

# DNS实验

同济大学软件学院

# DNS原理

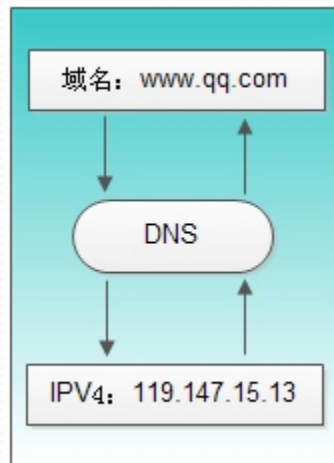
## 1. DNS的概述

为什么需要DNS解析域名为IP地址？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。我们无法记住10个以上IP地址的网站，所以我们访问网站时，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”的计算机自动把我们的域名“翻译”成了相应的IP地址，然后调出IP地址所对应的网页。



# DNS原理

具体什么是DNS? 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。DNS就是这样的一位“翻译官”, 它的基本工作原理可用下图来表示为什么需要DNS解析域名为IP地址?



# DNS原理

## 2. DNS的过程

DNS是应用层协议，事实上他是为其他应用层协议工作的，包括不限于HTTP和SMTP以及FTP，用于将用户提供的主机名解析为ip地址。具体过程如下：

- ①用户主机上运行着DNS的客户端，就是我们的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，就是访问的主机名，比如http://www.baidu.com/，并将这个主机名传送给DNS应用的客户端



## 2. DNS的过程

- ③DNS客户端向DNS服务器端发送一份查询报文，报文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客户端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。

## 2. DNS的过程

- ③DNS客户端向DNS服务器端发送一份查询报文，报文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客户端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。

## 3. DNS服务的体系架构

DNS domain name system 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的客户机端，并指明需要被转换的主机名。（在很多基于UNIX的机器上，应用程序为了执行这种转换需要调用函数 `gethostbyname()` ）。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。



## 3. DNS服务的体系架构

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。



## 3. 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，但他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（故障一个，全球着急）。

## 3. 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。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原理

## 3. DNS分布式集群工作方式



图2-19 DNS服务器的部分层次结构



## 4. DNS域名称

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。

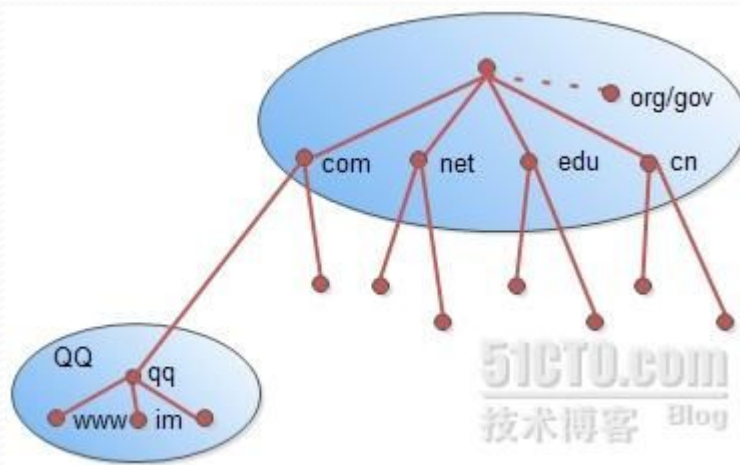
DNS数据库中的名称形成一个分层树状结构称为域命名空间。域名包含单个标签分隔点，例如：im.qq.com完全限定的域名 (FQDN) 唯一地标识在 DNS 分层树中的主机的位置，通过指定的路径中点分隔从根引用的主机的名称列表。下图显示与主机称为 im 内qq.com DNS 树的示例。



# DNS原理

## 4. DNS域名称

主机的 FQDN 是 im.qq.com DNS 域的名称  
层次结构



## 4. 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 域名称的五个类别的介绍详见下表中，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

## 4. DNS域名称空间的组织方式

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下表所示。一些常见的DNS域名称如下图：

DNS域名称	组织类型
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
xx	国家/地区代码 (cn表中国)
...	...



## 5. 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。我们在建立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见下图：

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





## 6. 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。

## 6. DNS服务的工作过程

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。

## 6. DNS服务的工作过程

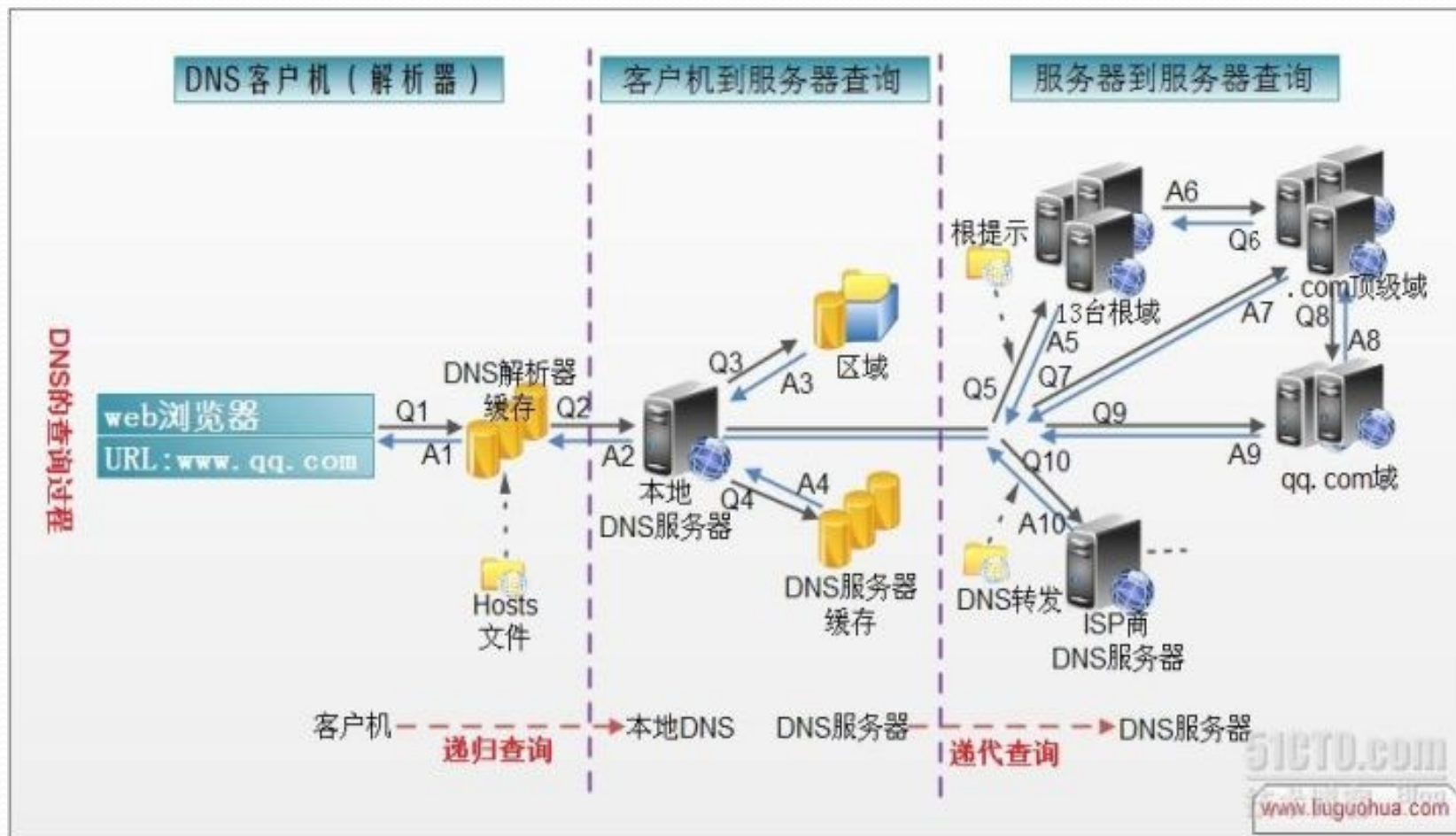
另外，客户机自己也可尝试联系其他的 DNS 服务器来解析名称。如果客户机这么做，它会使用基于服务器应答的独立和附加的查询，该过程称作迭代，即DNS服务器之间的交互查询就是迭代查询。

DNS 查询的过程如下图所示。



# DNS原理

## 6. DNS服务的工作过程





# DNS原理

## 6. DNS服务的工作过程

- 1) 在浏览器中输入www.qq.com 域名，操作系统会先检查自己本地的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。
- 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，在此我们叫它本地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。

# DNS原理

## 6. DNS服务的工作过程

- 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。
- 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，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。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://qq.com>)给本地DNS服务器。

# DNS原理

## 6. DNS服务的工作过程

5) 当本地DNS服务器收到这个地址后，就会找http://qq.com域服务器，重复上面的动作，进行查询，直至找到www.qq.com主机。

6) 如果用的是转发模式，此DNS服务器就会把请求转发至上一级DNS服务器，由上一级服务器进行解析，上一级服务器如果不能解析，或找根DNS或把转请求转至上上级，以此循环。不管是本地DNS服务器用是是转发，还是根提示，最后都是把结果返回给本地DNS服务器，由此DNS服务器再返回给客户机。

从客户端到本地DNS服务器是属于递归查询，而DNS服务器之间就是的交互查询就是迭代查询。



## 7. DNS域名解析顺序

### 1) 浏览器缓存

当用户通过浏览器访问某域名时，浏览器首先会在自己的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）；

### 2) 系统缓存

当浏览器缓存中无域名对应IP则会自动检查用户计算机系统Hosts文件DNS缓存是否有该域名对应IP；

### 3) 路由器缓存

当浏览器及系统缓存中均无域名对应IP则进入路由器缓存中检查，以上三步均为客服端的DNS缓存；

### 4) ISP（互联网服务提供商）DNS缓存

当在用户客服端查找不到域名对应IP地址，则将进入ISP DNS缓存中进行查询。比如你用的是电信的网络，则会进入电信的DNS缓存服务器中进行查找；



## 6. DNS域名解析顺序

### 5) 根域名服务器

当以上均未完成，则进入根服务器进行查询。全球仅有13台根域名服务器，1个主根域名服务器，其余12为辅根域名服务器。根域名收到请求后会查看区域文件记录，若无则将其管辖范围内顶级域名（如.com）服务器IP告诉本地DNS服务器；

### 6) 顶级域名服务器

顶级域名服务器收到请求后查看区域文件记录，若无则将其管辖范围内主域名服务器的IP地址告诉本地DNS服务器；

## 6. DNS域名解析顺序

### 7) 主域名服务器

主域名服务器接受到请求后查询自己的缓存，如果没有则进入下一级域名服务器进行查找，并重复该步骤直至找到正确纪录；

### 8) 保存结果至缓存

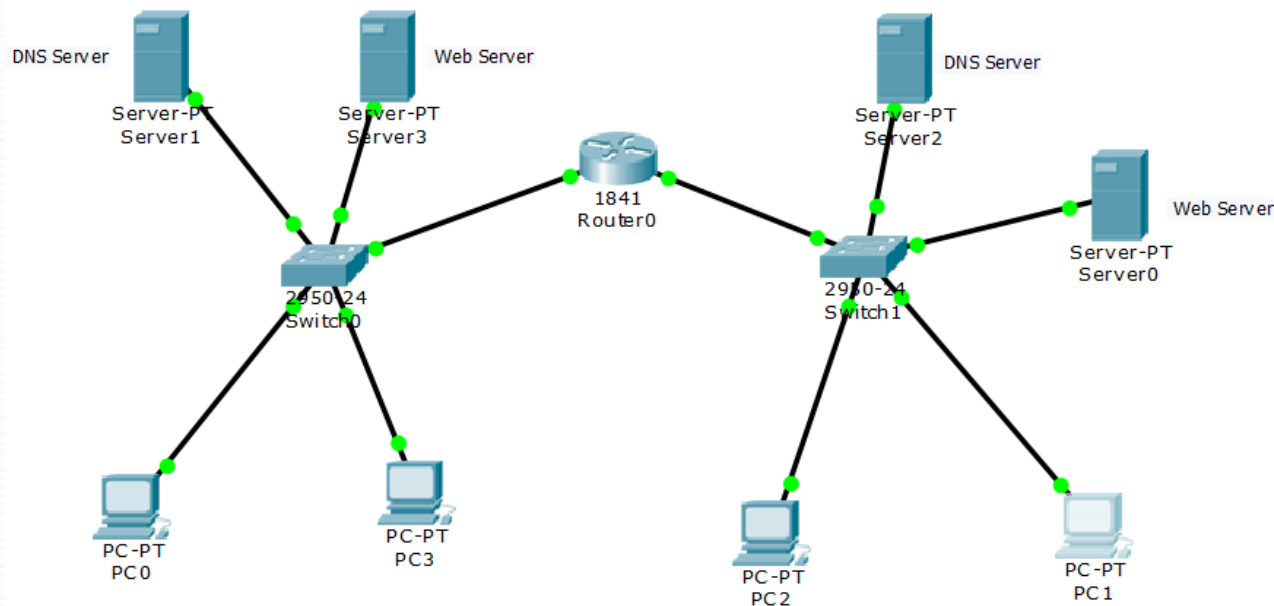
本地域名服务器把返回的结果保存到缓存，以备下一次使用，同时将该结果反馈给客户端，客户端通过这个IP地址与web服务器建立链接。

# DNS数据

## 7.Packet Tracer 分析DNS

### 网络结构图

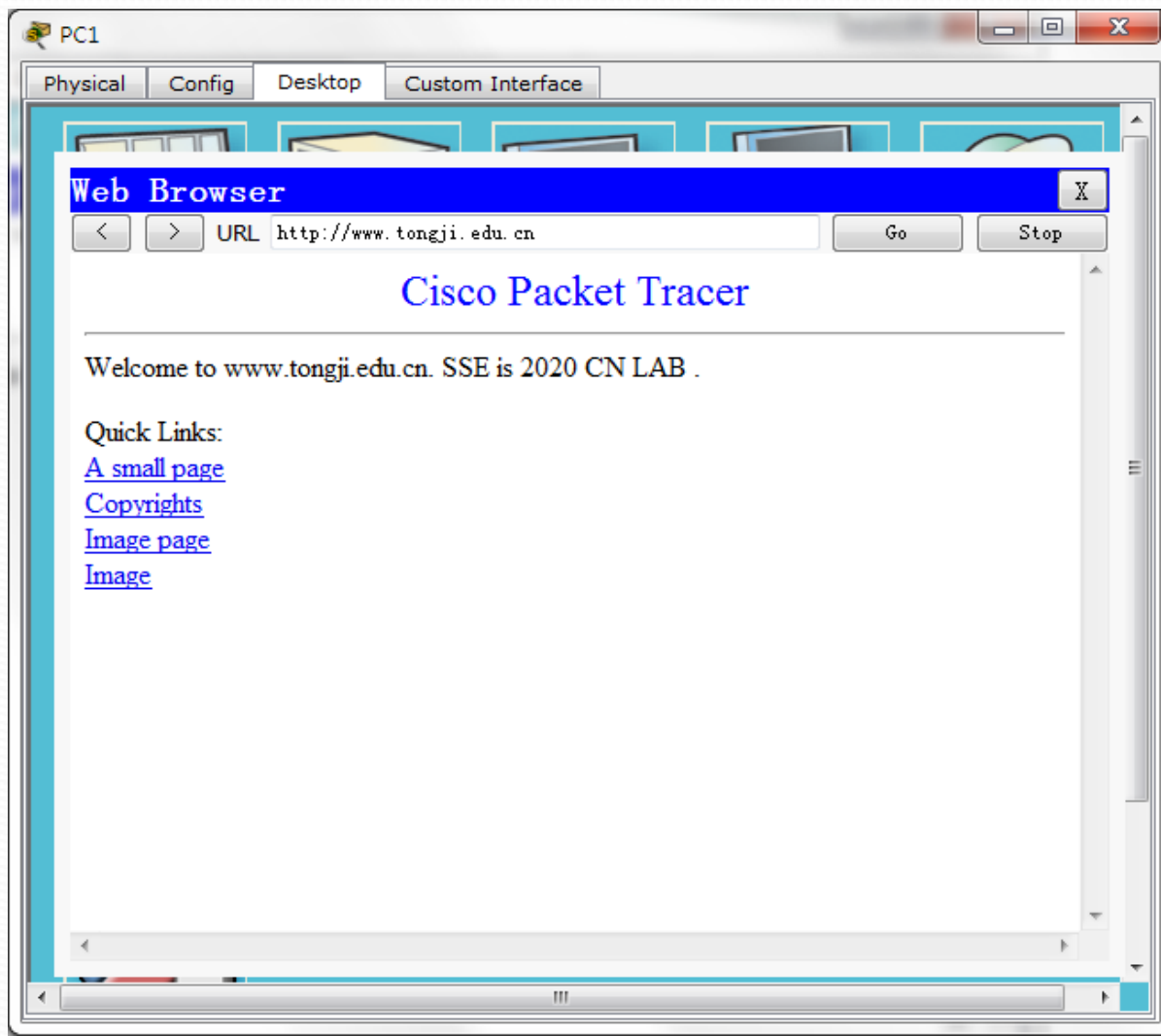
1) 设置WEB服务器和简单的DNS服务器； 2) 打开PC0浏览器，输入配置Web服务器的Web地址，如www.tongji.edu.cn,产生TCP数据报文。





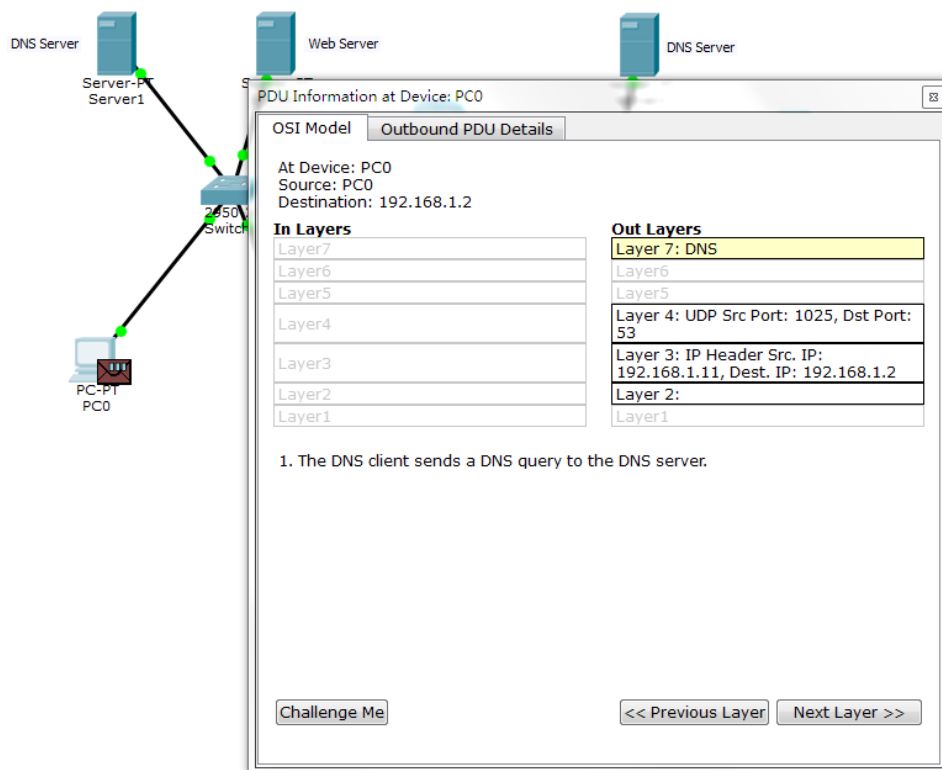
# DNS数据报文

## 7. Packet Tracer 分析报文 PC1 WEB Browser

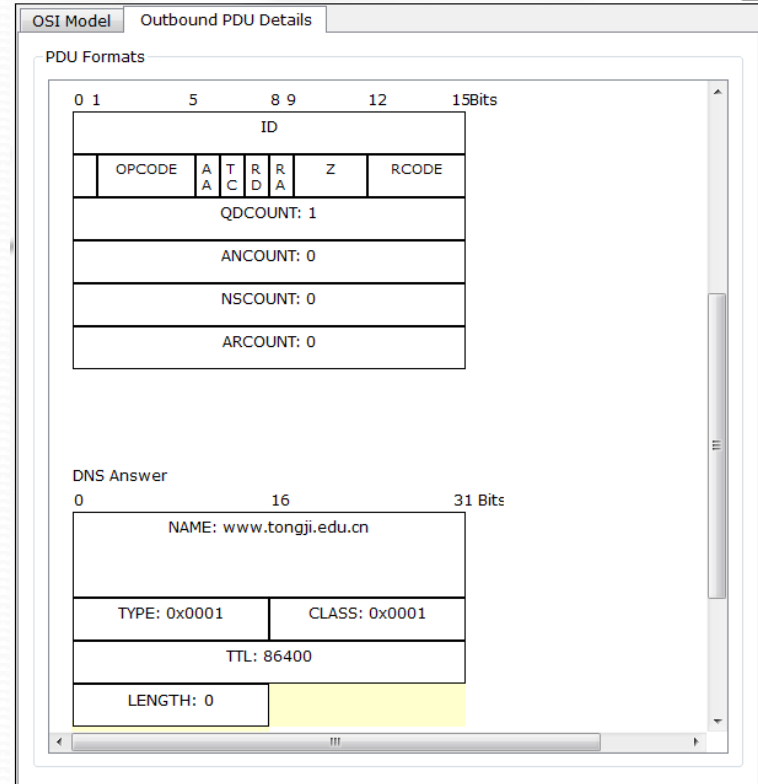


# DNS数据

## 7.Packet Tracer 分析DNS

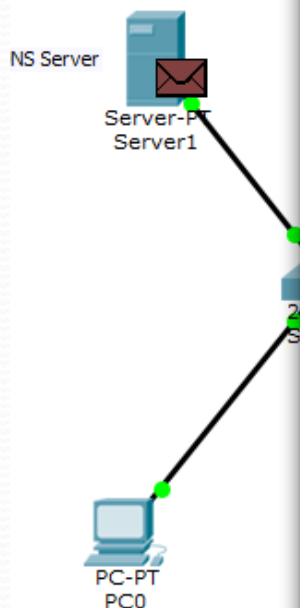


PDU Information at Device: PC0



# DNS数据

## 7.Packet Tracer 分析DNS



PDU Information at Device: Server1

OSI Model   Inbound PDU Details   Outbound PDU Details

At Device: Server1  
Source: PC0  
Destination: 192.168.1.2

**In Layers**

Layer 7: DNS
Layer 6
Layer 5
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: Ethernet II Header 0050.0FAB.0418 >> 00E0.8FB6.9970
Layer 1: Port FastEthernet0

**Out 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(s): FastEthernet0

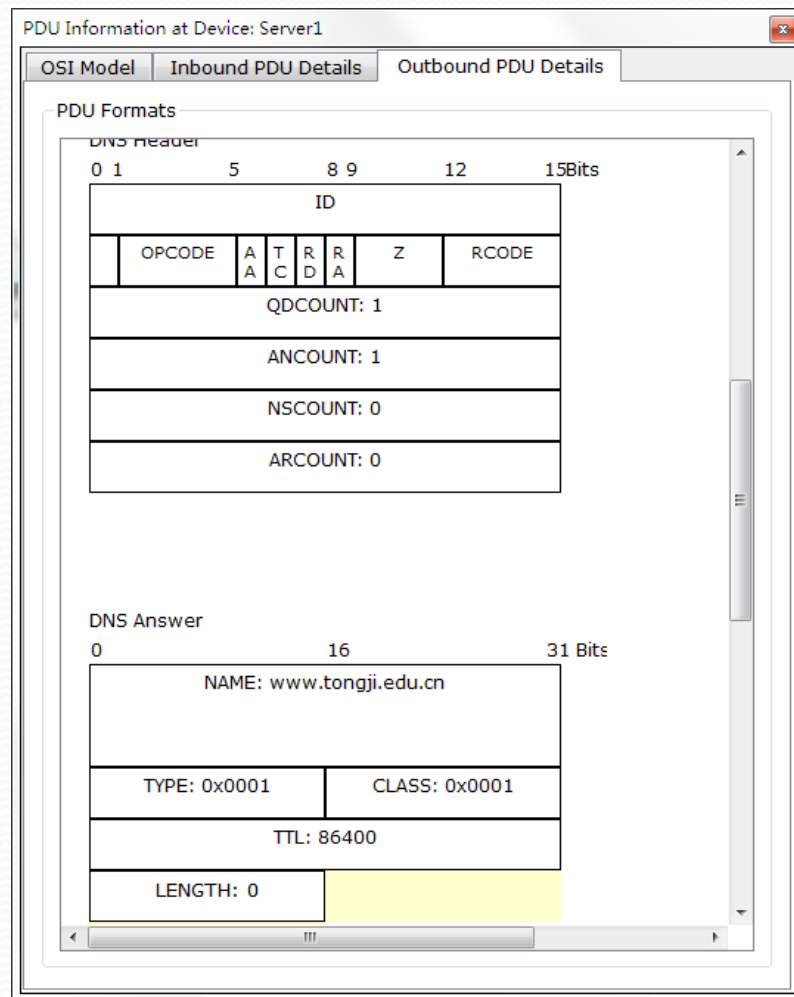
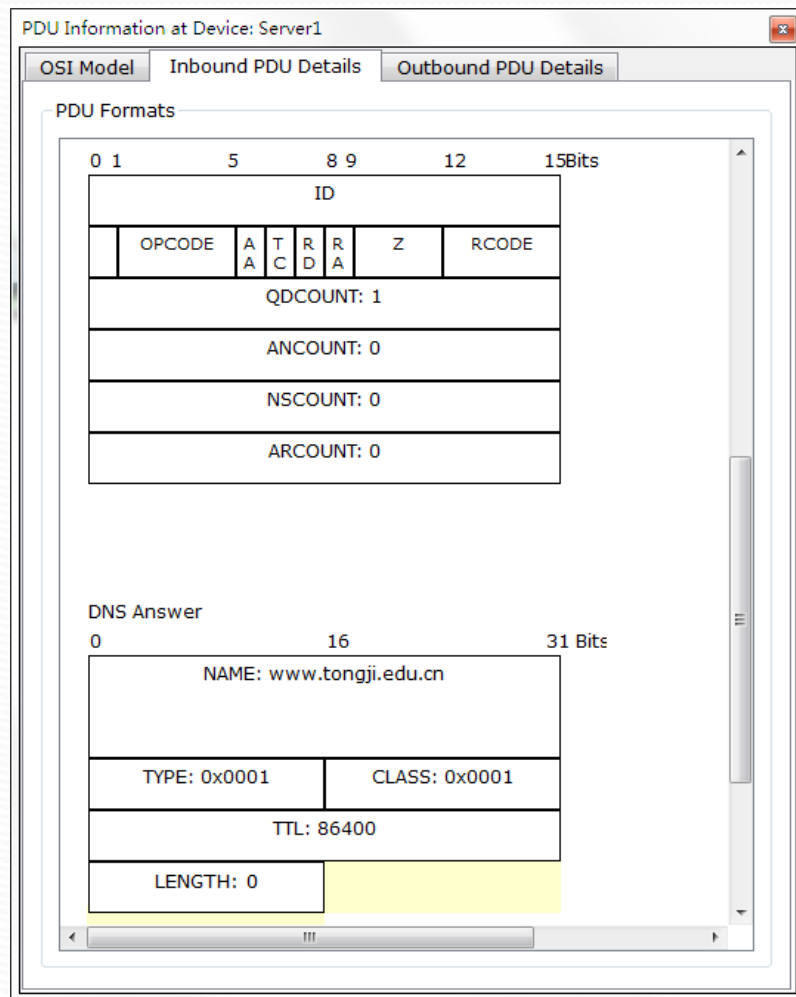
1. FastEthernet0 receives the frame.

Challenge Me   << Previous Layer   Next Layer >>



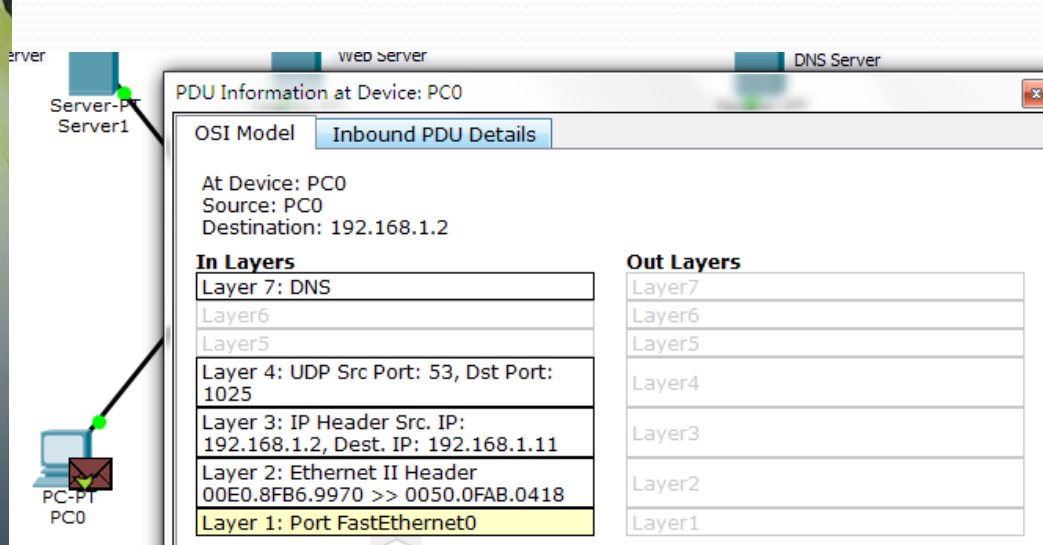
# DNS数据

## 7.Packet Tracer 分析DNS



# DNS数据

## 7.Packet Tracer 分析DNS



server

web Server

DNS Server

Server-PT  
Server1

PC-PT  
PC0

PDU Information at Device: PC0

OSI Model Inbound PDU Details

At Device: PC0  
Source: PC0  
Destination: 192.168.1.2

**In Layers**

Layer 7: DNS
Layer6
Layer5
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**

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

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		

## 7.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

### 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



# 8. Wireshark DNS报文抓取分析

Capturing from Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: dns Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
8638	43.475002	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query A po.im.alisoft.com
8639	43.485812	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response, No such name
10081	59.041782	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query A qbwup.imtt.qq.com
10082	59.049077	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME bench.mig.tencent-cloud.net CNAME httpb-wup.ias.tencent-cloud.net A 120.204.10.176
10083	59.049315	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query AAAA qbwup.imtt.qq.com
10085	59.057491	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME bench.mig.tencent-cloud.net CNAME httpb-wup.ias.tencent-cloud.net
13282	71.762309	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query A image.sinajs.cn
13283	71.767188	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME imagesinajs.gslb.sinaedge.com CNAME kln.grid.sinaedge.com A 112.25.53.216
13284	71.767461	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query AAAA image.sinajs.cn
13285	71.771346	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME imagesinajs.gslb.sinaedge.com CNAME kln.grid.sinaedge.com AAAA 2409:8c20:a12:4ff::200:76
21807	114.600165	192.168.1.4	224.0.0.251	MDNS	Standard query PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.local, "QU" question PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local
21808	114.600166	fe80::10d9:6638:dd96:db8c	ff02::fb	MDNS	Standard query PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.local, "QU" question PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local
21819	115.624089	192.168.1.4	224.0.0.251	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.local
21820	115.624091	fe80::10d9:6638:dd96:db8c	ff02::fb	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.local
21827	118.695850	192.168.1.4	224.0.0.251	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.local

Frame 10083: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)

Ethernet II, Src: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2), Dst: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)

Internet Protocol Version 6, Src: fe80::65b1:5003:1e0f:6db4 (fe80::65b1:5003:1e0f:6db4), Dst: fe80::1 (fe80::1)

User Datagram Protocol, Src Port: 60327 (60327), Dst Port: domain (53)

Domain Name System (query)

Response In: 10081

Transaction ID: 0x35de

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

- qbwap.imtt.qq.com: type AAAA, class IN
  - Name: qbwup.imtt.qq.com
  - Type: AAAA (IPv6 address)
  - Class: IN (0x0001)

# 8. Wireshark DNS报文抓取分析

Capturing from Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: dns Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
10081	59.041782	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query A qbwup.imtt.qq.com
10082	59.049077	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME bench.mig.tencent-cloud.net CNAME http1b-wup.ias.tencent-cloud.net A 120.204.10.176
10083	59.049315	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query AAAA qbwup.imtt.qq.com
10085	59.057491	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME bench.mig.tencent-cloud.net CNAME http1b-wup.ias.tencent-cloud.net
13282	71.762309	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query A image.sinajs.cn
13283	71.767188	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME imagesinajs.gslb.sinaedge.com CNAME kln.grid.sinaedge.com A 112.25.53.216
13284	71.767461	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query AAAA image.sinajs.cn
13285	71.771346	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME imagesinajs.gslb.sinaedge.com CNAME kln.grid.sinaedge.com AAAA 2409:8c20:a12:4ff::200:76
21807	114.600165	192.168.1.4	224.0.0.251	MDNS	Standard query PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.local, "QU" question PTR _airplay._tcp.local, "QU" question PTR _raop
21808	114.600166	192.168.1.4	ff02::fb	MDNS	Standard query PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.local, "QU" question PTR _airplay._tcp.local, "QU" question PTR _raop
21819	115.624089	192.168.1.4	224.0.0.251	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop
21820	115.624091	192.168.1.4	ff02::fb	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop
21827	118.695850	192.168.1.4	224.0.0.251	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop
21828	118.695851	192.168.1.4	ff02::fb	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop

Frame 10085: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits)

- Ethernet II, Src: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29), Dst: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::65b1:5003:1e0f:6db4 (fe80::65b1:5003:1e0f:6db4)
- User Datagram Protocol, Src Port: domain (53), Dst Port: 60327 (60327)
- Domain Name System (response)
  - Request in: 10083
  - [Time: 0.008176000 seconds]
  - Transaction ID: 0x35de
  - 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
    - ... 0... .. = Non-authenticated data: Unacceptable
    - ... 0000 = Reply code: No error (0)
  - Questions: 1
  - Answer RRs: 2
  - Authority RRs: 1
  - Additional RRs: 0
  - Queries
    - qbwup.imtt.qq.com: type AAAA, class IN
      - Name: qbwup.imtt.qq.com
      - Type: AAAA (IPv6 address)
      - Class: IN (0x0001)
  - Answers
    - qbwup.imtt.qq.com: type CNAME, class IN, cname bench.mig.tencent-cloud.net
    - bench.mig.tencent-cloud.net: type CNAME, class IN, cname http1b-wup.ias.tencent-cloud.net
      - Name: bench.mig.tencent-cloud.net
      - Type: CNAME (Canonical name for an alias)
      - Class: IN (0x0001)
      - Time to live: 6 minutes, 52 seconds
      - Data length: 17
      - Primary name: http1b-wup.ias.tencent-cloud.net
  - Authoritative nameservers
    - tencent-cloud.net: type SOA, class IN, mname ns-open1.qq.com

# 实验主要分析内容

1. 分析在Packet tracer中DNS报文情况;
2. 用WireShark抓取DNS数据包;
3. 查看DNS报文字段内容, 并解读;