MTU 問題討論

台大計中

童鵬哲

MTU versus MSS

What’s MTU?

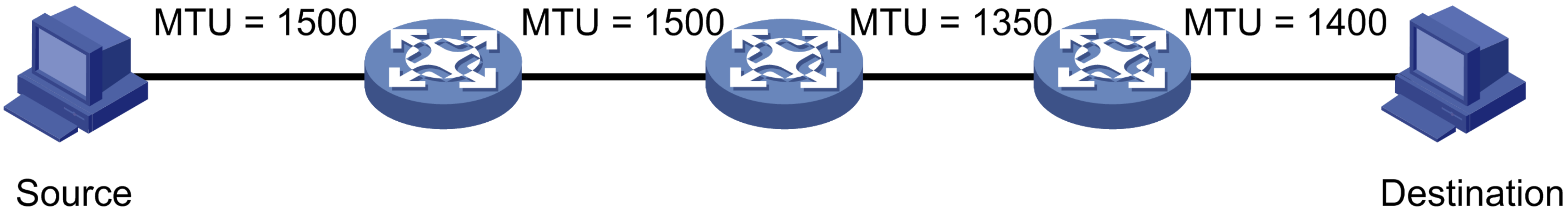
MTU (Maximum Transmission Unit)

— 封包在網路上最大可以被傳輸的大小(packet size)

— 每個網路設備或介面，可接受最大封包大小不一定一樣。

— 不論自己的設備MTU可以設定多大，需考慮封包傳送到目的地途中所有經過的設備之MTU。

— 在乙太網路上，標準的MTU定義為 1500 bytes。



出處:北區ASOC整理

What’s MSS?

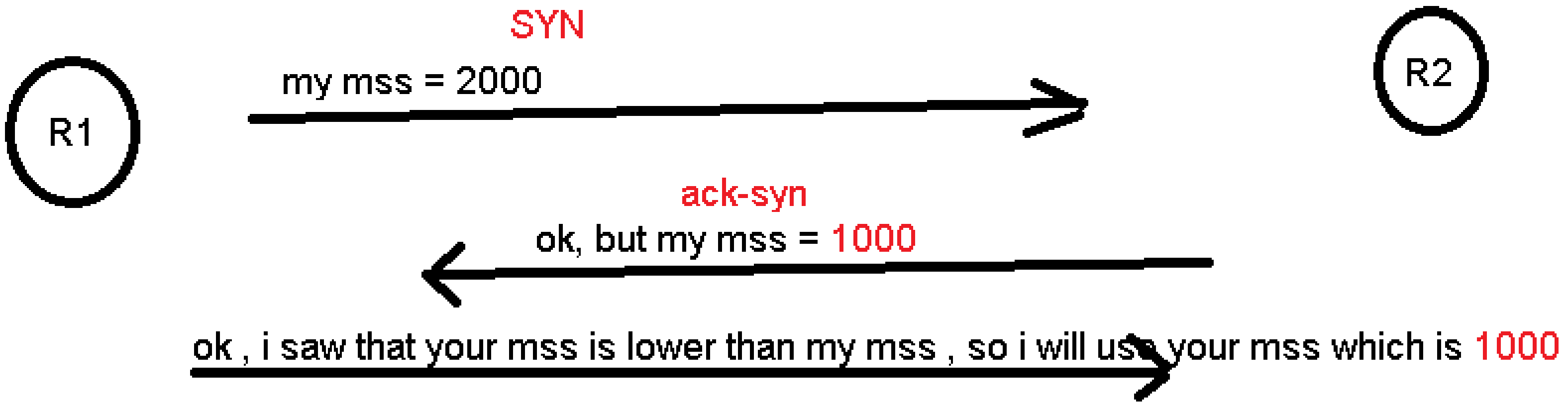
MSS (TCP Maximum Segment Size)

— TCP封包在網路上，每個封包可以傳輸的最大的data大小 (payload size)。

— 為了達到最佳的傳輸效能，TCP協議在建立連接的時候通常要協商雙方的MSS值。

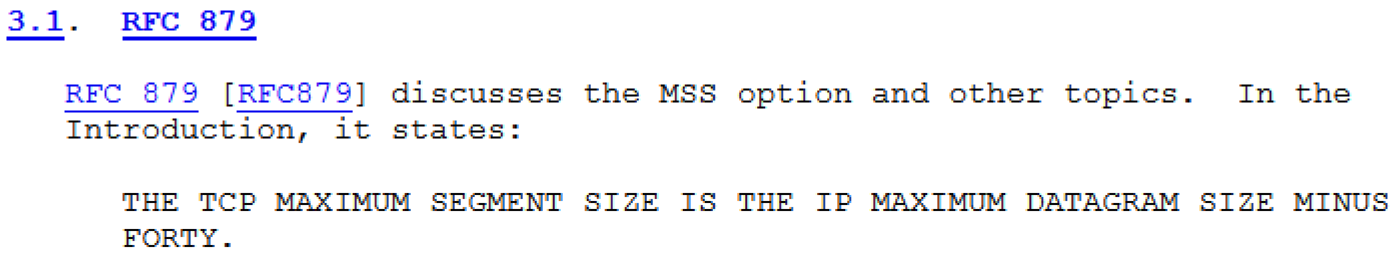
— 傳送端主機會根據其出口介面的傳輸單元最大值 (MTU) 來計算 TCP MSS。

— **MSS** = MTU – 40 (20 Byte for TCP + 20 Byte IP)。


SYN
my mss = 2000
R1
R2
ack-syn
ok, but my mss = 1000
ok , i saw that your mss is lower than my mss , so i will use your mss which is 1000

出處:北區ASOC整理

MTU vs. MSS



3.1. RFC 879

RFC 879 [RFC879] discusses the MSS option and other topics. In the Introduction, it states:

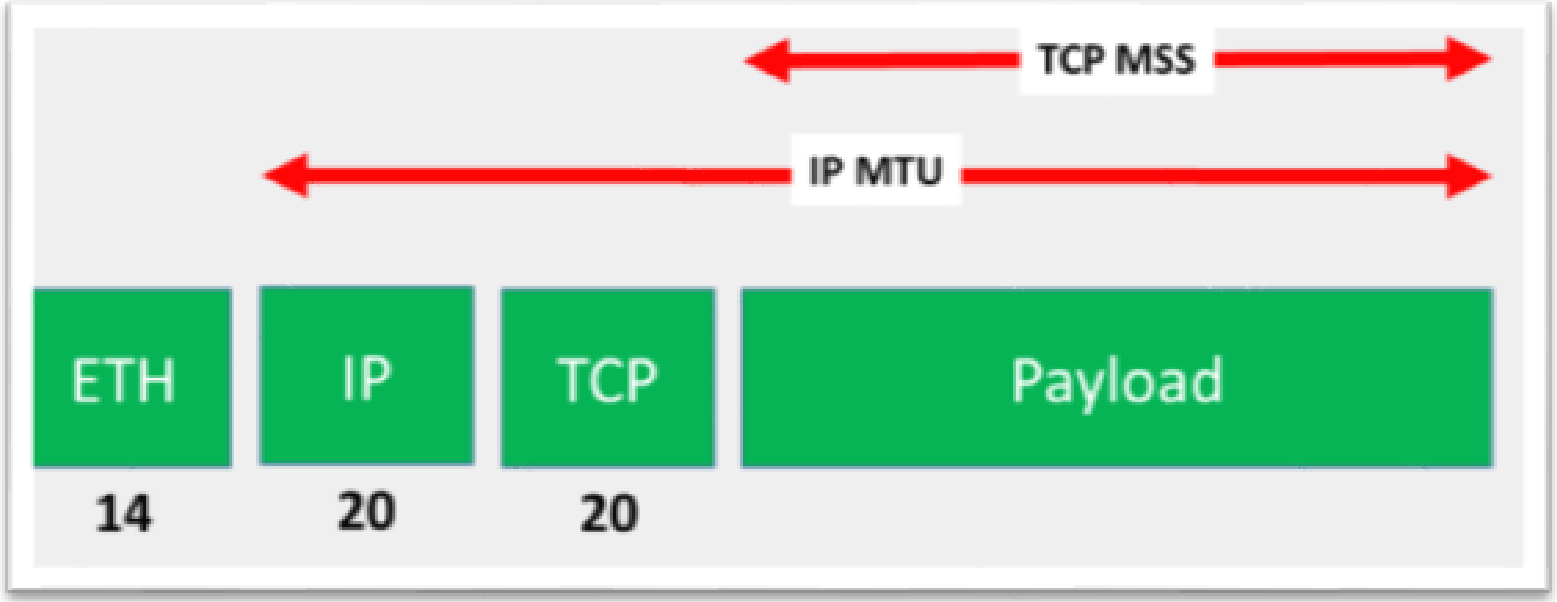
THE TCP MAXIMUM SEGMENT SIZE IS THE IP MAXIMUM DATAGRAM SIZE MINUS FORTY.

https://datatracker.ietf.org/doc/html/rfc6691

IP = 20 Bytes
TCP = 20 Bytes

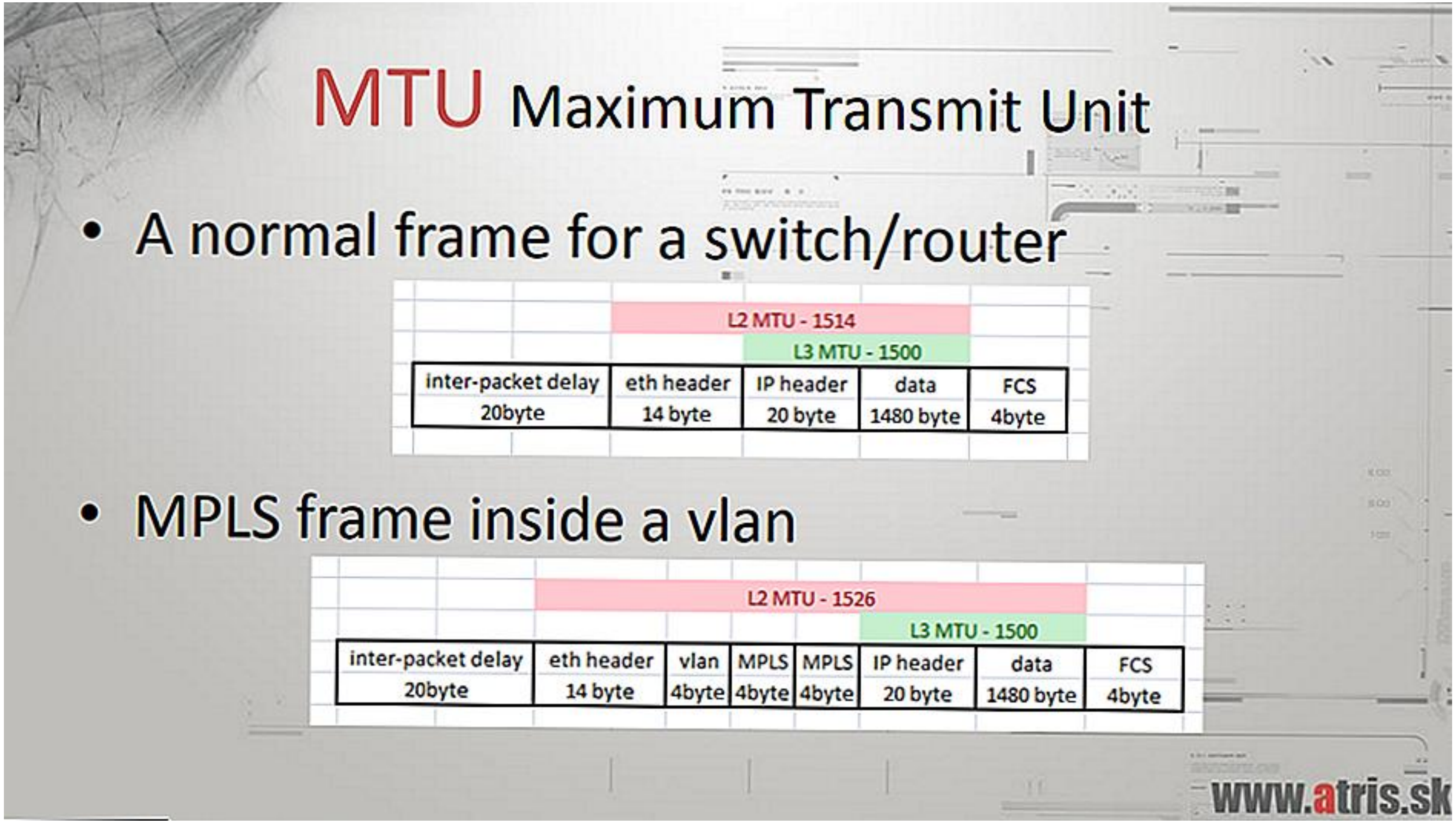
MTU = Payload + IP + TCP = 1500

MSS = MTU – 40 (20 Byte for TCP + 20 Byte IP)
= 1500 – 40
= **1460**



出處:北區ASOC整理

MPLS MTU



MTU Maximum Transmit Unit

- A normal frame for a switch/router

	L2 MTU - 1514			
		L3 MTU - 1500		
inter-packet delay 20byte	eth header 14 byte	IP header 20 byte	data 1480 byte	FCS 4byte

- MPLS frame inside a vlan

	L2 MTU - 1526						
					L3 MTU - 1500		
inter-packet delay 20byte	eth header 14 byte	vlan 4byte	MPLS 4byte	MPLS 4byte	IP header 20 byte	data 1480 byte	FCS 4byte

www.atris.sk

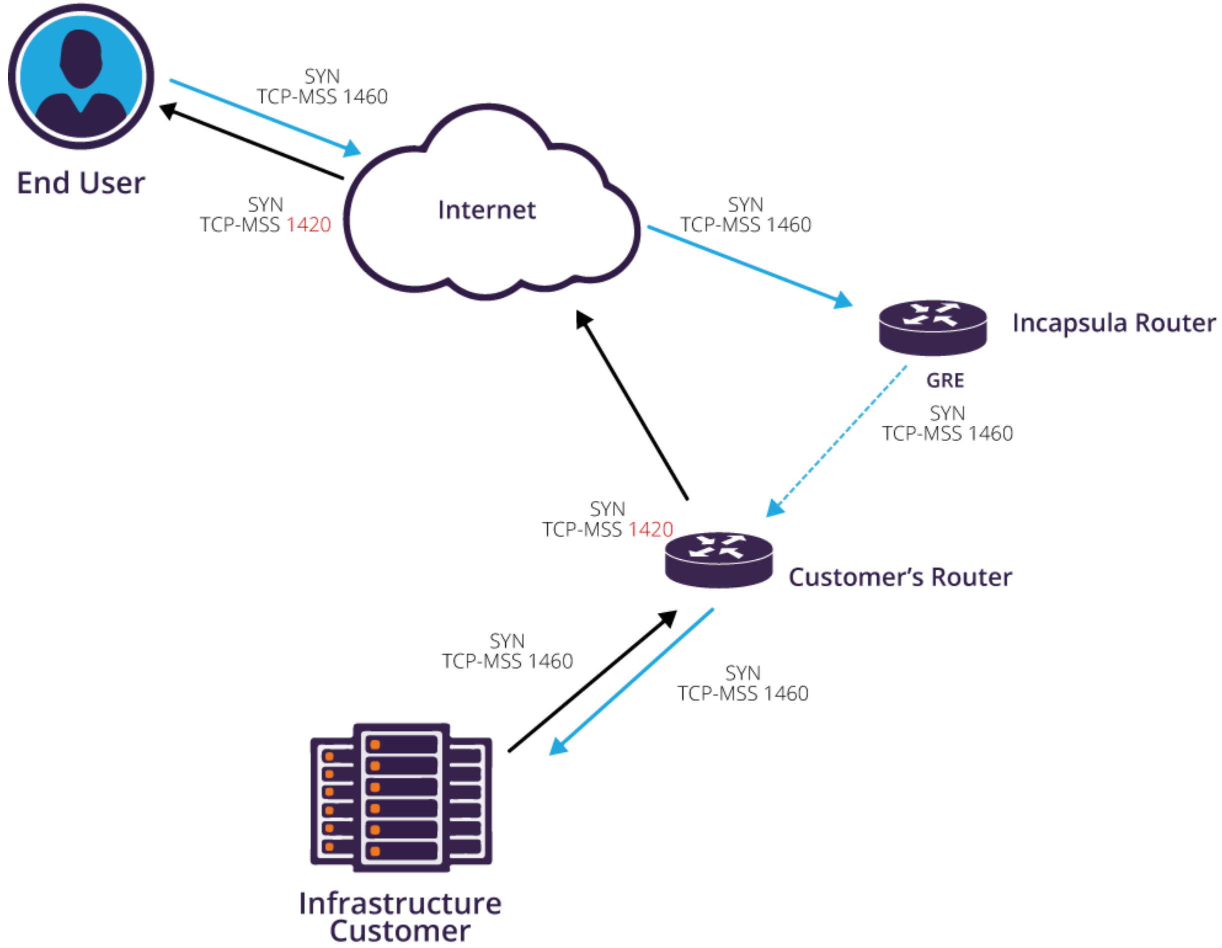
出處:北區ASOC整理

MTU 問題-自救解法

MTU問題-自救方法說明

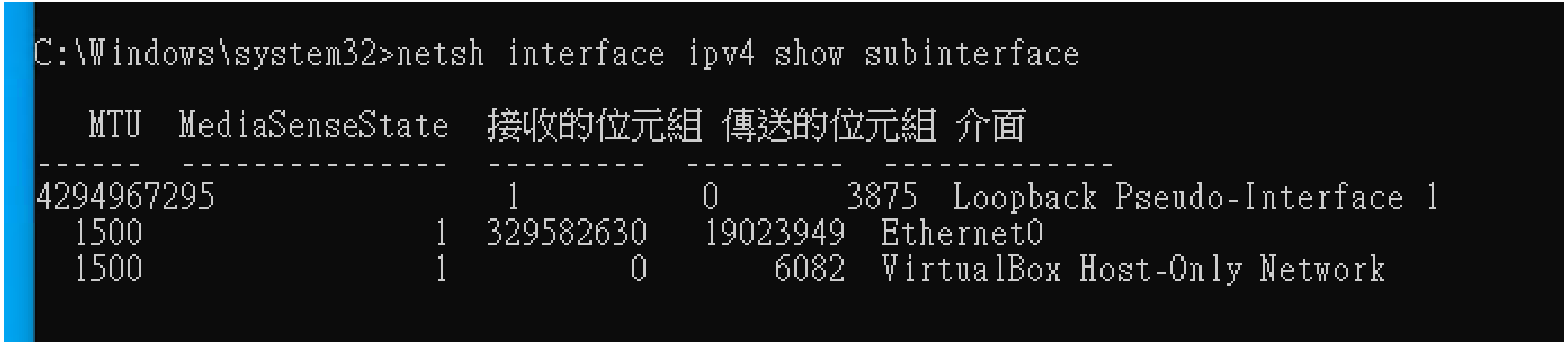
- **MSS** = MTU – 40 (20 Byte for TCP + 20 Byte IP)。
- 利用 TCP MSS 的協商機制。
- 壓低 MTU 來影響 MSS 協商，

  讓整體封包大小下降。



出處:北區ASOC整理

MTU 1500

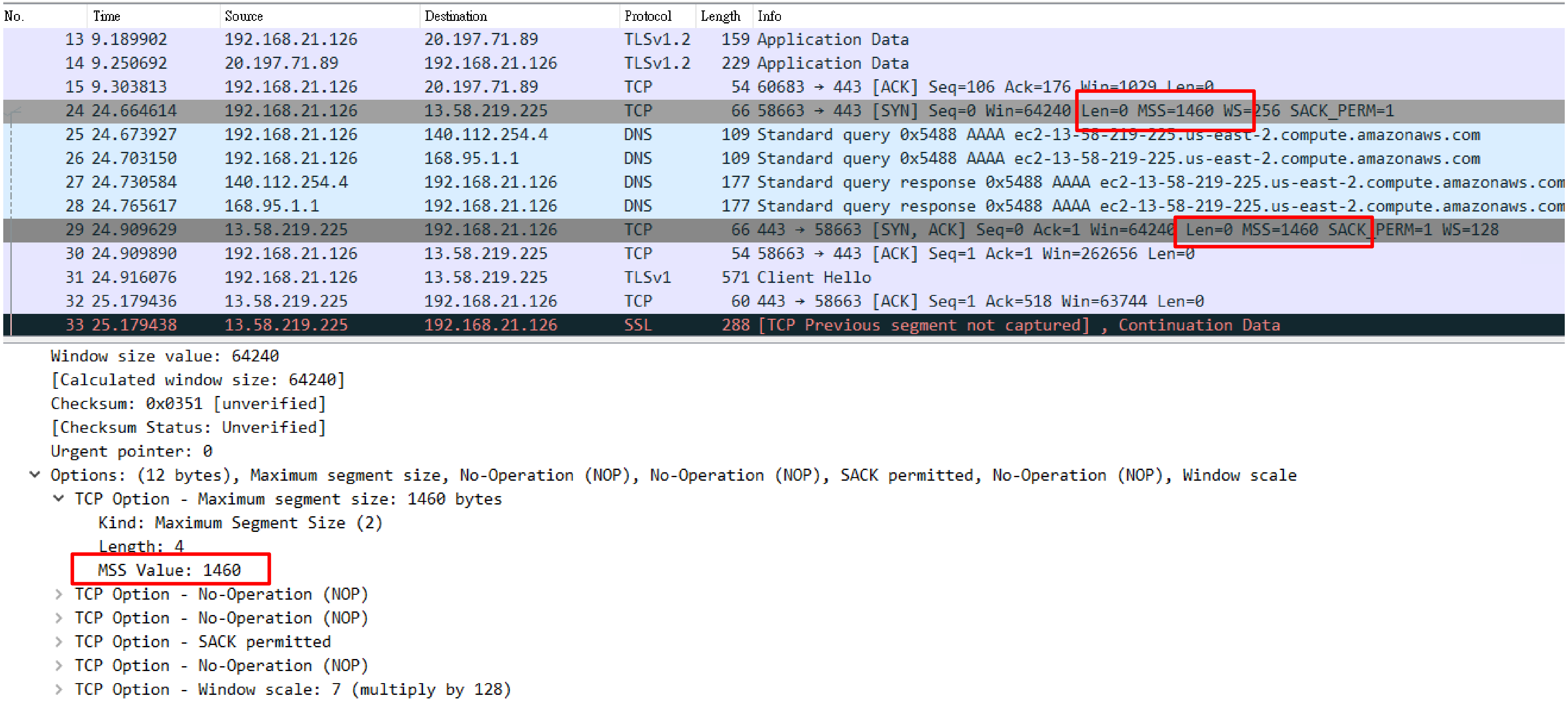


```
C:\Windows\system32>netsh interface ipv4 show subinterface

   MTU  MediaSenseState  接收的位元組 傳送的位元組 介面
------  ---------------  ---------  ---------  -------------
4294967295                1          0       3875  Loopback Pseudo-Interface 1
  1500                1  329582630   19023949  Ethernet0
  1500                1          0       6082  VirtualBox Host-Only Network
```

出處:北區ASOC整理

MTU 1500

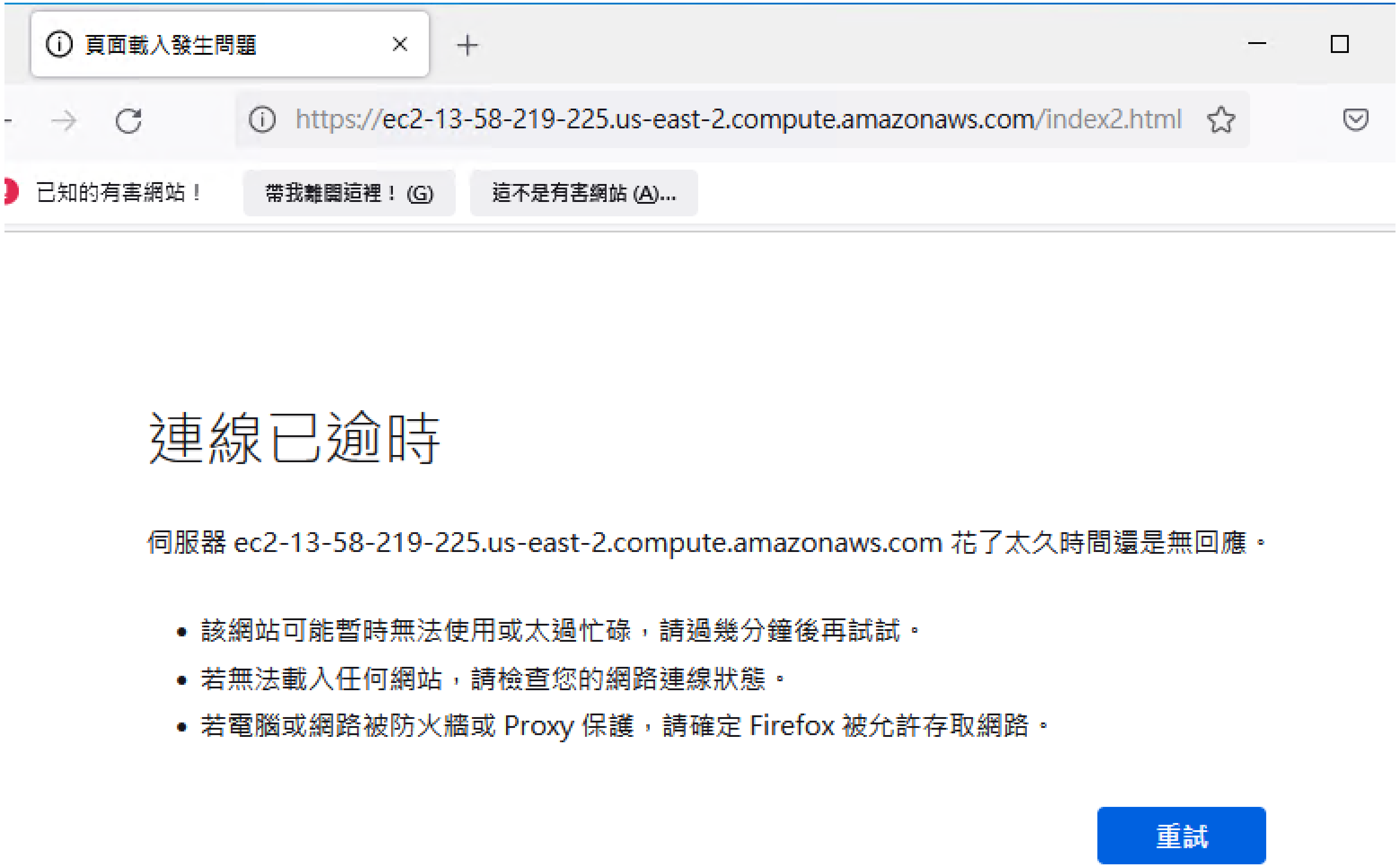


```
No.   Time       Source          Destination     Protocol  Length Info
   13 9.189902   192.168.21.126  20.197.71.89    TLSv1.2    159 Application Data
   14 9.250692   20.197.71.89    192.168.21.126  TLSv1.2    229 Application Data
   15 9.303813   192.168.21.126  20.197.71.89    TCP         54 60683 → 443 [ACK] Seq=106 Ack=176 Win=1029 Len=0
   24 24.664614  192.168.21.126  13.58.219.225   TCP         66 58663 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   25 24.673927  192.168.21.126  140.112.254.4   DNS        109 Standard query 0x5488 AAAA ec2-13-58-219-225.us-east-2.compute.amazonaws.com
   26 24.703150  192.168.21.126  168.95.1.1      DNS        109 Standard query 0x5488 AAAA ec2-13-58-219-225.us-east-2.compute.amazonaws.com
   27 24.730584  140.112.254.4   192.168.21.126  DNS        177 Standard query response 0x5488 AAAA ec2-13-58-219-225.us-east-2.compute.amazonaws.com
   28 24.765617  168.95.1.1      192.168.21.126  DNS        177 Standard query response 0x5488 AAAA ec2-13-58-219-225.us-east-2.compute.amazonaws.com
   29 24.909629  13.58.219.225   192.168.21.126  TCP         66 443 → 58663 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
   30 24.909890  192.168.21.126  13.58.219.225   TCP         54 58663 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
   31 24.916076  192.168.21.126  13.58.219.225   TLSv1      571 Client Hello
   32 25.179436  13.58.219.225   192.168.21.126  TCP         60 443 → 58663 [ACK] Seq=1 Ack=518 Win=63744 Len=0
   33 25.179438  13.58.219.225   192.168.21.126  SSL        288 [TCP Previous segment not captured] , Continuation Data
```

```
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0x0351 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ⌄ Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    ⌄ TCP Option - Maximum segment size: 1460 bytes
        Kind: Maximum Segment Size (2)
        Length: 4
        MSS Value: 1460
    › TCP Option - No-Operation (NOP)
    › TCP Option - No-Operation (NOP)
    › TCP Option - SACK permitted
    › TCP Option - No-Operation (NOP)
    › TCP Option - Window scale: 7 (multiply by 128)
```

出處:北區ASOC整理

MTU 1500



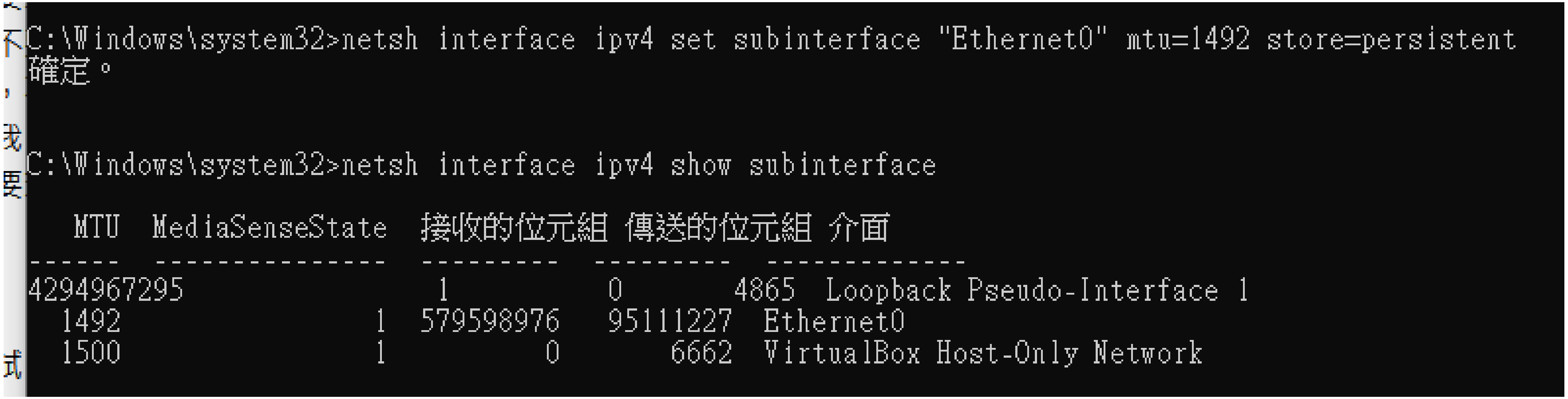
連線已逾時

伺服器 ec2-13-58-219-225.us-east-2.compute.amazonaws.com 花了太久時間還是無回應。

- 該網站可能暫時無法使用或太過忙碌，請過幾分鐘後再試試。
- 若無法載入任何網站，請檢查您的網路連線狀態。
- 若電腦或網路被防火牆或 Proxy 保護，請確定 Firefox 被允許存取網路。

出處:北區ASOC整理

MTU 1492



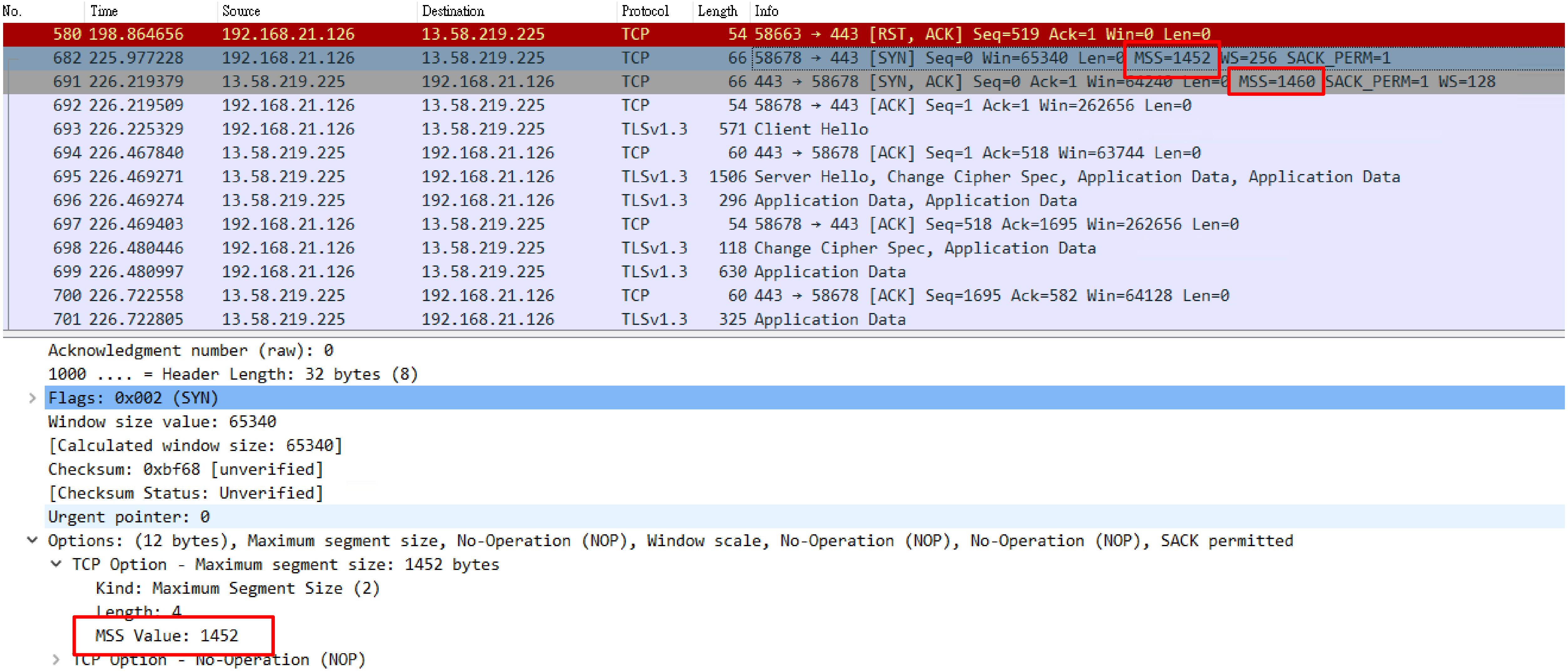
```
C:\Windows\system32>netsh interface ipv4 set subinterface "Ethernet0" mtu=1492 store=persistent
確定。


C:\Windows\system32>netsh interface ipv4 show subinterface

   MTU  MediaSenseState  接收的位元組 傳送的位元組 介面
------  ---------------  ---------  ---------  -------------
4294967295                1          0       4865  Loopback Pseudo-Interface 1
  1492                1  579598976   95111227  Ethernet0
  1500                1          0       6662  VirtualBox Host-Only Network
```

出處:北區ASOC整理

MTU 1492

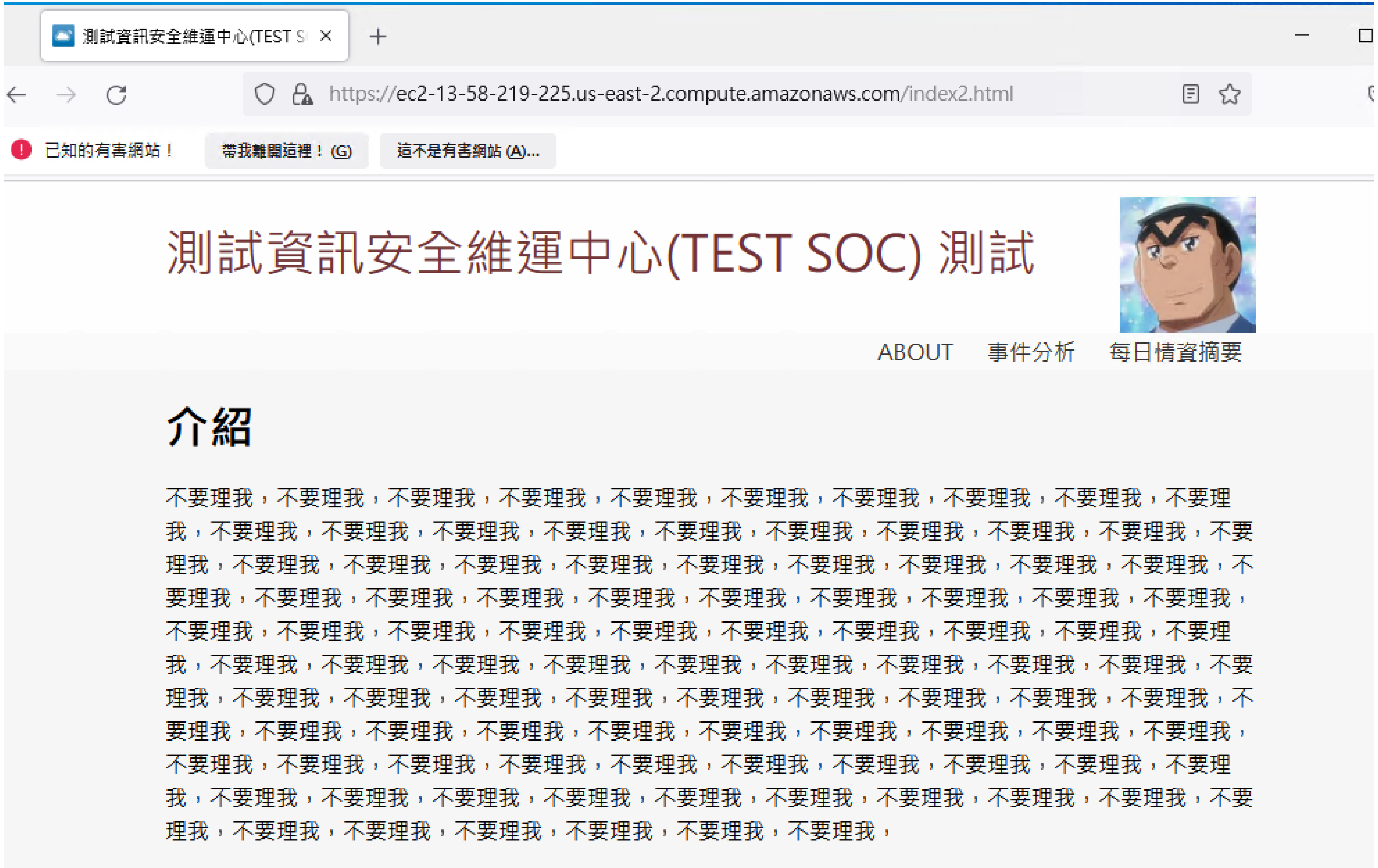


```
No.    Time         Source           Destination      Protocol  Length Info
580 198.864656 192.168.21.126   13.58.219.225    TCP          54 58663 → 443 [RST, ACK] Seq=519 Ack=1 Win=0 Len=0
682 225.977228 192.168.21.126   13.58.219.225    TCP          66 58678 → 443 [SYN] Seq=0 Win=65340 Len=0 MSS=1452 WS=256 SACK_PERM=1
691 226.219379 13.58.219.225    192.168.21.126   TCP          66 443 → 58678 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
692 226.219509 192.168.21.126   13.58.219.225    TCP          54 58678 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
693 226.225329 192.168.21.126   13.58.219.225    TLSv1.3     571 Client Hello
694 226.467840 13.58.219.225    192.168.21.126   TCP          60 443 → 58678 [ACK] Seq=1 Ack=518 Win=63744 Len=0
695 226.469271 13.58.219.225    192.168.21.126   TLSv1.3    1506 Server Hello, Change Cipher Spec, Application Data, Application Data
696 226.469274 13.58.219.225    192.168.21.126   TLSv1.3     296 Application Data, Application Data
697 226.469403 192.168.21.126   13.58.219.225    TCP          54 58678 → 443 [ACK] Seq=518 Ack=1695 Win=262656 Len=0
698 226.480446 192.168.21.126   13.58.219.225    TLSv1.3     118 Change Cipher Spec, Application Data
699 226.480997 192.168.21.126   13.58.219.225    TLSv1.3     630 Application Data
700 226.722558 13.58.219.225    192.168.21.126   TCP          60 443 → 58678 [ACK] Seq=1695 Ack=582 Win=64128 Len=0
701 226.722805 13.58.219.225    192.168.21.126   TLSv1.3     325 Application Data
```

```
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 65340
    [Calculated window size: 65340]
    Checksum: 0xbf68 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ˅ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    ˅ TCP Option - Maximum segment size: 1452 bytes
          Kind: Maximum Segment Size (2)
          Length: 4
          MSS Value: 1452
    > TCP Option - No-Operation (NOP)
```

出處:北區ASOC整理

MTU 1492



https://ec2-13-58-219-225.us-east-2.compute.amazonaws.com/index2.html

已知的有害網站！

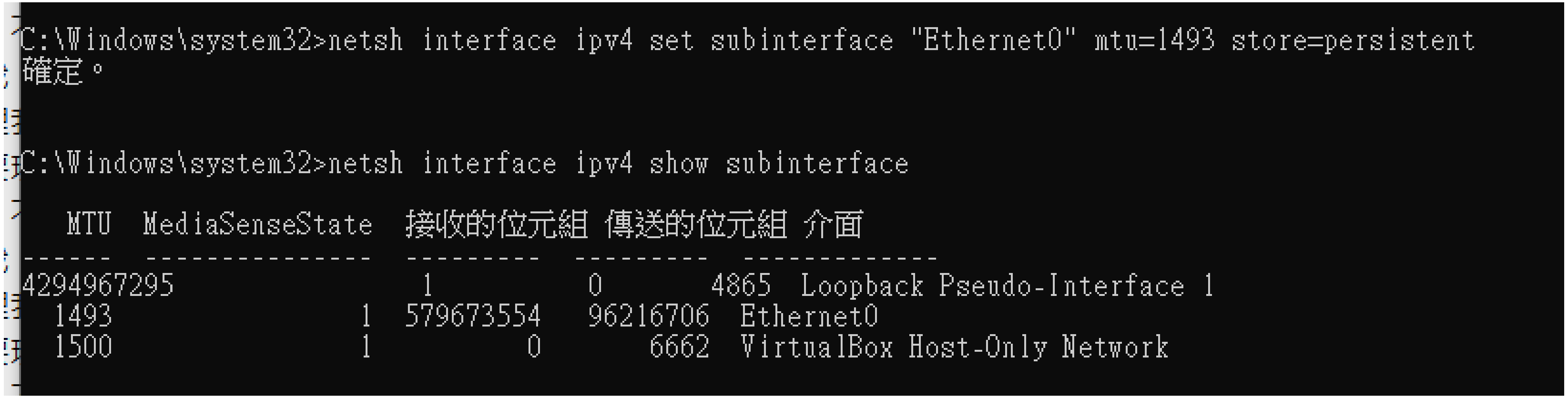
測試資訊安全維運中心(TEST SOC) 測試

介紹

不要理我，

出處:北區ASOC整理

MTU 1493



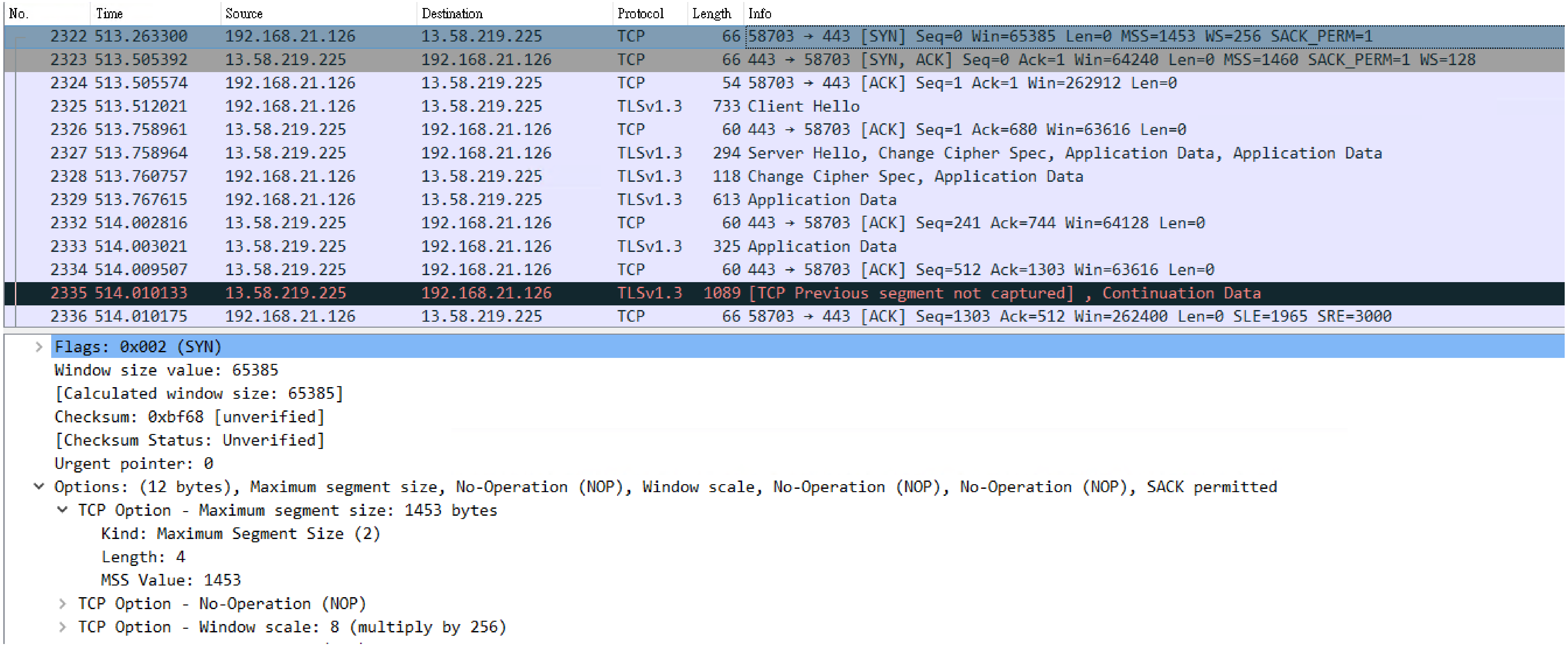
```
C:\Windows\system32>netsh interface ipv4 set subinterface "Ethernet0" mtu=1493 store=persistent
確定。


C:\Windows\system32>netsh interface ipv4 show subinterface

   MTU  MediaSenseState  接收的位元組 傳送的位元組 介面
------  ---------------  ---------  ---------  -------------
4294967295                1          0       4865  Loopback Pseudo-Interface 1
  1493                1  579673554   96216706  Ethernet0
  1500                1          0       6662  VirtualBox Host-Only Network
```

出處:北區ASOC整理

MTU 1493

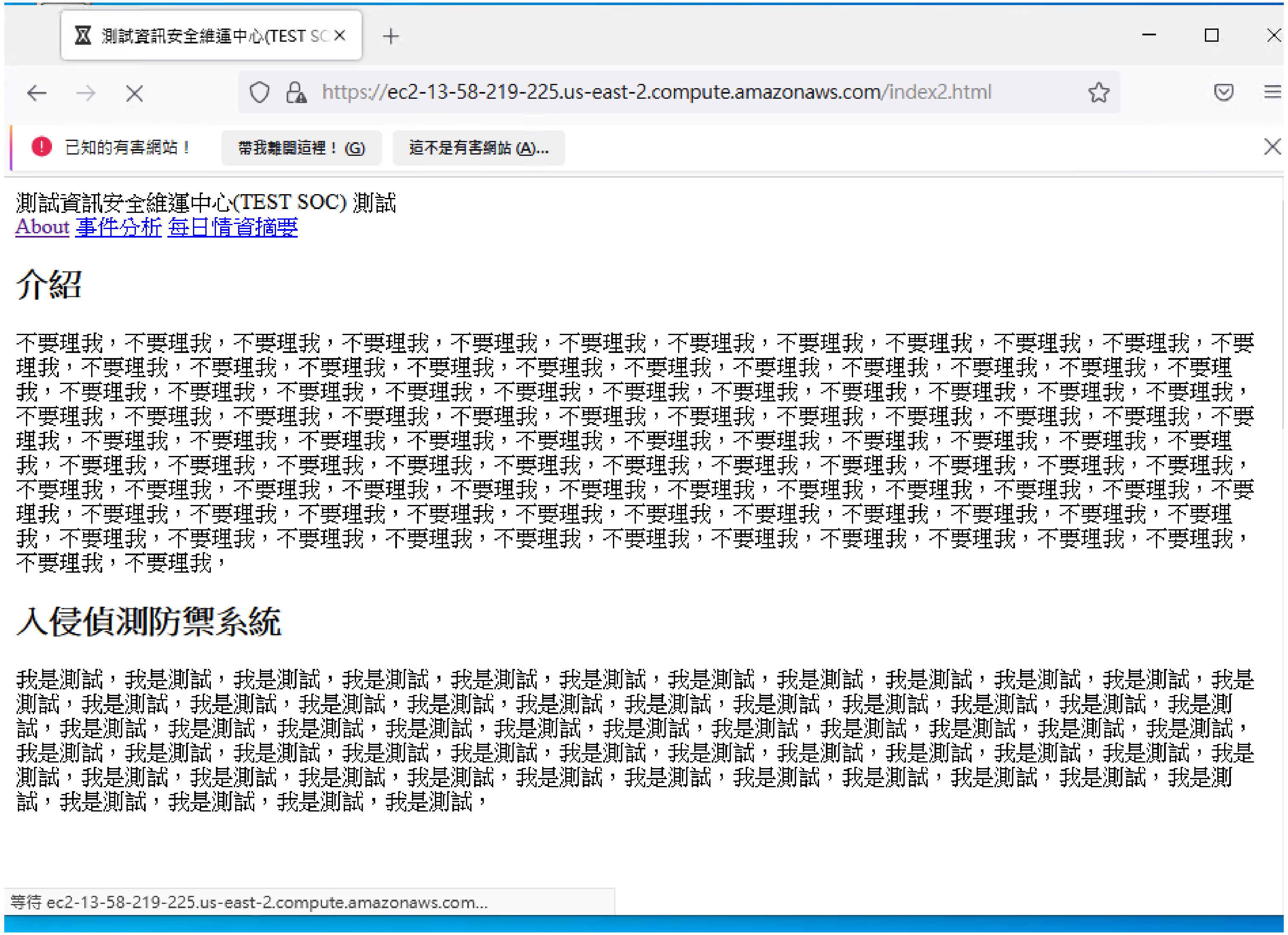


```
No.  Time        Source          Destination     Protocol  Length Info
2322 513.263300  192.168.21.126  13.58.219.225   TCP          66 58703 → 443 [SYN] Seq=0 Win=65385 Len=0 MSS=1453 WS=256 SACK_PERM=1
2323 513.505392  13.58.219.225   192.168.21.126  TCP          66 443 → 58703 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
2324 513.505574  192.168.21.126  13.58.219.225   TCP          54 58703 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
2325 513.512021  192.168.21.126  13.58.219.225   TLSv1.3     733 Client Hello
2326 513.758961  13.58.219.225   192.168.21.126  TCP          60 443 → 58703 [ACK] Seq=1 Ack=680 Win=63616 Len=0
2327 513.758964  13.58.219.225   192.168.21.126  TLSv1.3     294 Server Hello, Change Cipher Spec, Application Data, Application Data
2328 513.760757  192.168.21.126  13.58.219.225   TLSv1.3     118 Change Cipher Spec, Application Data
2329 513.767615  192.168.21.126  13.58.219.225   TLSv1.3     613 Application Data
2332 514.002816  13.58.219.225   192.168.21.126  TCP          60 443 → 58703 [ACK] Seq=241 Ack=744 Win=64128 Len=0
2333 514.003021  13.58.219.225   192.168.21.126  TLSv1.3     325 Application Data
2334 514.009507  13.58.219.225   192.168.21.126  TCP          60 443 → 58703 [ACK] Seq=512 Ack=1303 Win=63616 Len=0
2335 514.010133  13.58.219.225   192.168.21.126  TLSv1.3    1089 [TCP Previous segment not captured] , Continuation Data
2336 514.010175  192.168.21.126  13.58.219.225   TCP          66 58703 → 443 [ACK] Seq=1303 Ack=512 Win=262400 Len=0 SLE=1965 SRE=3000
```

```
  > Flags: 0x002 (SYN)
    Window size value: 65385
    [Calculated window size: 65385]
    Checksum: 0xbf68 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ∨ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    ∨ TCP Option - Maximum segment size: 1453 bytes
        Kind: Maximum Segment Size (2)
        Length: 4
        MSS Value: 1453
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 8 (multiply by 256)
```

出處:北區ASOC整理

MTU 1493



測試資訊安全維運中心(TEST SC ×

https://ec2-13-58-219-225.us-east-2.compute.amazonaws.com/index2.html

已知的有害網站！ 帶我離開這裡！(G) 這不是有害網站 (A)...

測試資訊安全維運中心(TEST SOC) 測試
About 事件分析 每日情資摘要

介紹

不要理我，

入侵偵測防禦系統

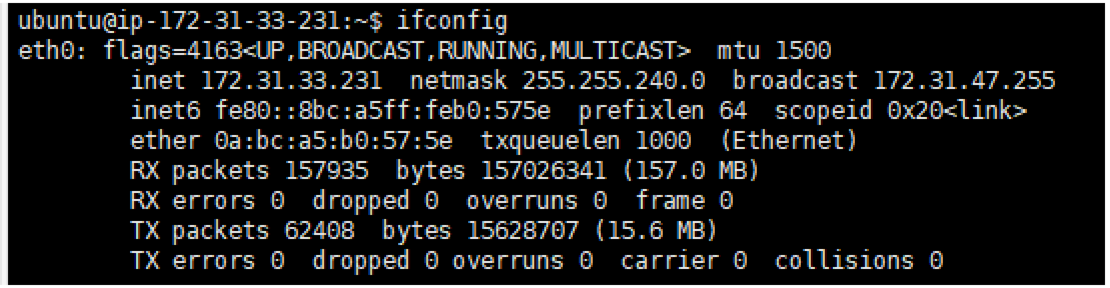
我是測試，

等待 ec2-13-58-219-225.us-east-2.compute.amazonaws.com...

出處:北區ASOC整理

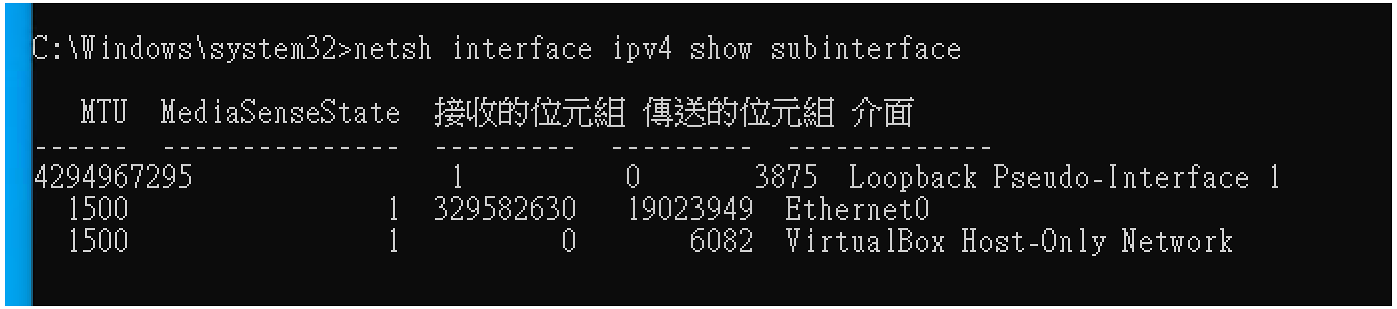
MTU 調整 command

Linux
ifconfig
sudo ifconfig eth0 mtu 1492



```
ubuntu@ip-172-31-33-231:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.33.231  netmask 255.255.240.0  broadcast 172.31.47.255
        inet6 fe80::8bc:a5ff:feb0:575e  prefixlen 64  scopeid 0x20<link>
        ether 0a:bc:a5:b0:57:5e  txqueuelen 1000  (Ethernet)
        RX packets 157935  bytes 157026341 (157.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62408  bytes 15628707 (15.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Windows
netsh interface ipv4 show subinterface
netsh interface ipv4 set subinterface "Ethernet0" mtu=1500 store=persistent



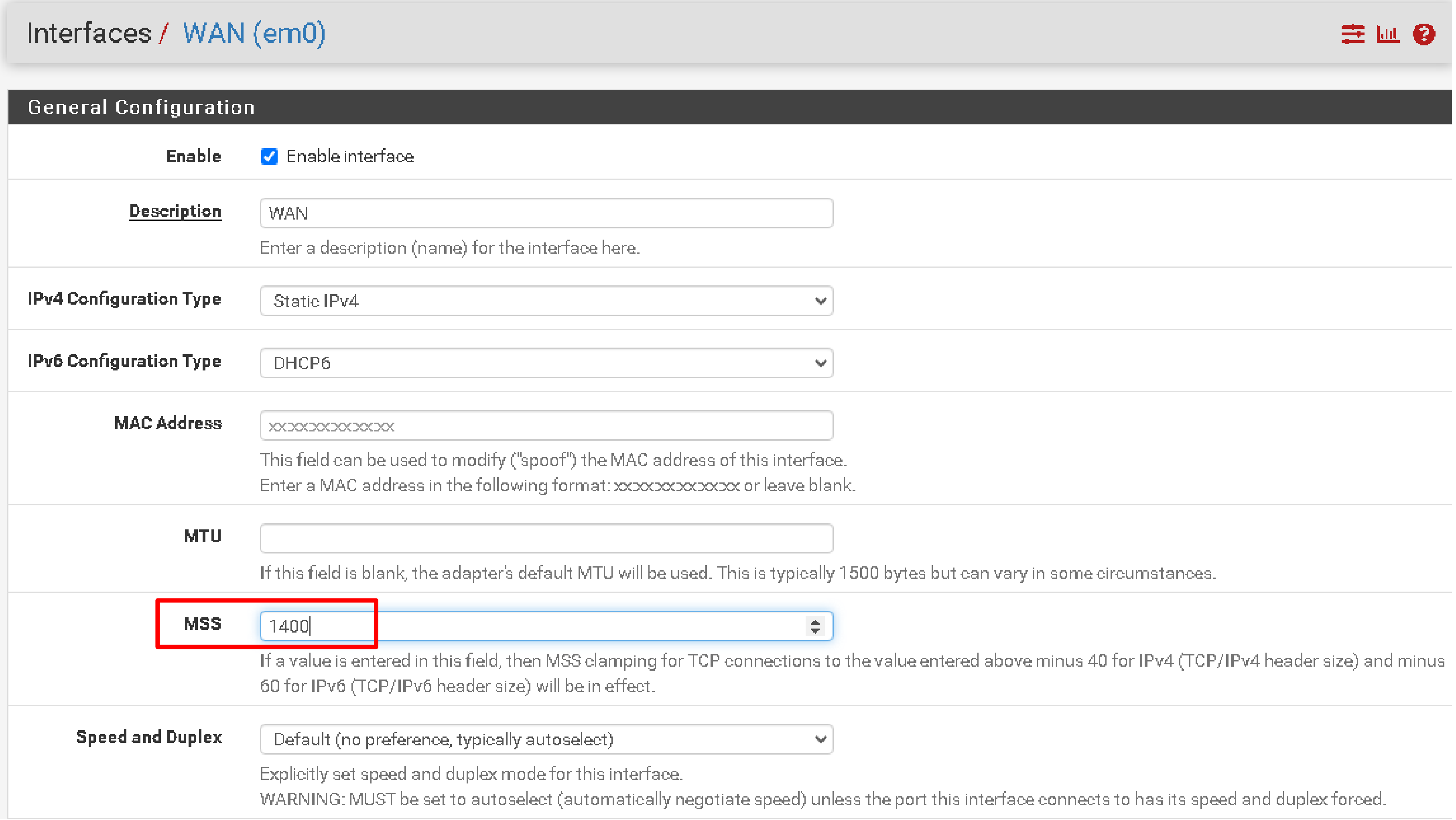
```
C:\Windows\system32>netsh interface ipv4 show subinterface

   MTU  MediaSenseState   接收的位元組  傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
4294967295                1          0       3875  Loopback Pseudo-Interface 1
  1500                1  329582630   19023949  Ethernet0
  1500                1          0       6082  VirtualBox Host-Only Network
```

出處:北區ASOC整理

Router MSS 調整

MSS clamping



Interfaces / WAN (em0)

General Configuration

Enable ☑ Enable interface

Description: WAN

Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: DHCP6

MAC Address: xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS: 1400

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)

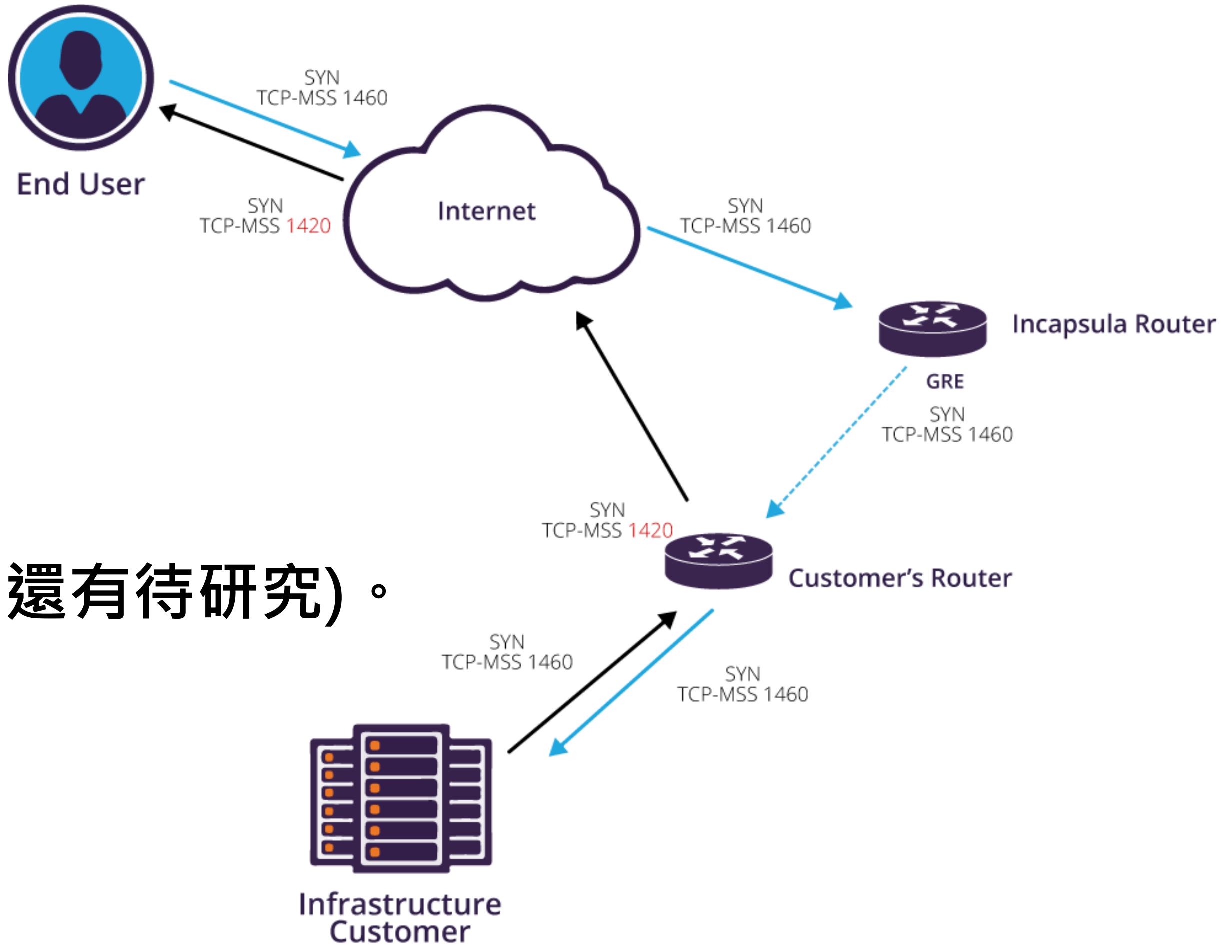
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

出處:北區ASOC整理

MTU問題-自救解法

- **MSS** = MTU – 40 (20 Byte for TCP + 20 Byte IP)。
- 利用 TCP MSS 的協商機制。
- 壓低 MTU 來影響 MSS 協商，

  讓整體封包大小下降。



- **自行壓低 client 端 MTU。**
- **調整 Layer3設備 MSS 值 (比較複雜，還有待研究)。**

出處:北區ASOC整理