

Exp 16: 区域名称服务系统(DNS)

目的: 了解域名解析系统(DNS, Domain Name System)与UTP通讯协定的关系。

摘要: 本实验中学生可以通过UDP通讯协议传送一个DNS的询问包到DNS服务器取得网域名称详细信息, 并清楚了解到DNS解析的作业流程。除此之外也使用Windows操作系统中Command Prompt的tracert 指令进行验证。

时间: 3 小时。

一、网络拓扑

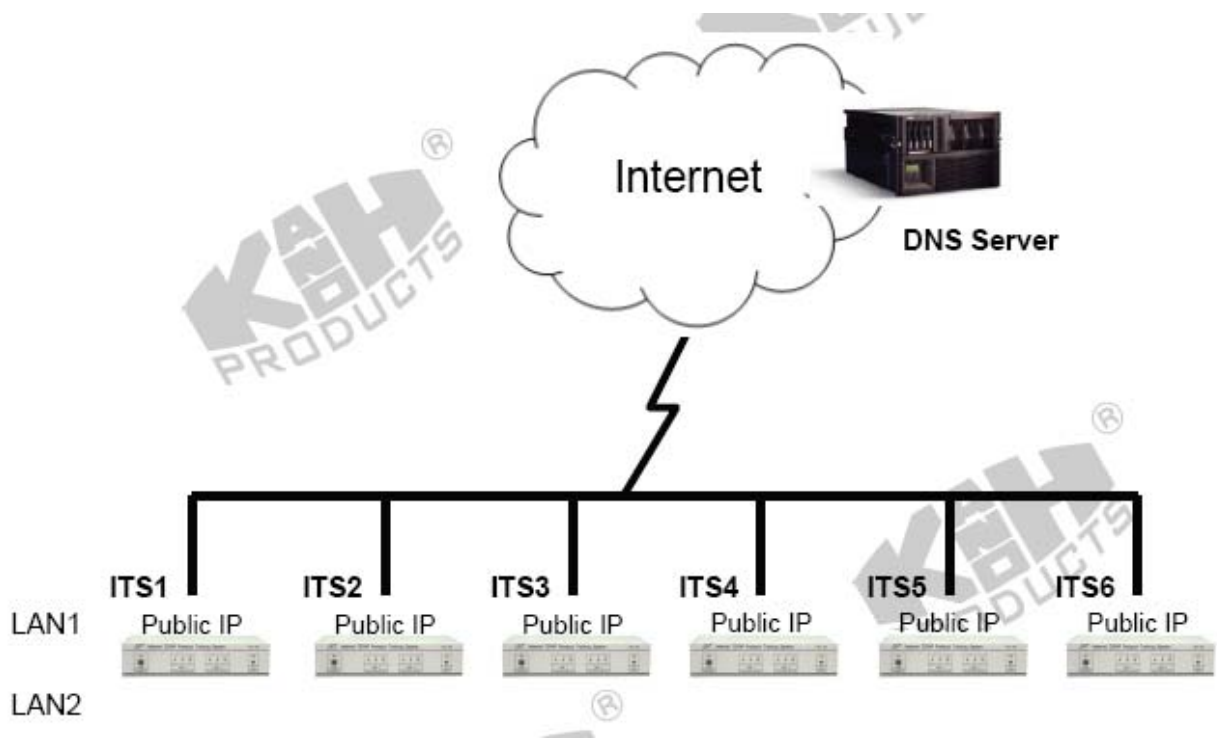


图16.1

二、技术背景

协议数据:

Protocol suite:	TCP/IP
Port:	53: TCP/UDP server.

表 16.1

数据包封装图:

MAC header	IP header	TCP/UDP header	DNS header	Data
------------	-----------	----------------	------------	------

表 16.2

网络上，当一个客户端(client)计算机传送一个网络域名询问报文给网域名称系统服务器(DNS sever)后，DNS sever会先检查这个欲查询的域名是否在自己的服务范围内。如果是，它会自行解析名称及IP 地址，并回传给client端。而如果DNS server不能解析，且client端的寻问封包是属于递归解析(recursive resolution)时，此DNS server会自动联系其它的DNS server并解析后传回。但如果client端的寻问报文是属于反复解析(iterative resolution)时，DNS server则会产生一个响应报文，说明client 端应该要自行连结到下一个DNS server做解析。

DNS 报文长度不定，其格式如下：

0	16	31
IDENTIFACATION	PARAMETER	
NUMBER OF QUESTIONS	NUMBER OF ANSWERS	
NUMBER OF AUTHORITY	NUMBER OF ADDITIONAL	
QUESTION SECTION		
...		
ANSWER SECTION		
...		
AUTHORITY SECTION		
...		
ADDITIONAL INFORMATION SECTION		
...		

表 6.3

其中PARAMETER 字段的详细说明如下：

Bits of PARAMETER field	Meaning
0	Operation: 0 Query 1 Response
1-4	Query Type: 0 Standard 1 Inverse 2 Completion 1 (now obsolete) 3 Completion 2 (now obsolete)
5	Set if Answer authoritative
6	Set if Message truncated
7	Set if Recursion desired
8	Set if Recursion available
9-11	Reserved
12-15	Response Type: 0 No error 1 Format error in query 2 Server failure 3 Name does not exist

表 6.4

而QUESTION SECTION字段又划分为三项：

0	16	31
QUERY DOMAIN NAME		
...		
QUERY TYPE		QUERY CLASS

表 6.5

QUERY DOMAIN NAME (长度不定): 欲解析的名称。下图说明了欲查询网域名称“kandh.com.tw” 在QUERY DOMAIN NAME 中的填写方式：

5	k	a	n	d	h	3	c	o	m	2	t	w	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---

表 6.6

QUERY TYPE(16 bits): 查询型态。0x01表示Query A(Address), 查询的是IP 地址, 0x0F 表示Query MX(Mail eXchange), 查询的是电子邮件送达地址。

QUERY CLASS(16 bits): 查询类别。目前仅使用IN (Internet), 其值为1。ANSWER SECTION、AUTHORITY SECTION及 ADDITIONAL INFORMATION SECTION。

字段则再细分如下:

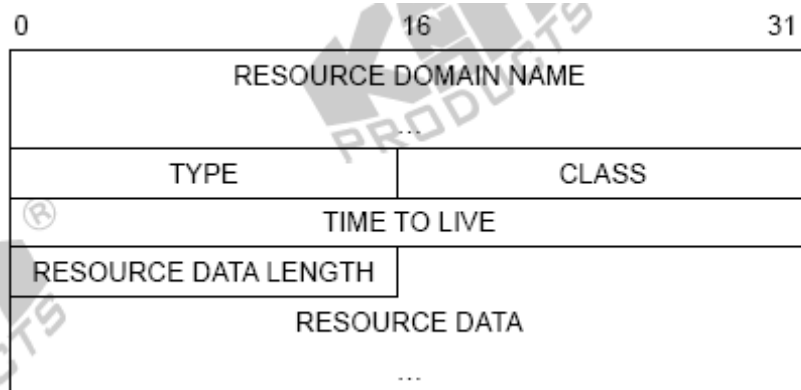


表 6.7

RESOURCE DOMAIN NAME (长度不定): 存放查询的编码压缩格式。如果前两个位为1, 则后14个位记录其DNS封包的偏移地址 (Offset)。如果前两个位为0, 则接下来的6个位则是用来填补8位的不足位置。

TYPE(16 bits): 说明此资源纪录的型态。

CLASS(16 bits): 说明网络的类别。目前仅使用IN (Internet), 其值为1。

TIME TO LIVE(32 bits): 表示此资源纪录在client 端可存活的秒数。

RESOURCE DATA LENGTH(16 bits): 纪录资源数据 (Resource Data) 的资料长度, 长度以Byte为单位。

RESOURCE DATA(长度不定): 存放查询的结果。

三、实验步骤

1、拓扑结构

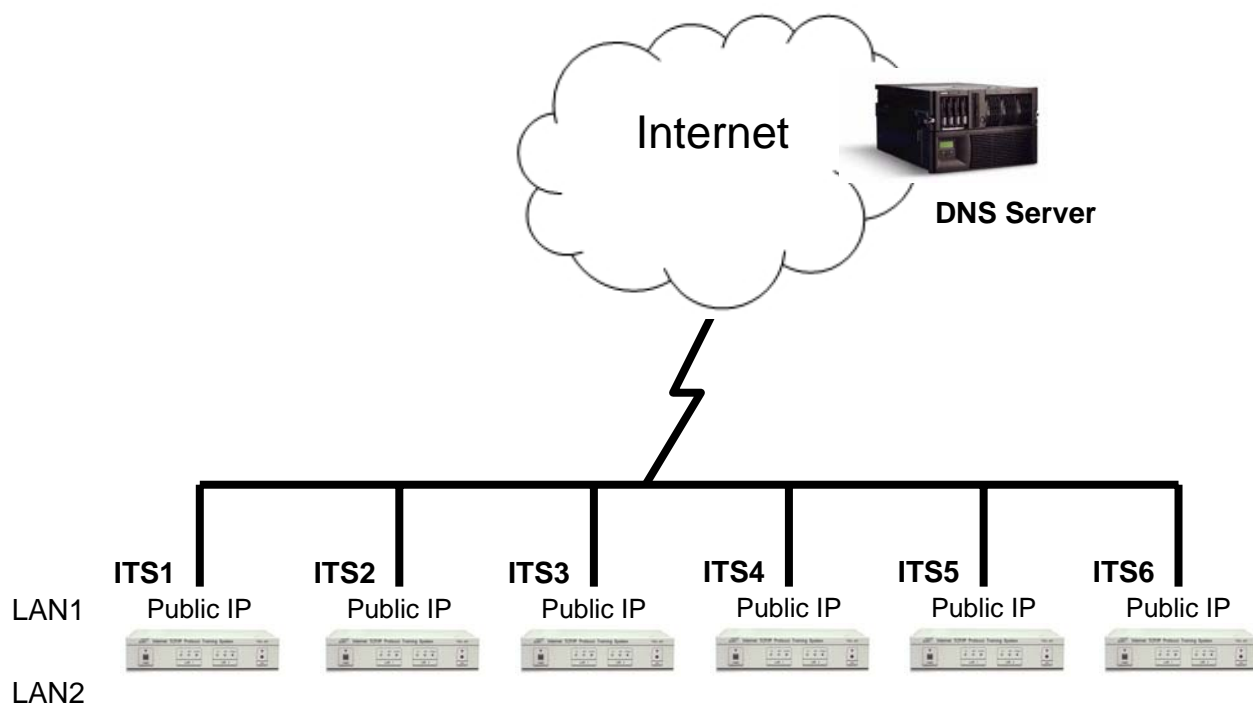


图 16.2

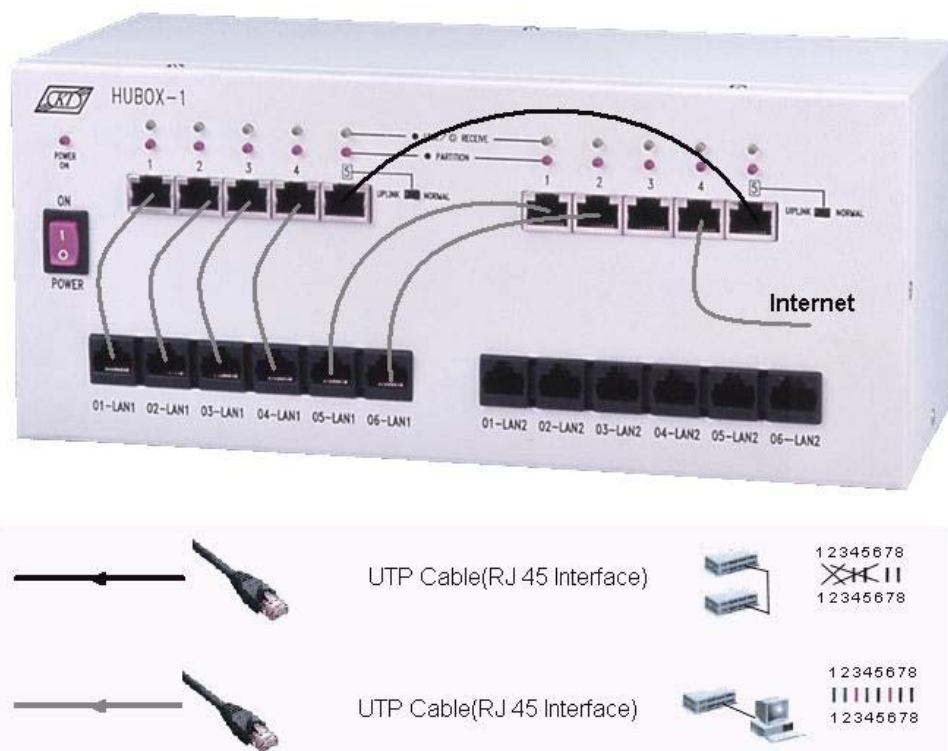


图 16.3

A. 前期设置

- 1) 执行 **XCLIENT.BAT**，打开 ITS 应用软件 KCodes Network Explorer。
- 2) 打开网络封包浏览器 Network Message Browser。
- 3) 在网络封包浏览器 Network Message Browser 界面中，选择“**Option**”打开“**Set Message Range**”对话框，见图 16.4。
- 4) 点击“**Add new rule**”按钮。你需要设定两个参数用于观察封包。首先，在 Remote Port 中定义“53”，然后点击“**Apply**”按钮。接着在 Local Port 中定义“53”，然后再次点击 **Apply** 按钮。
- 5) 最后点击 **Set & Close** 按钮。

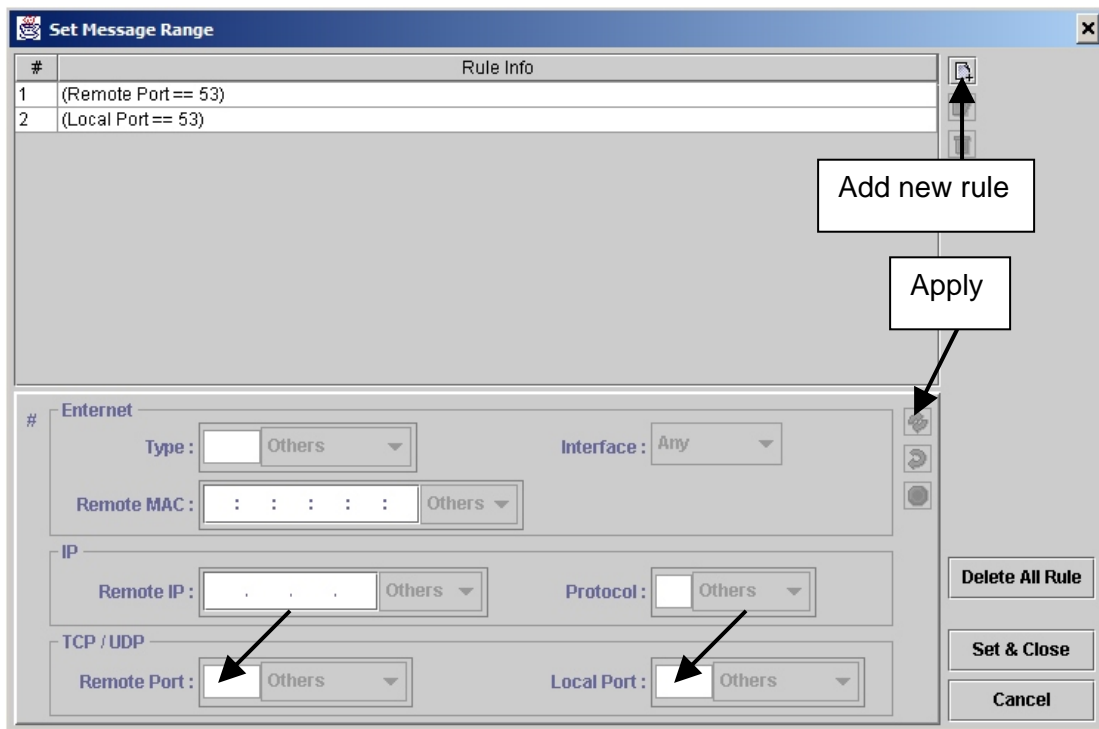


图 16.4

- 6) 从主菜单打开 Network Configuration 设置界面。
- 7) 在 Interface 1 中输入您实验室内分配的 IP 地址，设置您 Internet 网络的网关至路由表中。例如，定义 Interface 1 的 IP 地址为“192.168.1.223”，然后输入“192.168.1.254”至“Gateway”并且在“Destination”and“Mask”中输入“0.0.0.0”。(见图 16.5)
- 8) 模式选择“**Host**”，然后点击“**Set & Close**”按钮。

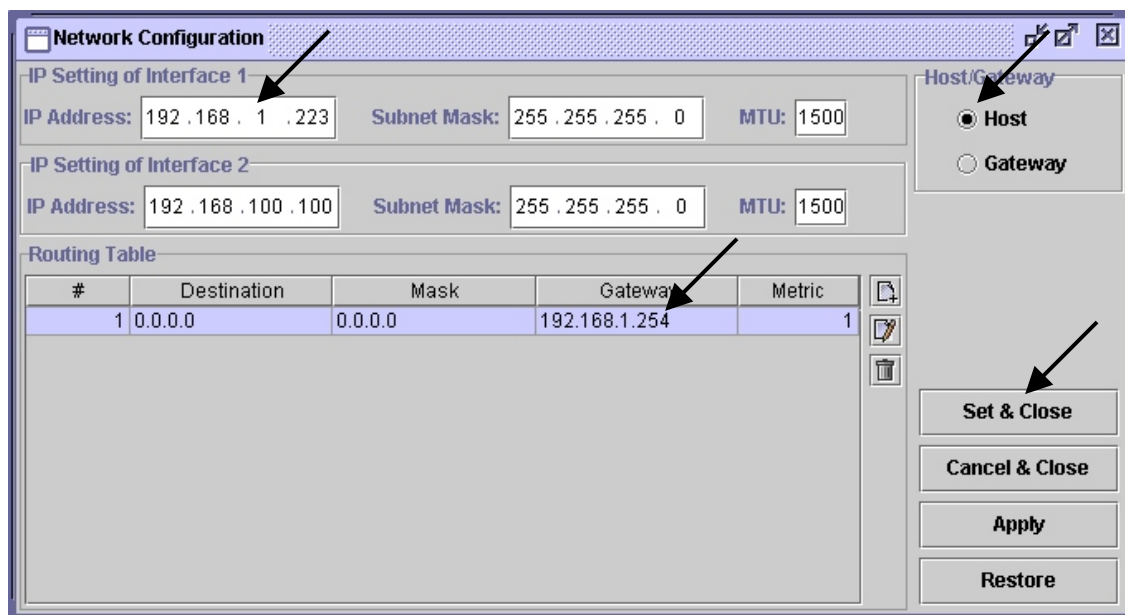


图 16.5

B. 发送 UDP 封包:

9) 打开“IP Datagram Sender”（在 send 主菜单中选择“**Send IP Packet**”）。

10) 定义您的 Internet DNS 服务器地址至“Destination IP Address”。例如，输入
 “168.95.1.1”至 Destination IP Address。

11) 再输入 “kandh.com.tw” 至数据段中（见图 16.6）。

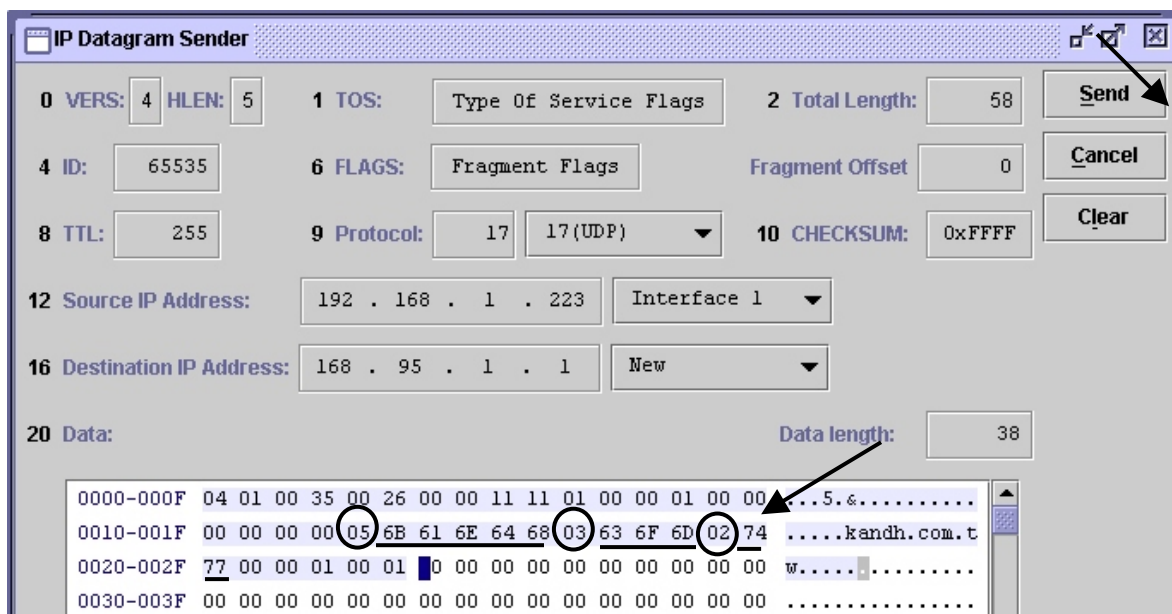


图 16.6

- 12) 最后点击“Send”按钮。ITS 将会立即发送一个 UDP 询问封包去询问“kandh.com.tw”。您将会收到一个 UDP 的回馈封包（见图 16.7）。

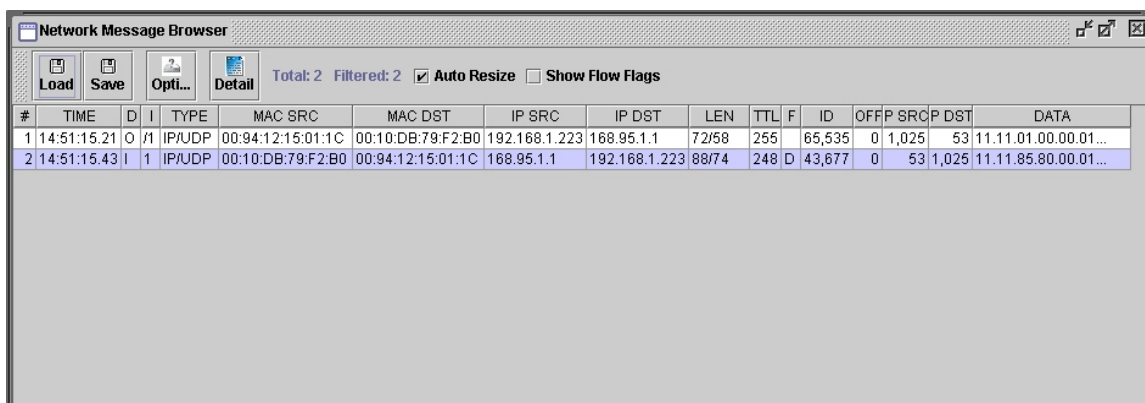


图 16.7

- 13) 在网络封包浏览器中（Network Message Browser）中选择 UDP 回馈封包，并且点击“Detail”按钮。您将会看见 UDP 数据包的全部内容（见图 16.8）。最后 4 个 16 进制数据包含了“kandh.com.tw”的 IP 地址 (61.218.30.102)。

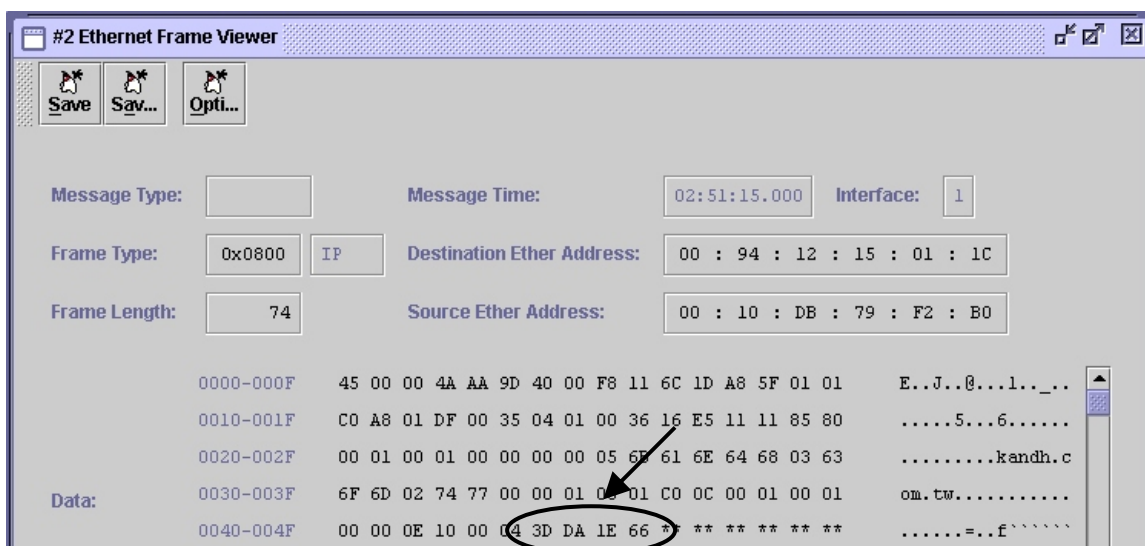
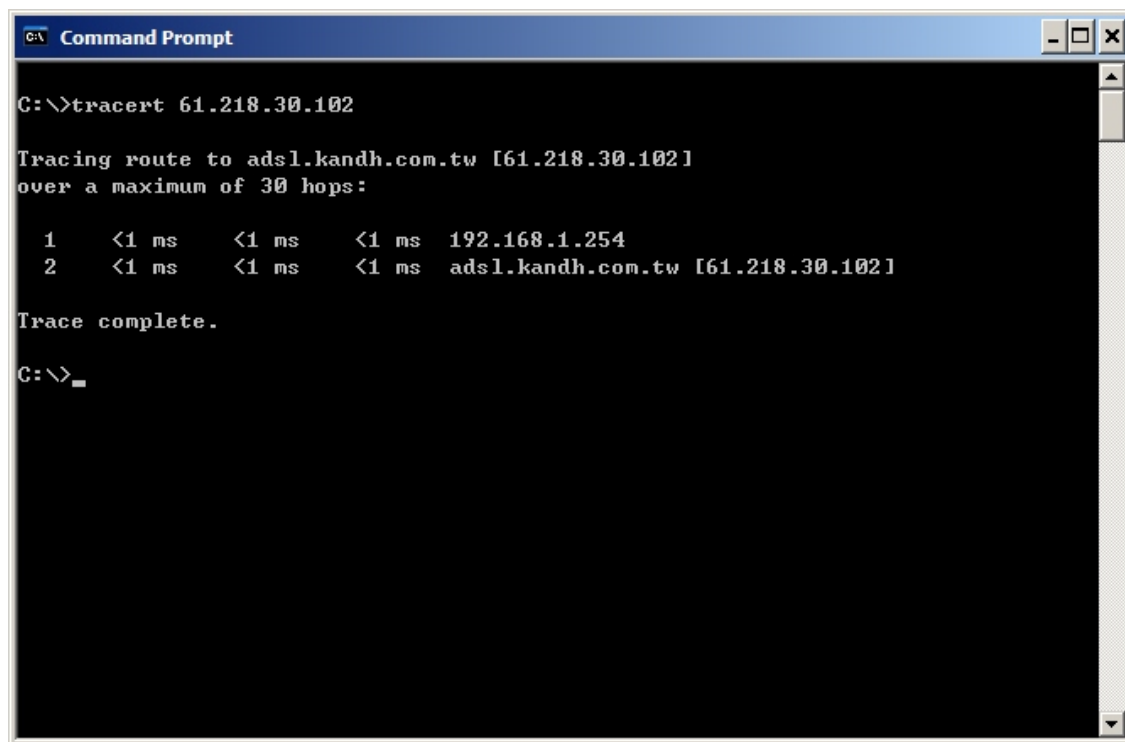


图 16.8

2、由 IP 地址映像域名

- 14) 打开 windows 的命令提示符界面。
- 15) 输入命令：**tracert 61.218.30.102**。系统将会询问该 IP 地址的域名，将会发现域名为“kandh.com.tw”（见图 16.9）。



```
C:\>tracert 61.218.30.102

Tracing route to adsl.kandh.com.tw [61.218.30.102]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.1.254
  1  <1 ms    <1 ms    <1 ms    adsl.kandh.com.tw [61.218.30.102]

Trace complete.

C:\>
```

图 16.9

四、实验讨论

- 1、将PC 的网络卡先接上ITS 的Interface 1，再从Interface 2联机到因特网，以ITS为路由器的方式进行设定，确认主机可以连上因特网后，在操作系统(Windows)下开启 Command Prompt窗口，输入指令并加上参数“ping -a 61.218.30.102”，从ITS 的网络讯息浏览器观察其现象，并讨论此指令做了什么动作。
- 2、既然已知道KandH的网域名称与IP地址，就试着直接连上www.kandh.com.tw的网站吧，里头除了ITS外还有许许多多的实验设备并提供完善的技术支持服务。

