Лабораторийн ажил №8

МТЭС, МКУТ, Компьютерийн ухаан

Б.Барсболд, 22B1NUM4397

Ажлын зорилго

Энэхүү ажлаар бид хост болон холболтын төхөөрөмжүүдийн сүлжээний орчин дахь ажилгаа шалгах үүрэг бүхий ICMP протокол болон ARP гэсэн 2 протоколуудын онцлогтой танилцана.

Онолын судалгаа

Internet Control Message Protocol (ICMP) нь чиглүүлэгч төхөөрөмжүүд болон хостууд хоорондоо network-layer-ийн мэдээллүүдийг хоорондоо дамжуулах зорилгоор ашиглагддаг. Хамгийн түгээмэл хэрэглэгддэг ICMP-ийн жишээ бол алдаа мэдээллэх юм. ICMP мэдээлэл нь UDP болон TCP-ийн адил IP датаграм дотор зөөвөрлөгддөг.

ICMP мессежүүд төрөл болон код гэсэн талбаруудаас гадна ICMP мессеж явахад хүргэсэн IP датаграмын header хэсэг болон эхний 8 байтыг агуулдаг.

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

Зураг 1 ICMP мессежийн төрлүүд

Туршилт

1. ping

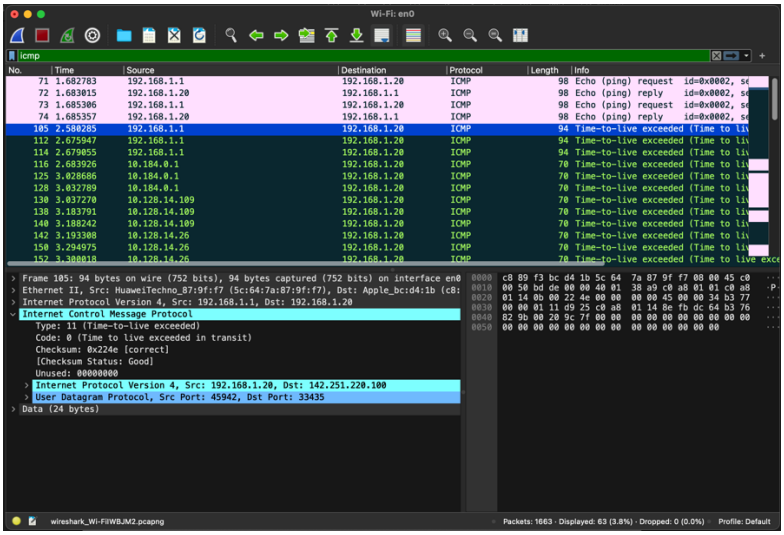
```
❯ ping -c 10 google.com
PING google.com (142.250.66.142): 56 data bytes
64 bytes from 142.250.66.142: icmp_seq=0 ttl=55 time=59.996 ms
64 bytes from 142.250.66.142: icmp_seq=1 ttl=55 time=94.211 ms
64 bytes from 142.250.66.142: icmp_seq=2 ttl=55 time=139.179 ms
64 bytes from 142.250.66.142: icmp_seq=3 ttl=55 time=129.208 ms
64 bytes from 142.250.66.142: icmp_seq=4 ttl=55 time=175.445 ms
64 bytes from 142.250.66.142: icmp_seq=5 ttl=55 time=321.607 ms
64 bytes from 142.250.66.142: icmp_seq=6 ttl=55 time=139.305 ms
64 bytes from 142.250.66.142: icmp_seq=7 ttl=55 time=60.760 ms
64 bytes from 142.250.66.142: icmp_seq=8 ttl=55 time=65.652 ms
64 bytes from 142.250.66.142: icmp_seq=9 ttl=55 time=83.003 ms

--- google.com ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 59.996/126.837/321.607/74.950 ms
```

Зураг 2 ping команд ашиглан google.com руу echo хүсэлт явуулж буй байдал

```
> Frame 268: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Apple_bc:d4:1b (c8:89:f3:bc:d4:1b), Dst: HuaweiTech
> Internet Protocol Version 4, Src: 192.168.1.20, Dst: 142.250.66.142
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0dde [correct]
    [Checksum Status: Good]
    Identifier (BE): 37169 (0x9131)
    Identifier (LE): 12689 (0x3191)
    Sequence Number (BE): 8 (0x0008)
    Sequence Number (LE): 2048 (0x0800)
    [Response frame: 269]
    Timestamp from icmp data: Apr 24, 2024 23:18:05.713988000 +08
    [Timestamp from icmp data (relative): 0.000294000 seconds]
  > Data (48 bytes)
```

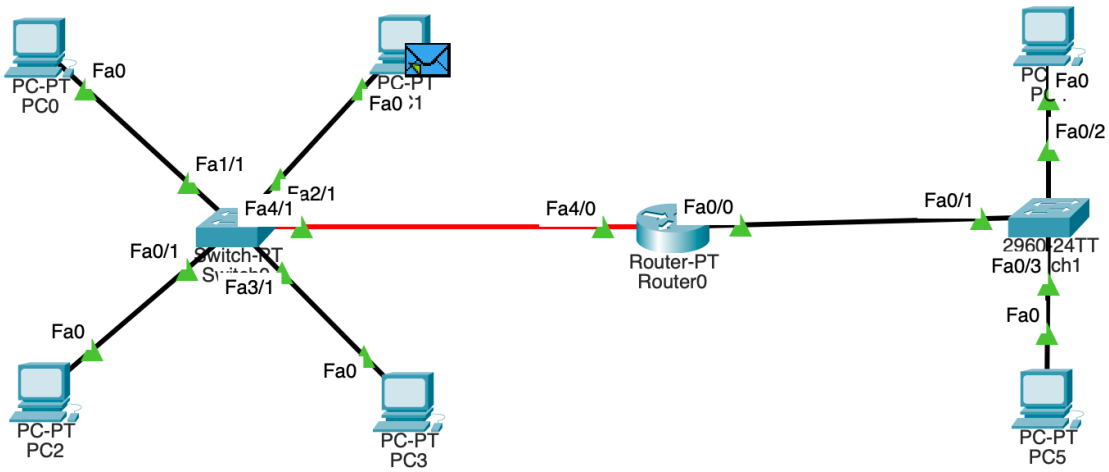
Зураг 3 Туршилтын ICMP мессежийн бүтэц

2. tracert



Зураг 4 traceroute командын үр дүн wireshark програм дээр

3. ARP



Зураг 5 Туршилтын топологийг байгуулсан байдал

Даалгавар

ICMP Анализ хийх

1. ping комманд ашиглан холболтыг шалгаж байгаа үеийн пакетийг задалж ICMP мессежийн type, code хэсгээс мессежийг тайлбарла.

ICMP мессежийн type, code хэсгийг харвал type=8, code=0 байна. Үүнийн Зураг 1-с харвал echo request мессеж байна.

2. tracert комманд ашиглан холболтыг шалгаж байгаа үеийн пакетийг задалж ICMP мессежийн type, code хэсгээс мессежийг тайлбарла.

ICMP мессежийг харвал type=11, code=0 байна. Үүнийг Зураг 1-с харвал TTL expired буюу хүрэх газар очхоос өмнө TTL нь 0 болсон гэсэн үг.

3. Дээрхи хоёр үр дүнгээс ялгаатай болон ижил зүйл байна уу? Тайлбарла.

Ижил төрөл нь хоёул ICMP мессеж байгаа хэдий ч мессежийн type хэсэг нь өөр байна. Учир нь нэг нь холболт амжилттай болсон үгүйг шалгах зорилготой бол нөгөө нь мессеж бүрийн TTL-г 1-р нэмэгдүүлэх замаар бүх дамжих замыг тодорхойлох юм.

ARP Анализ хийх

1. Pc0-ийн ARP Table-д нь IP болон MAC хаягууд-ын жагсаалтыг ажиглан тайлбар хий.

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           0002.16a0.0509        dynamic
```

Зураг 6 PC0-ийн ARP table

Энд бид PC1 руу зөвхөн ICMP мессеж илгээсэн тул зөвхөн энэ хостын IP хаяг болон MAC хаяг байна. Энэ record нь switch broadcast хэлбэрээр ARP мессеж илгээх үед буцаан хариу өгсөн хостийн MAC хаягийг аван хадгалсан.

2. Яагаад ARP request-ийг broadcast хэлбэрээр switch-ний портоос гаргаж байна вэ?

Swtich хамгийн эхэнд асаад бусад хостуудтай холбогдсон үед өөрийгөө ямар MAC хаягтай хостуудтай холболгдсон байгааг мэдэхгүй тул хамгийн эхэнд ARP request-г broadcast хэлбэрээр өөрт холбогдсон бүх төхөөрөмжүүдрүү явуулна. Хэрэв тухайн IP хаягтай төхөөрөмж өөртэй нь ямар нэгэн интерфейсээр холбогдсон байвал буцаан хариу өгч үүнийгээ ямар MAC хаягтай төхөөрөмжрүү явуулахаа мэддэг.

3. Сүлжээн дээр ямар төхөөрөмжүүд ARP request-г хүлээн авах вэ?

Бүх төрлийн хостууд болон чиглүүлэгч төхөөрөмжүүд хүлээн авна.

4. ARP Reply-ийг илгээж байгааг төхөөрөмж яаж мэддэг вэ?

Switch нь OSI моделийн 2-р түвшинд ажилдаг тул шууд ARP протоколтой харьцаж чадахгүй. Тэгхээр switch broadcast эсвэл unicast эсэхийг ялгаж чаддаг ба ARP request-г эхлүүлсэн төхөөрөмж рүү unicast хэлбэртэй явж буй мессежийг ARP reply гэж ялгаж чаддаг.