168.1.6 to 192.168.1.1, and packet 11 is a DNS Standard query response from 192.168.1.1 to 192.168.1.6. Packet 11 is selected. The packet details pane on the left shows the structure of the DNS response, including the Transaction ID (0xd04), Flags (0x8180), and various fields like Response, Opcode, Authoritative, Truncated, Recursion desired, Recursion available, Answer authenticated, Non-authenticated data, and Reply code. The packet bytes pane on the right shows the raw data of the packet in hexadecimal and ASCII.

Wireshark interface showing a DNS response packet analysis.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
10	5.636504	192.168.1.6	192.168.1.1	DNS	73	Standard query 0xd04 A www.baidu.com
11	5.649164	192.168.1.1	192.168.1.6	DNS	393	Standard query response 0xd04 A www.baidu.com CNAME www.a.shifen.com A 180.101.49.44 A 1...

Packet Details (Frame 11):

- Frame 11: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface...
- Ethernet II, Src: TaicangT_9a:7e:d4 (04:75:f9:9a:7e:d4), Dst: IntelCor_a7:24:8e (08:00:07:24:8e:04)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6
- User Datagram Protocol, Src Port: 53, Dst Port: 65104
- Domain Name System (response)
 - Transaction ID: 0xd04
 - 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
 -0 = Non-authenticated data: Unacceptable
 -0000 = Reply code: No error (0)
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 5
 - Additional RRs: 9

Packet Bytes:

Offset	Hex	ASCII
0000	f0 d5 bf a7 24 8e 04 75 f9 9a 7e d4 08 00 45 00\$.u...~...E..
0010	01 7b e0 c4 00 00 40 11 15 56 c0 a8 01 01 c0 a8	..{....@...V.....
0020	01 06 00 35 fe 50 01 67 00 00 0d 04 81 80 00 01	...5-P.g.....[... ..
0030	00 03 00 05 00 09 03 77 77 77 05 62 61 69 64 75w ww-baidu
0040	03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 00 01 00	..com.....
0050	00 02 58 00 12 03 77 77 77 01 61 06 73 68 69 66	..X...ww w-a-shif
0060	65 6e 03 63 6f 6d 00 c0 2b 00 01 00 01 00 00 02	en.com...+.....
0070	58 00 04 b4 65 31 2c c0 2b 00 01 00 01 00 00 02	X...e1,+.....
0080	58 00 04 b4 65 33 49 c0 2f 00 02 00 01 00 00 03	X...e3I./.....
0090	52 00 06 03 6e 73 35 c0 2f c0 2f 00 02 00 01 00	R...ns5././.....
00a0	00 03 52 00 06 03 6e 73 31 c0 2f c0 2f 00 02 00	..R...ns 1././...
00b0	01 00 00 03 52 00 06 03 6e 73 33 c0 2f c0 2f 00R...ns3././...
00c0	02 00 01 00 00 03 52 00 06 03 6e 73 34 c0 2f c0R...ns4./...
00d0	2f c0 02 00 01 00 00 03 52 00 06 03 6e 73 32 c0	/.....R...ns2...
00e0	2f c0 9f 00 01 00 01 00 00 00 4d 00 04 0e d7 b1	/.....M.....
00f0	e5 c0 9f 00 01 00 01 00 00 00 4d 00 04 0f 14 04M.o...
0100	1c c0 69 00 01 00 01 00 00 01 66 00 04 b4 4c 4c	..i.....f...LL
0110	5f c0 7b 00 01 00 01 00 00 01 0b 00 04 6e f2 44	_{.....n.D
0120	2a c0 b1 00 01 00 01 00 00 01 b0 00 04 dc b5 21	*.....!.....
0130	20 c0 8d 00 01 00 01 00 00 00 4d 00 04 24 9b 84M.\$...
0140	0c c0 8d 00 01 00 01 00 00 00 4d 00 04 99 03 eeM.....
0150	a2 c0 69 00 1c 00 01 00 00 01 fe 00 10 24 0e 00	..i.....\$...
0160	bf b8 01 10 06 00 00 00 ff b0 4f 34 6b c0 69 0004k.i...
0170	1c 00 01 00 00 01 fe 00 10 24 0e 09 40 06 03 00\$.@...
0180	0a 00 00 00 ff b0 8d 23 9d#...

Do query recursively? (dns.flags.recdesired), 2 byte(s)

分组: 29 · 已显示: 2 (6.9%) · 已丢弃: 0 (0.0%) 配置: Default

文件C:\Windows\System32\drivers\etc\hosts

34

```
hosts - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
8.8.8.8 www.baidu.com
```

添加一行

注意：可能部分系统需要管理员权限才能更改hosts文件内容

```
C:\Users\jiang>ping www.baidu.com
```

```
正在 Ping www.baidu.com [8.8.8.8] 具有 32 字节的数据:
来自 8.8.8.8 的回复: 字节=32 时间=29ms TTL=128
来自 8.8.8.8 的回复: 字节=32 时间=29ms TTL=128
来自 8.8.8.8 的回复: 字节=32 时间=29ms TTL=128
来自 8.8.8.8 的回复: 字节=32 时间=29ms TTL=128
```

```
8.8.8.8 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 = 29ms, 最长 = 29ms, 平均 = 29ms
```

实验分析讨论

- 1.分析在Packet tracer中DNS报文情况;
- 2.打开WireShark, 抓取DNS数据包, 查看DNS报文各字段内容, 并解读

A, WireShark开始捕捉->打开“命令提示符”并查询本机IP ->再运行“ping www.baidu.com”->结束捕捉。

B, 修改hosts文件-> WireShark开始捕捉->运行“ping www.baidu.com”->结束捕捉。

C, WireShark开始捕捉->运行“ping www.abc123.com(或任何一个不存在的网址)”->结束捕捉(对比ping一个已知网址过程的差别)