# COMP7906 Introduction to Cyber Security

Lab 1

ZHANG Hongyi

## Q1. Ping

### Is www.google.com alive?

```
~
❯ ping www.google.com

正在 Ping www.google.com [142.250.198.100] 具有 32 字节的数据:
来自 142.250.198.100 的回复: 字节=32 时间=5ms TTL=57
来自 142.250.198.100 的回复: 字节=32 时间=6ms TTL=57
来自 142.250.198.100 的回复: 字节=32 时间=7ms TTL=57
来自 142.250.198.100 的回复: 字节=32 时间=3ms TTL=57

142.250.198.100 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 = 3ms, 最长 = 7ms, 平均 = 5ms
```

**Yes.** www.google.com is alive.

### Is www.hku.hk alive?

```
❯ ping www.hku.hk

正在 Ping www.hku.hk [147.8.2.58] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

147.8.2.58 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

### List at least 4 cases that ping reports “Request timed out”

1. **Destination host is unreachable**: If the destination host or device is offline, it won’t respond to the ping request, resulting a timeout.
2. **Firewall blocking ping requests**: Firewalls (on the source, destination, or intermediary networks) may be configured to block ICMP traffic, which includes ping requests and replies. This can also result in the ping request timing out.

3. **Network congestion or routing issue**: Heavy traffic on the network or routing problems can prevent ICMP Echo Request from reaching its destination or the ICMP Echo Reply from returning to the sender on time.
4. **Incorrect IP address or hostname**: If the IP address or hostname entered in the ping command is incorrect or invalid, the request may be sent to a non-existent or wrong destination. If an invalid IP address is used, the network may attempt to route the packet to an unreachable destination, leading to a timeout. If a hostname is used and DNS fails to resolve it to the correct IP address (or resolves to a wrong one), the ping request may be sent to an unreachable or incorrect device, resulting in "Request timed out."

# Q2. Traceroute

## How many hosts between your lab pc to www.google.com?

```
❯ tracert www.google.com

通过最多 30 个跃点跟踪
到 www.google.com [142.250.198.100] 的路由：

  1    <1 毫秒    <1 毫秒     1 ms  ImmortalWrt.lan [192.168.31.1]
  2    <1 毫秒     2 ms    <1 毫秒 192.168.1.1
  3    37 ms    53 ms    62 ms  10.193.232.16
  4     6 ms     *        5 ms  10.193.233.22
  5     6 ms     5 ms     5 ms  10.195.43.62
  6     *        *        *     请求超时。
  7    24 ms     7 ms     7 ms  72.14.219.16
  8     6 ms     7 ms     6 ms  142.250.63.187
  9     5 ms     7 ms     7 ms  66.249.95.129
 10     6 ms     7 ms     7 ms  nchkgb-af-in-f4.1e100.net [142.250.198.100]

跟踪完成。
```

There are 10 hosts between my pc and www.google.com.

## How many hosts between your lab pc to www.hku.hk?

```
❯ tracert www.hku.hk

通过最多 30 个跃点跟踪
到 www.hku.hk [147.8.2.58] 的路由：

  1    <1 毫秒    <1 毫秒    <1 毫秒 ImmortalWrt.lan [192.168.31.1]
  2    <1 毫秒     1 ms    <1 毫秒 192.168.1.1
  3     5 ms    12 ms     7 ms  10.193.233.16
  4     7 ms     7 ms     6 ms  10.193.232.21
  5     2 ms     4 ms     5 ms  10.195.42.198
  6     *        *        *     请求超时。
  7     5 ms    17 ms    19 ms  209-9-115-33.static.as3491.net [209.9.115.33]
  8     6 ms     8 ms     6 ms  209-9-115-38.static.as3491.net [209.9.115.38]
  9     6 ms     7 ms     6 ms  203.188.117.2
 10     5 ms    12 ms    11 ms  147.8.239.15
 11     *        *        *     请求超时。
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14     *        *        *     请求超时。
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18     *        *        *     请求超时。
 19     *        *        *     请求超时。
 20     *        *        *     请求超时。
 21     *        *        *     请求超时。
 22     *        *        *     请求超时。
 23     *        *        *     请求超时。
 24     *        *        *     请求超时。
 25     *        *        *     请求超时。
 26     *        *        *     请求超时。
 27     *        *        *     请求超时。
 28     *        *        *     请求超时。
 29     *        *        *     请求超时。
 30     *        *        *     请求超时。

跟踪完成。
```

There are at least 10 hosts between my pc and www.hku.hk.

### What is the last host you can access with traceroute to www.hku.hk?

The last host I can access is 147.8.239.15.

## Q3. Nslookup

### The mail exchange servers of hku.hk

```
❯ nslookup
默认服务器：  ImmortalWrt.lan
Address:  192.168.31.1

> set querytype=mx
> hku.hk
服务器：  ImmortalWrt.lan
Address:  192.168.31.1

非权威应答：
hku.hk  MX preference = 10, mail exchanger = hku-nsp1.hku.hk
hku.hk  MX preference = 10, mail exchanger = hku-nsp2.hku.hk

hku-nsp2.hku.hk internet address = 147.8.145.52
```

### Name servers of hku.hk

```
> set querytype=ns
> hku.hk
服务器：  ImmortalWrt.lan
Address:  192.168.31.1

非权威应答：
hku.hk  nameserver = ns3.hku.hk
hku.hk  nameserver = ns4.hku.hk
hku.hk  nameserver = ns10.gdnsec.com
hku.hk  nameserver = ns10.gdnsdef.com
hku.hk  nameserver = ns1.hku.hk
hku.hk  nameserver = ns2.hku.hk
hku.hk  nameserver = ns2.cuhk.edu.hk

ns4.hku.hk      internet address = 147.8.145.30
ns4.hku.hk      AAAA IPv6 address = 2001:ce0:2201:101:0:ffff:0:4
ns10.gdnsec.com internet address = 45.116.40.10
ns10.gdnsec.com AAAA IPv6 address = 2404:ae00:3266::2d74:2809
ns10.gdnsdef.com        internet address = 45.116.42.10
ns10.gdnsdef.com        AAAA IPv6 address = 2404:ae00:3266::2d74:2a09
ns1.hku.hk      internet address = 147.8.2.3
ns1.hku.hk      AAAA IPv6 address = 2001:ce0:2201:101:0:ffff:0:1
ns2.hku.hk      internet address = 147.8.145.32
ns2.hku.hk      AAAA IPv6 address = 2001:ce0:2201:101:0:ffff:0:2
ns2.cuhk.edu.hk internet address = 137.189.6.21
ns2.cuhk.edu.hk AAAA IPv6 address = 2405:3000:3:6::15
ns3.hku.hk      internet address = 147.8.2.2
ns3.hku.hk      AAAA IPv6 address = 2001:ce0:2201:101:0:ffff:0:3
```

### Mail exchange servers of google.com

```
❯ nslookup
默认服务器：  ImmortalWrt.lan
Address:  192.168.31.1

> set querytype=mx
> google.com
服务器：  ImmortalWrt.lan
Address:  192.168.31.1

非权威应答：
google.com      MX preference = 10, mail exchanger = smtp.google.com
```

### Name servers of google.com

```
> set querytype=ns
> google.com
服务器:  ImmortalWrt.lan
Address:  192.168.31.1

非权威应答:
google.com      nameserver = ns2.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns3.google.com

ns2.google.com  internet address = 216.239.34.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
```

### Are the results the same when using different DNS server?

Here are screenshots of trying commands after setting the DNS as 223.5.5.5 (Aliyun Public DNS):

```
> set querytype=mx
> hku.hk
服务器:  public1.alidns.com
Address:  223.5.5.5

非权威应答:
hku.hk  MX preference = 10, mail exchanger = hku-nsp2.hku.hk
hku.hk  MX preference = 10, mail exchanger = hku-nsp1.hku.hk
```

```
> set querytype=ns
> hku.hk
服务器:  public1.alidns.com
Address:  223.5.5.5

非权威应答:
hku.hk  nameserver = ns1.hku.hk
hku.hk  nameserver = ns10.gdnsdef.com
hku.hk  nameserver = ns4.hku.hk
hku.hk  nameserver = ns3.hku.hk
hku.hk  nameserver = ns2.hku.hk
hku.hk  nameserver = ns2.cuhk.edu.hk
hku.hk  nameserver = ns10.gdnsec.com
```

```
> google.com
服务器:  public1.alidns.com
Address:  223.5.5.5

非权威应答:
google.com      MX preference = 10, mail exchanger = smtp.google.com
```

```
服务器:  public1.alidns.com
Address:  223.5.5.5

非权威应答:
google.com      nameserver = ns4.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns3.google.com
```

As we can see, the result didn't change.

### What is the TTL setting in hku.hk domain?

```
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        hku.hk, type = A, class = IN
    ANSWERS:
    →  hku.hk
        internet address = 147.8.2.58
        ttl = 53275 (14 hours 47 mins 55 secs)
```

It is easy to see that the TTL setting in hku.hk is 53275 seconds (14 hours 47 mins 55 secs).

## Nmap

### Alive hosts in the network

```
❯ nmap -sn 192.168.31.42/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-08 22:41 中国标准时间
Nmap scan report for ImmortalWrt.lan (192.168.31.1)
Host is up (0.0020s latency).
MAC Address: 44:F7:70:2C:DF:B0 (Beijing Xiaomi Mobile Software)
Nmap scan report for TI-84ProMaxPlusUltra.lan (192.168.31.18)
Host is up (0.092s latency).
MAC Address: 9C:FC:E8:F2:CB:A5 (Intel Corporate)
Nmap scan report for iPhone.lan (192.168.31.43)
Host is up (0.085s latency).
MAC Address: C6:B0:B4:88:62:FD (Unknown)
Nmap scan report for AliVe.lan (192.168.31.42)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 34.06 seconds
```

### Their open ports

```
❯ nmap 192.168.31.42/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-08 22:42 中国标准时间
Nmap scan report for ImmortalWrt.lan (192.168.31.1)
Host is up (0.00040s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 44:F7:70:2C:DF:B0 (Beijing Xiaomi Mobile Software)

Nmap scan report for TI-84ProMaxPlusUltra.lan (192.168.31.18)
Host is up (0.013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: 9C:FC:E8:F2:CB:A5 (Intel Corporate)

Nmap scan report for iPhone.lan (192.168.31.43)
Host is up (0.0067s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: C6:B0:B4:88:62:FD (Unknown)

Nmap scan report for AliVe.lan (192.168.31.42)
Host is up (0.00013s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
110/tcp  filtered pop3
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
548/tcp  filtered afp
3000/tcp open     ppp
3001/tcp open     nessus

Nmap done: 256 IP addresses (4 hosts up) scanned in 83.03 seconds
```

## OS of these hosts

Linux:

```
❯ nmap -O 192.168.31.42/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-08 22:52 中国标准时间
Nmap scan report for ImmortalWrt.lan (192.168.31.1)
Host is up (0.00058s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 44:F7:70:2C:DF:B0 (Beijing Xiaomi Mobile Software)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
```

Windows:

```
Nmap scan report for TI-84ProMaxPlusUltra.lan (192.168.31.18)
Host is up (0.0030s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: 9C:FC:E8:F2:CB:A5 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|11|2019 (92%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1803 (92%), Microsoft Windows 10 1903 - 21H1 (92%), Microsoft Windows 11 (89
%), Microsoft Windows 10 1809 (87%), Microsoft Windows 10 1909 (85%), Microsoft Windows 10 1909 - 2004 (85%), Windows Se
rver 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
Nmap scan report for AliVe.lan (192.168.31.42)
Host is up (0.00027s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
110/tcp  filtered pop3
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
548/tcp  filtered afp
3000/tcp open     ppp
3001/tcp open     nessus
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

iOS:

```
Nmap scan report for iPhone.lan (192.168.31.43)
Host is up (0.014s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: C6:B0:B4:88:62:FD (Unknown)
Device type: general purpose
Running: Apple macOS 11.X|12.X|13.X
OS CPE: cpe:/o:apple:mac_os_x:11 cpe:/o:apple:mac_os_x:12 cpe:/o:apple:mac_os_x:13
OS details: Apple macOS 11 (Big Sur) - 13 (Ventura) or iOS 16 (Darwin 20.6.0 - 22.4.0)
Network Distance: 1 hop
```

# Whois

## Who is the technical contact of hku.hk domain?

```
Technical Contact Information:

Given name:  KATHERINE
Family name:  KWOK
Company name:  THE UNIVERSITY OF HONG KONG
Address:  INFORMATION TECHNOLOGY SERVICES, THE UNIVERSITY OF HONG KONG, POKFULAM ROAD, HONG KONG
Country:  Hong Kong (HK)
Phone:  +852-39172497
Fax:  +852-25597904
Email:  dnrtech@hku.hk
```

## How many email addresses did you find? What are they?

I found 4 email addresses.

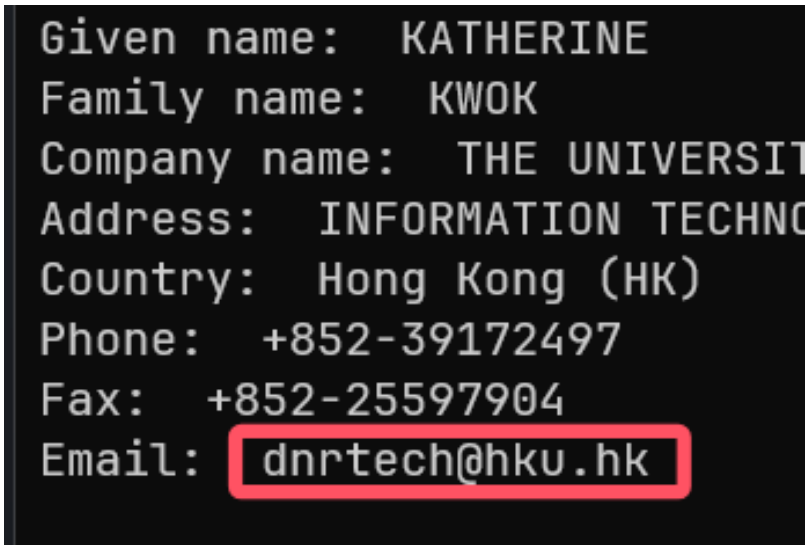
```
Registrar Name: Hong Kong Domain Name Registration Company Limited

Registrar Contact Information: Email: enquiry@hkdnr.hk
```

The first one is the domain registrar contact information.

```
Address:  INFORMATION TECHNOLOGY SERVICES, TH
Country:  Hong Kong (HK)
Email:  dnradmin@hku.hk
Domain Name Commencement Date: 03-01-1990
Expiry Date: 07-06-2033
Re-registration Status:  Complete
```

The second one is the registrant contact information.


The third one is the administrative contact information.




The last one is the technical contact information.