



西安电子科技大学网信院

《组网与运维》

线上实验报告

班级：

姓名：

学号：

日期：

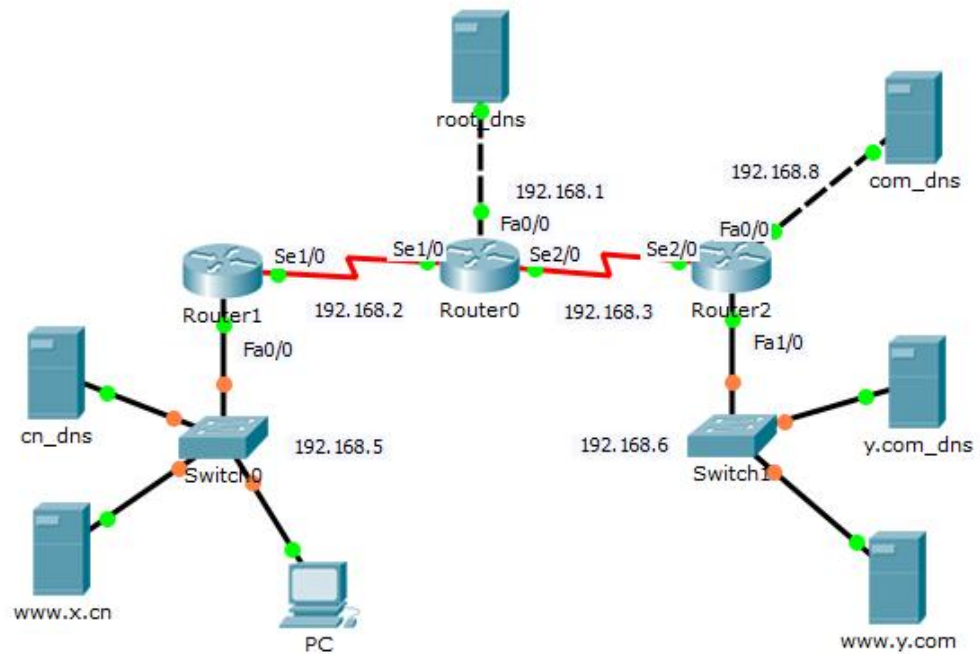
7. DNS解析实验

一、实验目的

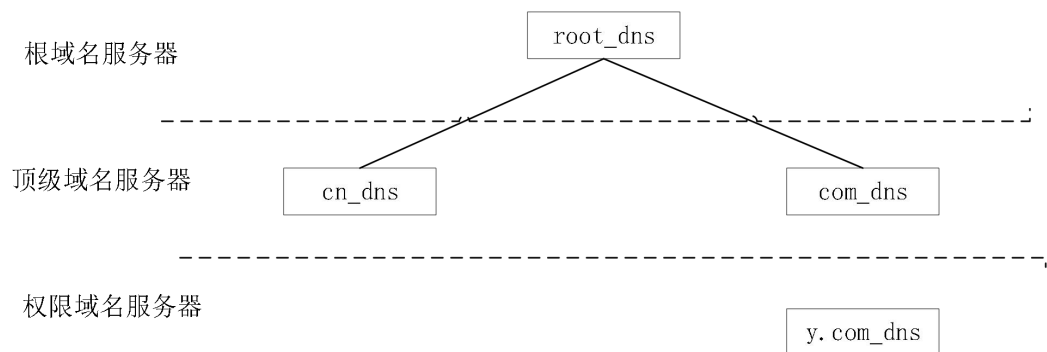
1. 理解 DNS 系统的工作原理。
2. 熟悉 DNS 服务器的工作过程。
3. 熟悉 DNS 报文格式。
4. 理解 DNS 缓存的作用。

二、实验步骤

1. 给出实验中用到的拓扑图



2. 绘制 DNS 域名服务器层次结构

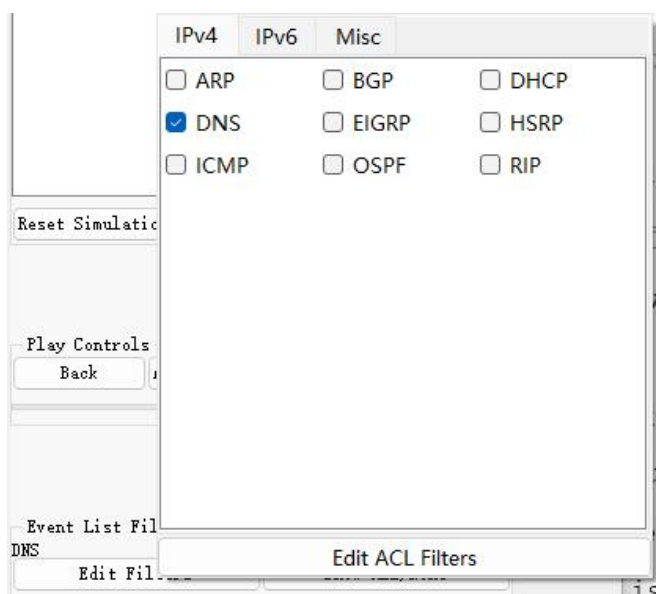


3. 任务一：观察本地域名解析过程

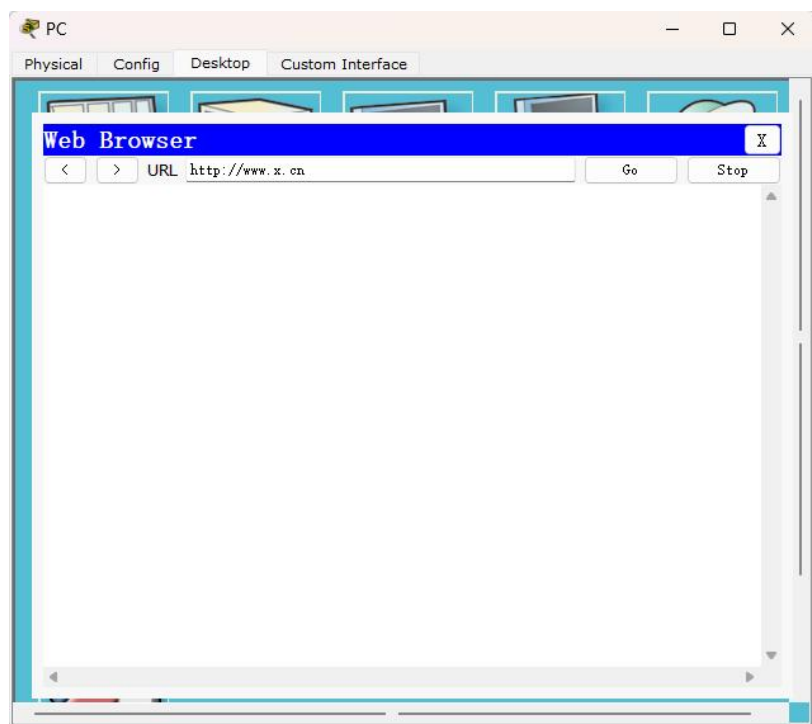
✧ 步骤一：在 PC 的浏览器窗口请求内部 Web 服务器的网页。

选择 Simulation（模拟）选项卡，进入模拟模式。

在 Event List Filters（事件列表过滤器）区域中单击 Edit Filters（编辑过滤器）按钮，仅选择 DNS 事件。



单击逻辑工作空间中的 PC，在 Desktop（桌面）选项卡中打开 Web Browser（Web 浏览器），在 URL 框中输入 www.x.cn，然后单击 Go（转到）按钮。最小化模拟浏览器窗口。

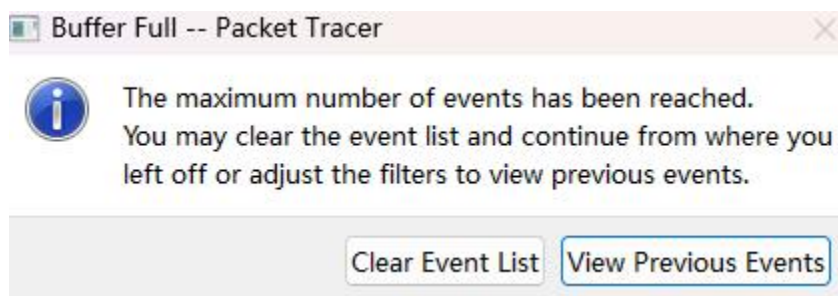


✧ 步骤 2: 捕获 DNS 事件并分析本地域名解析过程。

在 Simulation Panel (模拟面板) 中单击 Auto Capture/Play (自动捕获/播放) 按钮, 此时会播放 PC 与 Server 之间的数据包交换动画, 并且相关的事件会被添加到 Event List (事件列表) 中。

Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC	DNS	
	0.005	--	PC	DNS	
	0.007	--	PC	DNS	
	0.008	PC	Switch0	DNS	
	0.009	Switch0	cn_dns	DNS	
	0.010	cn_dns	Switch0	DNS	
	0.011	Switch0	PC	DNS	

捕获结束时将会出现一个 Buff Full (缓冲区满) 的对话框, 该对话框提示已达到事件数量的最大值, 该对话框中有两个按钮: Clear Event List (清除事件列表) 和 View Previous Events (查看历史事件), 单击 View Previous Events (查看历史事件) 按钮关闭对话框。



在 Event List (事件列表) 区域中单击 info (信息) 列中的某个 DNS 事件的单色框, 将会打开相应的 PDU Information (PDU 信息) 窗口。本步骤需要查看该窗口 OSI Model (OSI 模型) 选项卡中 In Layers (入站) 和 Out Layer (出站) 的 Layer 7 (第 7 层) 的信息, 以及 Inbound/Outbound PDU Details (入站/出站 PDU 详细数据) 选项卡中第 7 层的 PDU 信息。

PDU Information at Device: cn_dns x

OSI Model

Inbound PDU Details

Outbound PDU Details

At Device: cn_dns
Source: PC
Destination: 192.168.5.1

In Layers

Layer 7: DNS
Layer 6
Layer 5
Layer 4: UDP Src Port: 1025, Dst Port: 53
Layer 3: IP Header Src. IP: 192.168.5.12, Dest. IP: 192.168.5.1
Layer 2: Ethernet II Header 0010.1121.63E3 >> 0060.5C5E.0751
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: 192.168.5.1, Dest. IP: 192.168.5.12
Layer 2: Ethernet II Header 0060.5C5E.0751 >> 0010.1121.63E3
Layer 1: Port(s): FastEthernet0

1. The DNS server receives a DNS query.
2. The name queried resolved locally

PDU Information at Device: cn_dns x

OSI Model

Inbound PDU Details

Outbound PDU Details

At Device: cn_dns
Source: PC
Destination: 192.168.5.1

In Layers

Layer 7: DNS
Layer 6
Layer 5
Layer 4: UDP Src Port: 1025, Dst Port: 53
Layer 3: IP Header Src. IP: 192.168.5.12, Dest. IP: 192.168.5.1
Layer 2: Ethernet II Header 0010.1121.63E3 >> 0060.5C5E.0751
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: 192.168.5.1, Dest. IP: 192.168.5.12
Layer 2: Ethernet II Header 0060.5C5E.0751 >> 0010.1121.63E3
Layer 1: Port(s): FastEthernet0

1. The DNS server finds a domain with this name. It sends back a response.

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0060.5C5E.0751		SRC MAC: 0010.1121.63E3	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 52			
ID: 0x4			0x0	0x0		
TTL: 128		PRO: 0x11	CHKSUM			
SRC IP: 192.168.5.12						
DST IP: 192.168.5.1						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

0	16	31	Bits
SRC PORT: 1025		DEST PORT: 53	
LENGTH: 0x20		CHECKSUM: 0x0	
DATA (VARIABLE)			

DNS Header

0	1	5	8	9	12	15	Bits
ID							
	OPCODE		A	T	R	R	Z
			A	C	D	A	
QDCOUNT: 1							
ANCOUNT: 0							
NSCOUNT: 0							
ARCOUNT: 0							

DNS Answer

0	16	31 Bits
NAME: www.x.cn		
TYPE: 0x0001		CLASS: 0x0001
TTL: 86400		
LENGTH: 0		

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0010.1121.63E3		SRC MAC: 0060.5C5E.0751	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 74			
ID: 0x1			0x0	0x0		
TTL: 128		PRO: 0x11	CHKSUM			
SRC IP: 192.168.5.1						
DST IP: 192.168.5.12						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

0	16	31	Bits
SRC PORT: 53		DEST PORT: 1025	
LENGTH: 0x36		CHECKSUM: 0x0	
DATA (VARIABLE)			

DNS Header

0	1	5	8	9	12	15	Bits
ID							
	OPCODE	A A	T C	R D	R A	Z	RCODE
QDCOUNT: 1							
ANCOUNT: 1							
NSCOUNT: 0							
ARCOUNT: 0							

DNS Answer

0	16	31 Bits
NAME: www.x.cn		
TYPE: 0x0001		CLASS: 0x0001
TTL: 86400		
LENGTH: 0		

本地 DNS 服务器的解析过程大致如下：

①由于 PC 中设置了 DNS 服务器的地址为 192.168.2.1，因此，当 PC 输入域名 www.x.cn 请求网页时，它将作为 DNS 客户端向本地域名服务器 cn_dns 发送一个 DNS 查询请求，请求域名 www.x.cn 的 IP 地址。

②本地域名服务器 cn_dns 收到 PC 的 DNS 查询请求后，首先尝试在本地区域文件查找，发现确实存在相应的资源记录，于是将域名 www.x.cn 对应的 IP 地址 192.168.5.1 放入 DNS 的应答报文发送给 PC。

③PC 收到本地域名服务器 cn_dns 的应答报文后，取出报文中解析出的 IP 地址 192.168.5.1，并对其进行访问，此时在 Web Browser（Web 浏览器）中显示相应的 Web 页面。

注意分析以下几项内容：

- DNS 的响应报文的组成。
- DNS 首部中的查询记录数(QDCOUNT)及应答记录数(ANCOUNT)。
- DNS QUERY（DNS 查询）及 DNS ANSWER（DNS 应答）部分各字段的值及含义。

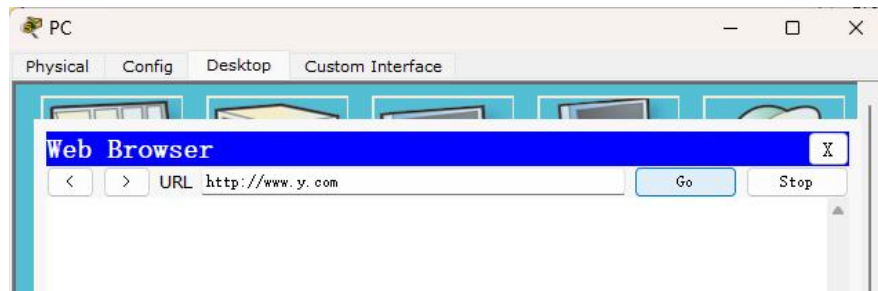
完成后单击 Reset Simulation（重置模拟）按钮，将原有的事件全部清空；同时关闭 PC 的 Web Browser（Web 浏览器）窗口。

4. 任务二：观察外网域名解析过程

✧ 步骤一：在 PC 的浏览器窗口请求外部 Web 服务器的网页。

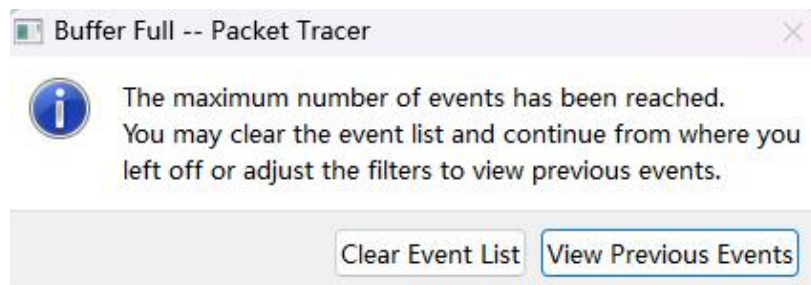
保持模拟模式中 Event List Filters（事件列表过滤器）区域的选择（仍为仅选择 DNS 事件）不变。

单击逻辑工作空间中的 PC，在 Desktop（桌面）选项卡中打开 Web Browser（Web 浏览器），在 URL 框中输入 www.y.com，然后单击 Go（转到）按钮。最小化模拟浏览器窗口。



✧ 步骤 2: 捕获 DNS 事件并分析外网域名解析过程。

在 Simulation Panel（模拟面板）中单击 Auto Capture/Play（自动捕获/播放）按钮，进行捕获，当捕获结束出现 Buff Full（缓冲区满）对话框时，单击 View Previous Events（查看历史事件）按钮，关闭对话框。



应注意重点观察解析外网域名时各级域名服务器的具体解析过程。此处可忽略路由器和交换机的转发过程，仅分析 DNS 的请求和响应报文在 DNS 服务器之间的交互情况。

DNS 服务器之间的解析过程如下：

①PC 向本地域名服务器 cn_dns 发送一个 DNS 查询请求包，请求解析域名 www. y. com。

②本地域名服务器 cn_dns 收到 PC 的 DNS 查询请求后，在本地区域文件中未找到相应的资源记录，于是 cn_dns 作为 DNS 客户端向根域名服务器 root_dns 发送 DNS 请求包，请求解析域名 www. y. com。

③根域名服务器 root_dns 收到 cn_dns 发来的 DNS 查询请求后，在本地区域文件中未能直接解析出域名 www. y. com，但找到能解析 “. com” 扩展名的顶级域名服务器 com_dns，于是 root_dns 也作为 DNS 客户端向顶级域名服务器 com_dns 发送 DNS 请求包，请求解析域名 www. y. com。

④顶级域名服务器 com_dns 收到 root_dns 发来的 DNS 查询请求后，在本地区域文件中未能直接解析出域名 www.y.com，但找到能解析“y.com”扩展名的权限域名服务器 y.com_dns，于是 com_dns 也作为 DNS 客户端向权限域名服务器 y.com_dns 发送 DNS 请求包，请求解析域名 www.y.com。

⑤权限域名服务器 y.com_dns 收到 com_dns 发来的 DNS 查询请求后，在本地区域文件中找到相应的资源记录直接解析出域名 www.y.com，于是将 IP 地址 192.168.6.2 写入 DNS 应答报文中，发送给顶级域名服务器 com_dns。

⑥com_dns 作为 DNS 客户端收到 DNS 应答报文后，取出 IP 地址 192.168.6.2，同时作为 DNS 服务器将 IP 地址写入 DNS 应答报文中，发送给根域名服务器 root_dns。

⑦root_dns 作为 DNS 客户端收到 DNS 应答报文后，取出 IP 地址 192.168.6.2，同时作为 DNS 服务器将 IP 地址写入 DNS 应答报文中，发送给本地域名服务器 cn_dns。

⑧cn_dns 作为 DNS 客户端收到 DNS 应答报文后，取出 IP 地址 192.168.6.2，同时作为 DNS 服务器将 IP 地址写入 DNS 应答报文中，发送给 PC。

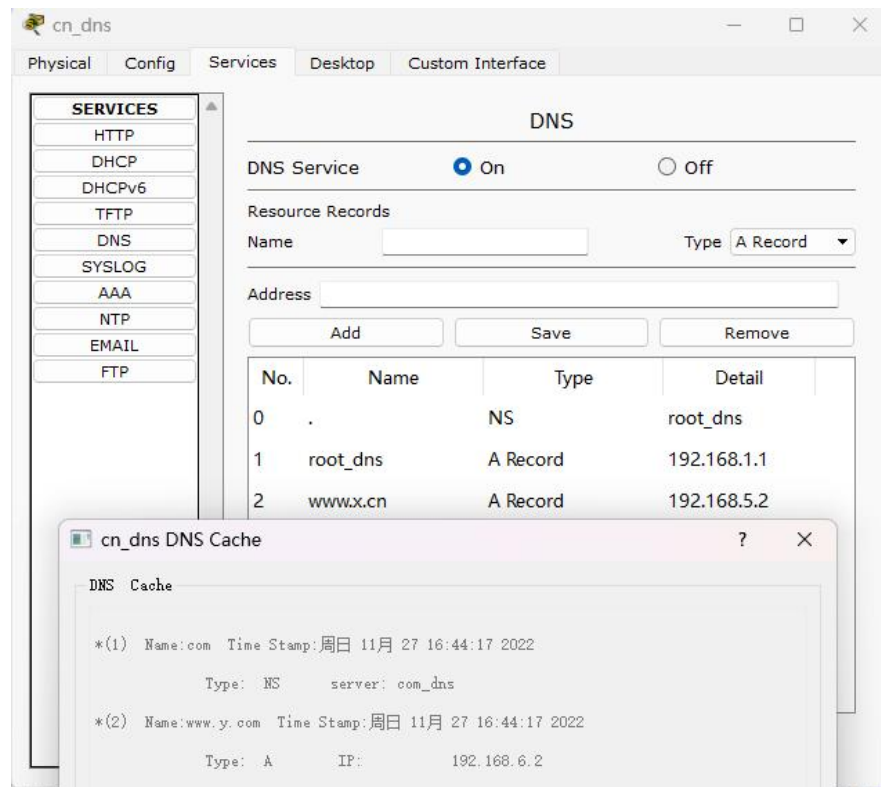
PC 收到本地域名服务器 cn_dns 的应答报文后，取出 IP 地址 192.168.6.2，并对其进行访问，此时在 Web Browser（Web 浏览器）中显示相应的 Web 页面。

完成后单击 Reset Simulation（重置模拟）按钮，将原有的事件全部清空，同时关闭 PC 的 Web Browser（Web 浏览器）窗口。

5. 任务三：观察缓存的作用

✧ 步骤一：查看本地域名服务器 cn_dns 的缓存。

单击逻辑工作空间中的本地域名服务器 cn_dns，在 Config（配置）选项卡中选择 DNS 服务，并单击页面下方的 DNS Cache（DNS 缓存）按钮，查看此时本地域名服务器 cn_dns 中的缓存。



- ✧ 步骤 2: 在 PC 的浏览器窗口请求外部 Web 服务器的网页。
重复任务二, 再次观察此次解析外网域名的过程。

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.003	--	PC	DNS	
	0.004	PC	Switch0	DNS	
	0.005	Switch0	Router1	DNS	
	0.005	Switch0	cn_dns	DNS	
	0.005	Switch0	www.x.cn	DNS	
	0.006	cn_dns	Switch0	DNS	
👁	0.007	Switch0	PC	DNS	



完成后单击 Reset Simulation (重置模拟) 按钮, 将原有的事件全部清空; 同时关闭 PC 的 Web Browser (Web 浏览器) 窗口。

三、思考与总结

1. DNS 协议使用运输层的什么协议？

答：DNS 协议使用运输层的 UDP。

2. DNS 缓存有什么作用？在 Packet Tracer 中如何清空 DNS 缓存。

答：DNS 缓存用来存放最近解析过的域名等信息，因此可以提高解析效率。若需要在 Packet Tracer 中清空某个 DNS 服务器的缓存，可以进入该 DNS 服务器的配置窗口，单击窗口下方的 DNS Cache 按钮，在弹出的窗口中单击下方的 Clear Cache 按钮即可清空 DNS 缓存。

3. 本实验中 PC 与本地域名服务器 cn_dns 之间的解析是递归还是迭代？本地域名服务器 cn_dns 与根域名服务器 root_dns 之间呢？若后者用另一种解析方法，则域名服务器之间 DNS 的请求和应答的交互过程应如何运行？

答：本实验中 PC 与本地域名服务器 cn_dns 之间的解析是递归查询，本地域名服务器 cn_dns 与根域名服务器 root_dns 之间也是递归查询。若后者用的是迭代查询，则当 cn_dns 向根域名服务器 root_dns 请求解析而 root_dns 无法解析出结果时，不是由 root_dns 全权帮助 cn_dns 直接解析出结果并将解析结果告知 cn_dns 而是 root_dns 会告诉 cn_dns 应该向哪一个域名服务器进行查询，剩下的解析由 cn_dns 自己进行。

4. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

答：通过本次实验，了解了有关 DNS 协议有关知识。