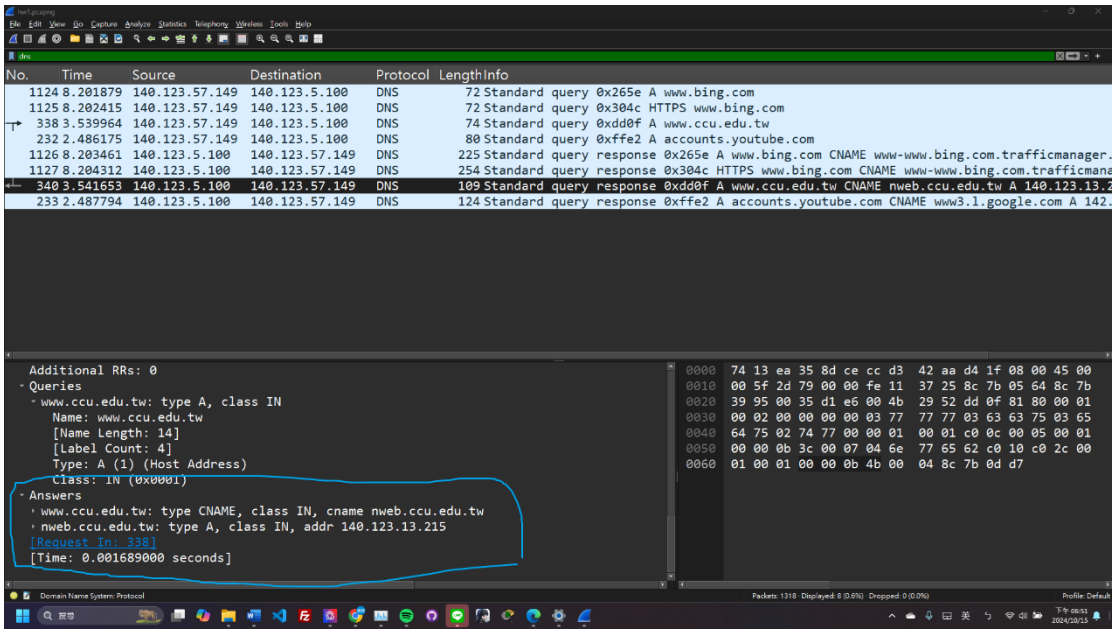
2. Traffic Analysis

Q1: The full TCP stream statistic and total data in bytes for the access session

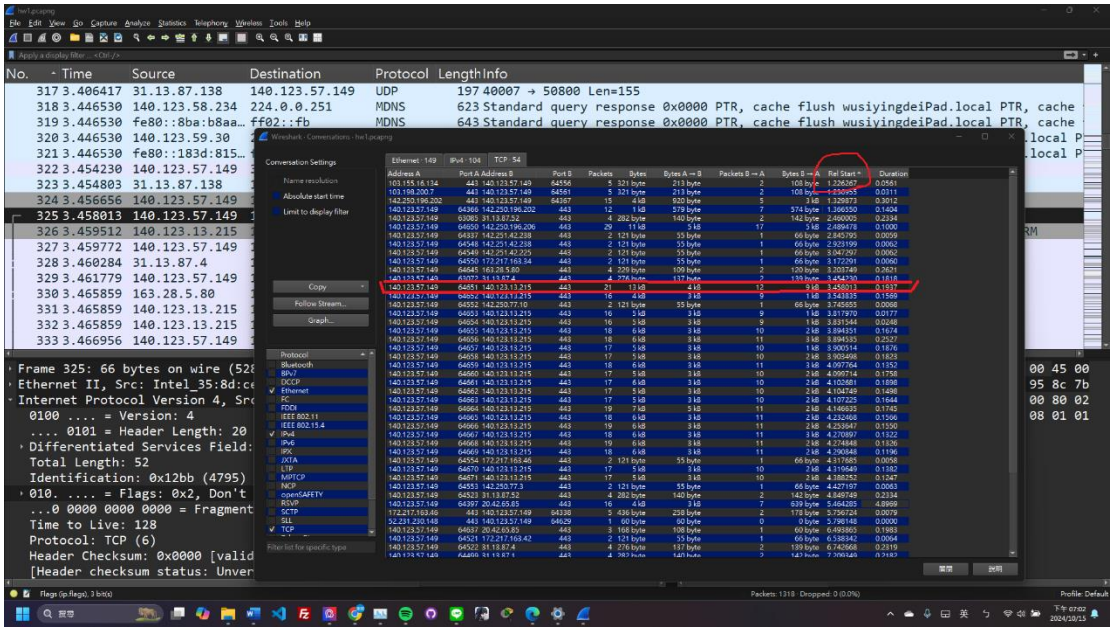
A1: 13 kB

First we need to know the ip address of ccu.edu.tw



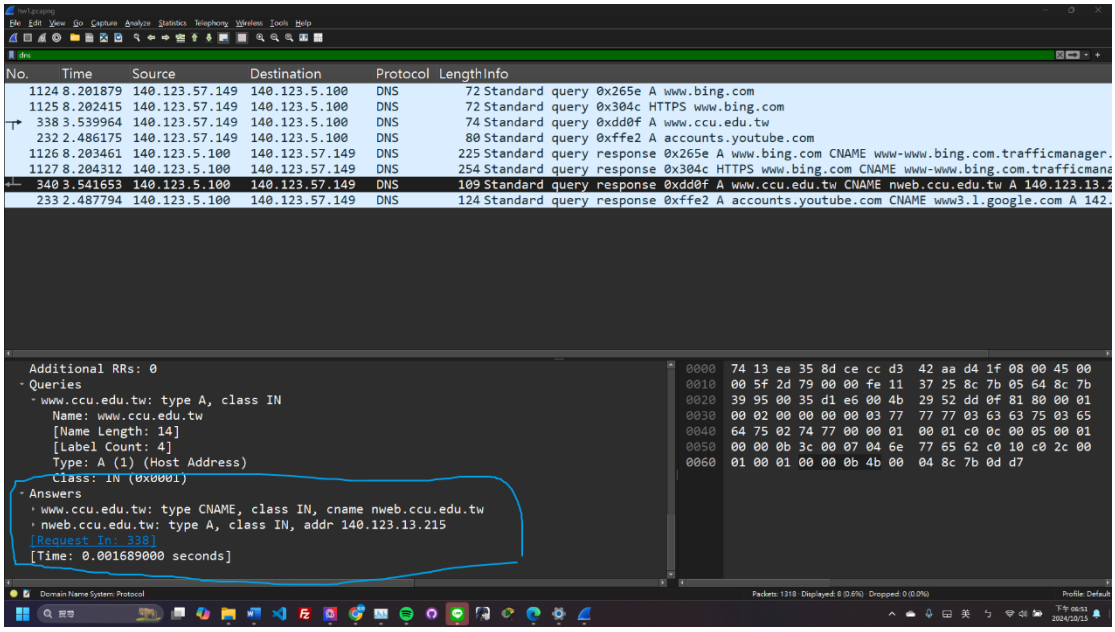
and our ip address(140.123.57.149)

Then we filter 140.123.13.215 and 140.123.57.149, find out the earliest tcp conversation. This is what we want.



Q2: The IP address of the website (DNS resolution)

A2: 140.123.13.215


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1124 8.201879 140.123.57.149 140.123.5.100 DNS 72 Standard query 0x265e A www.bing.com
1125 8.202415 140.123.57.149 140.123.5.100 DNS 72 Standard query 0x304c HTTPS www.bing.com
338 3.539964 140.123.57.149 140.123.5.100 DNS 74 Standard query 0xdd0f A www.ccu.edu.tw
232 2.486175 140.123.57.149 140.123.5.100 DNS 80 Standard query 0xffe2 A accounts.youtube.com
1126 8.203461 140.123.5.100 140.123.57.149 DNS 225 Standard query response 0x265e A www.bing.com CNAME www-www.bing.com.trafficmanager.
1127 8.204312 140.123.5.100 140.123.57.149 DNS 254 Standard query response 0x304c HTTPS www.bing.com CNAME www-www.bing.com.trafficmana
340 3.541653 140.123.5.100 140.123.57.149 DNS 109 Standard query response 0xdd0f A www.ccu.edu.tw CNAME nweb.ccu.edu.tw A 140.123.13.2
233 2.487794 140.123.5.100 140.123.57.149 DNS 124 Standard query response 0xffe2 A accounts.youtube.com CNAME www3.l.google.com A 142.
Additional RRs: 0
Queries
www.ccu.edu.tw: type A, class IN
Name: www.ccu.edu.tw
[Name Length: 14]
[Label Count: 4]
Type: A (1) (Host Address)
Class: IN (0x0001)
Answers
www.ccu.edu.tw: type CNAME, class IN, cname nweb.ccu.edu.tw
nweb.ccu.edu.tw: type A, class IN, addr 140.123.13.215
[Request In: 338]
[Time: 0.001689000 seconds]
0000 74 13 ea 35 8d ce cc d3 42 aa d4 1f 08 00 45 00
0010 00 5f 2d 79 00 00 fe 11 37 25 8c 7b 05 64 8c 7b
0020 39 95 00 35 d1 e6 00 4b 29 52 dd 0f 81 80 00 01
0030 00 02 00 00 00 00 03 77 77 77 03 63 63 75 03 65
0040 64 75 02 74 77 00 00 01 00 01 c0 0c 00 05 00 01
0050 00 00 0b 3c 00 07 04 6e 77 65 62 c0 10 c0 2c 00
0060 01 00 01 00 00 0b 4b 00 04 8c 7b 0d d7
Domain Name System: Protocol
Packets: 1318 · Displayed: 8 (0.6%) · Dropped: 0 (0.0%)
Profile: Default

3. Fix the network problem

Q1: What are the reasons of when PC1 pings PC2 in the provided pkt, it shows “Request time out”?

A1:

1. At 11:27 in this video,teacher was dealing with pinging to “My PC”. But he failed. He modified the RIP settings on two routers. So we checked the RIP settings of NTU Router and CCU Router, we found they were incorrect (Fig. 5). The RIP setting of NTU Router needs to add the section circled in blue, while the RIP setting of CCU Router should include the section circled in orange, as shown in Fig. 6.

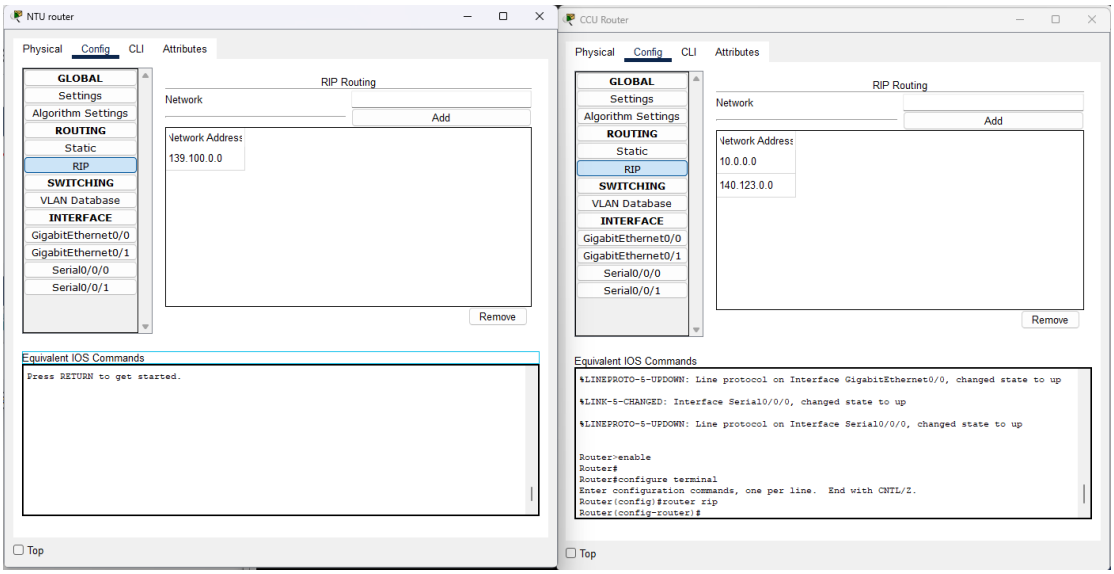


Fig. 5

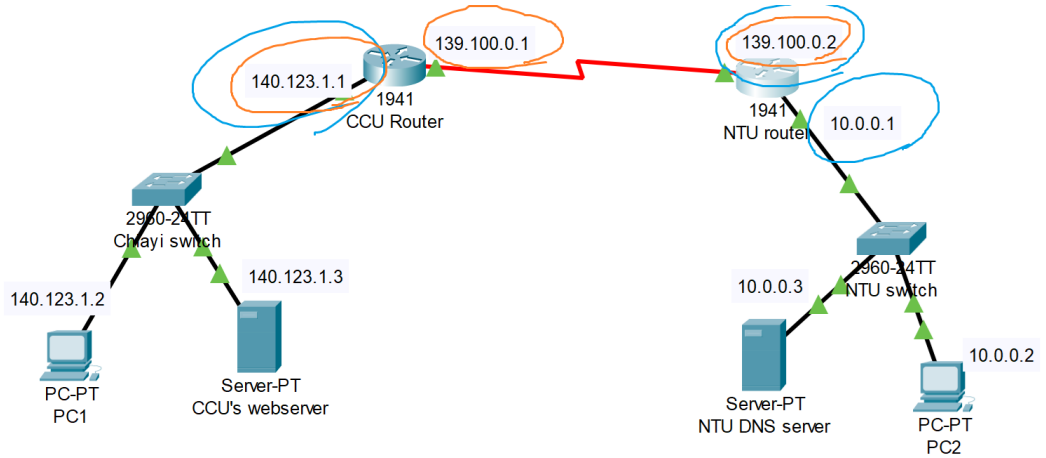
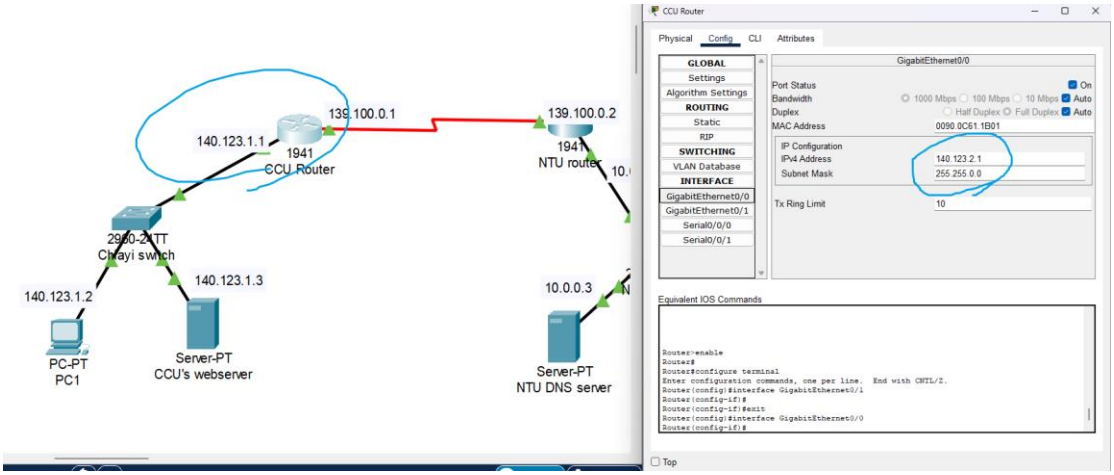


Fig. 6

2. The IP Configuration of CCU Router is wrong(Fig. 7)



(Fig. 7)

Q2: How to fix the above problem? Show screenshots to proof how you fix to let PC1 ping PC2 successfully.

A2: We need to modified two routers. In Figures 8, 9, and 10, the left side shows the configuration before modification, and the right side shows the configuration after modification.

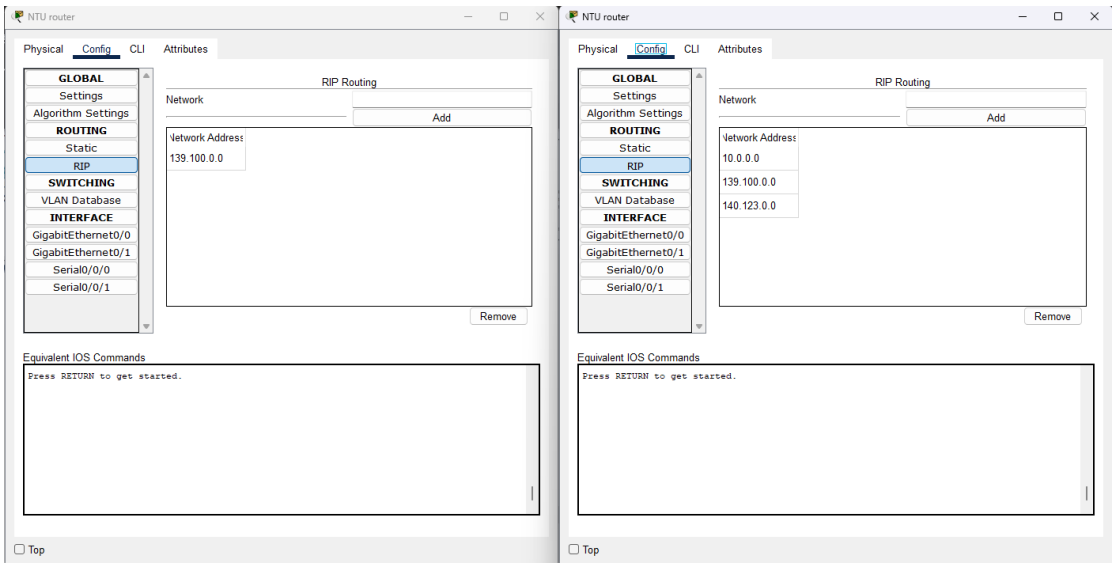


Fig. 8

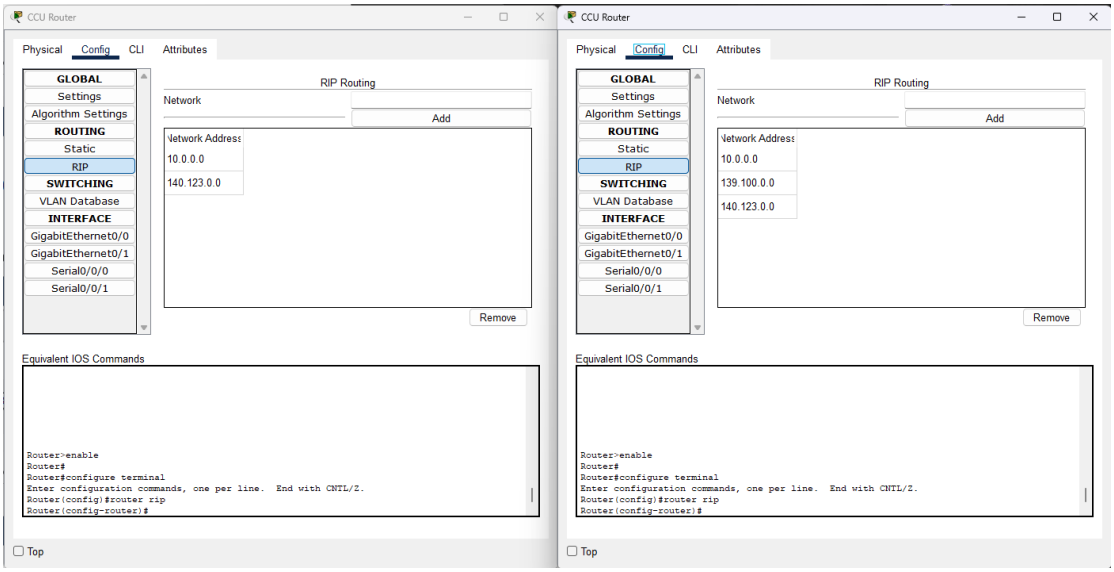


Fig. 9

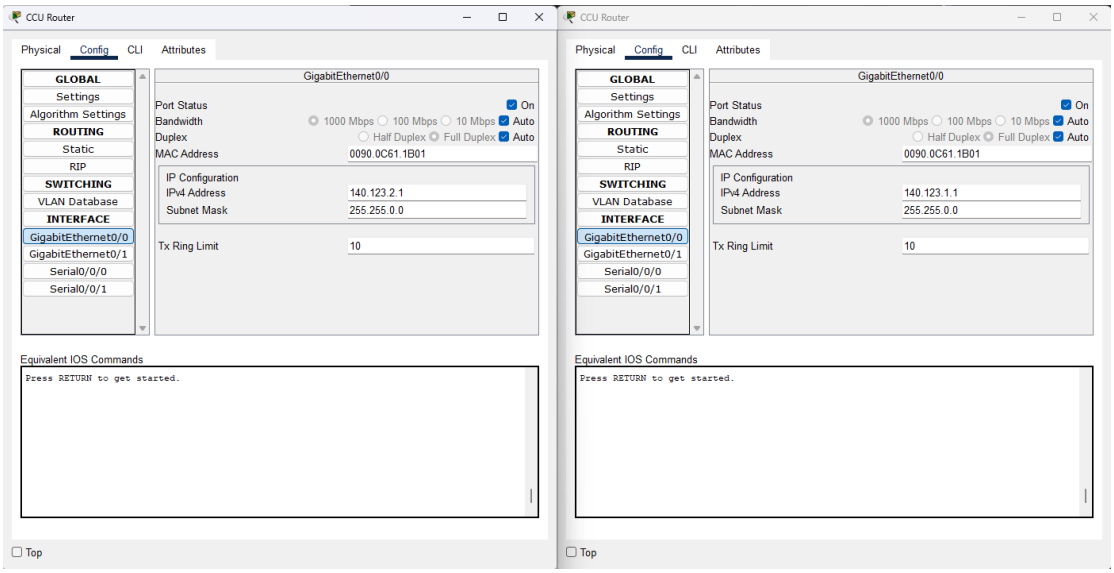
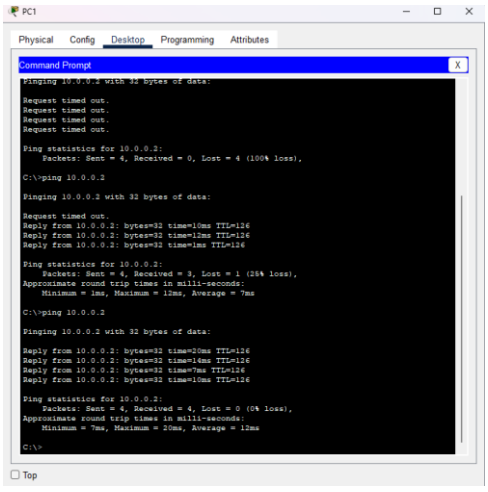


Fig. 10

Now we can use PC1 to ping PC2!



Reference：

https://www.youtube.com/watch?v=9-sXlykDSs4
https://www.youtube.com/watch?v=3f9z-upxqW4&t=12s
https://www.youtube.com/watch?v=Bl6dZJq_Wc0&t=274s
https://www.computernetworkingnotes.com/ccna-study-guide/extended-acl-configuration-commands-explained.html
https://www.cisco.com/c/zh_tw/support/docs/security/ios-firewall/23602-confaccesslists.html
https://support.hpe.com/techhub/eginfolib/networking/docs/switches/RA/15-18/5998-8151_ra_2620_asg/content/ch10s09.html
https://lobotsai.blogspot.com/2012/03/ccna_10.html