8 ICMP, ARP ПРОТОКОЛ

**О.Энэрэл 22B1NUM0506**

**МТЭС, Програм хангамж**

# Ажлын зорилго

Энэ ажлаар хост болон холболтын төхөөрөмжүүдийн сүлжээний орчин дахь ажиллагааг шалгах үүрэгтэй ICMP болон ARP протоколуудын ажиллагааг судална.

# Туршилт

* + 1. ICMP протокол ба ping командf

Доорх алхамуудын дагуу [www.google.com](http://www.google.com/) руу холбогдох холболтын мэдээллийг ping ашиглан цуглуулаарай.

1. Командын мөртэй ажиллах талбарыг нээнэ.
2. Wireshark программыг нээж пакетуудыг барьж авах процессыг эхлүүлнэ.
3. Командын мөр дээр “ping -n 10 google.com” командыг бичнэ. -n 10 нь 10 хяналтын мессежийг илгээнэ (-ийг харна уу).

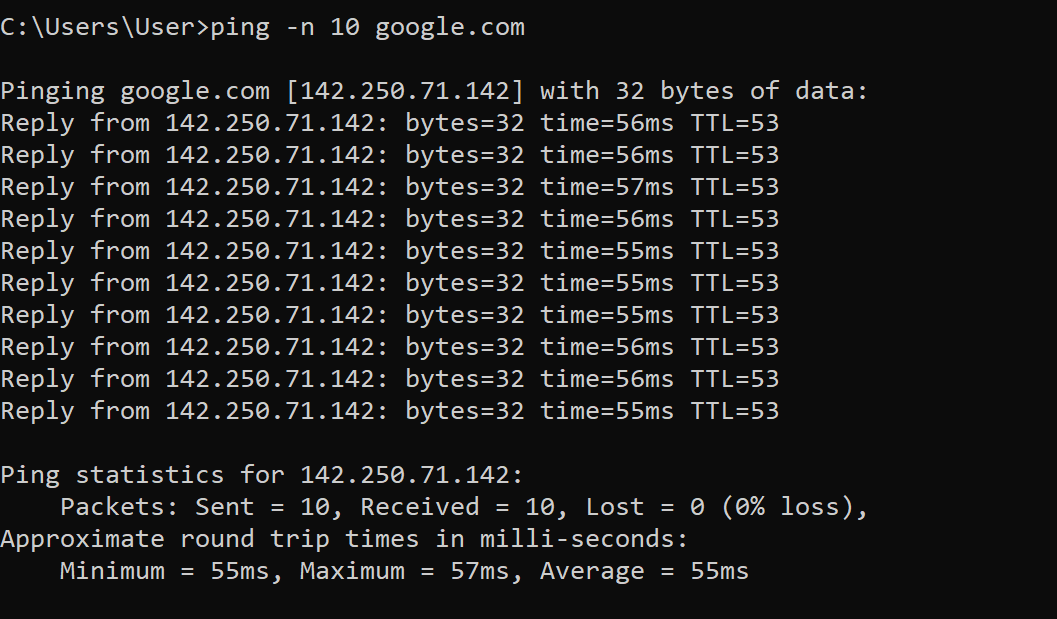


Figure 1 ping -n 10 google.com

1. Ping команд дууссаны дараа Wireshark программын барьж авах процессыг зогсооно.
   * 1. ICMP протокол ба tracert команд

Доорх алхамуудын дагуу [www.google.com](http://www.google.com/) руу холбогдох замын талаарх мэдээллийг цуглуулаарай.

1. Командын мөртэй ажиллах талбарыг нээнэ.
2. Wireshark программаа нээж пакетуудыг барьж авах процессыг эхлүүлнэ.
3. Командын мөр дээр “tracert google.com” командыг бичнэ.
4. tracert команд дууссаны дараа Wireshark программын бичих процессыг зогсооно.

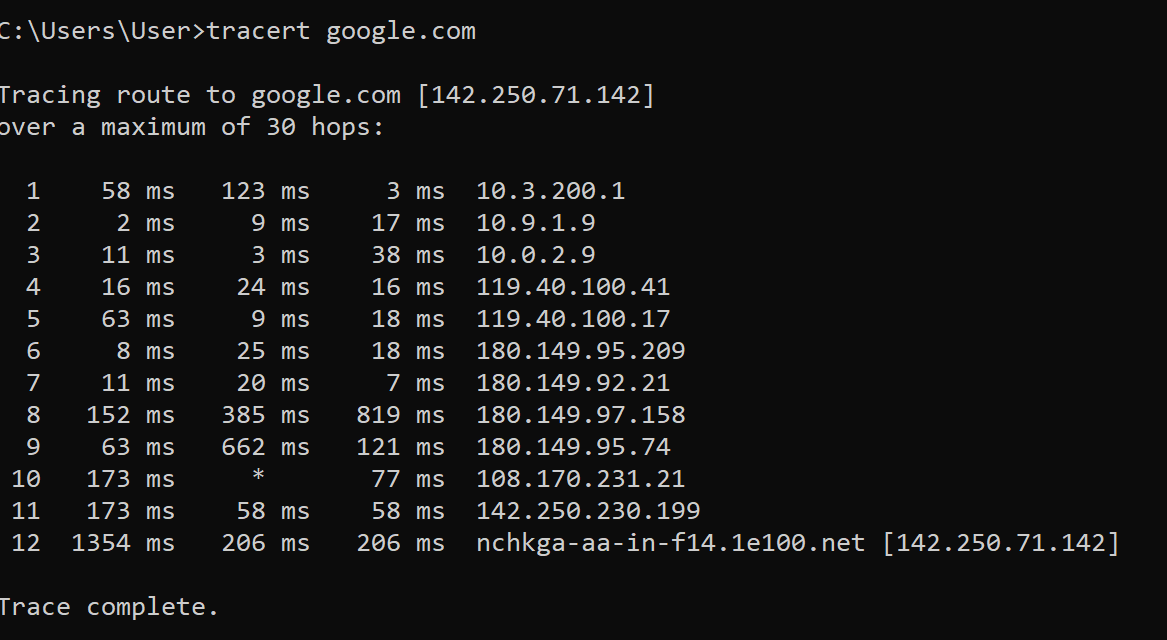


Figure 2 tracert google.com

Туршилтаар цуглуулсан ICMP урсгалын .pcap өргөтгөлтэй файлаас ICMP протоколоор шүүж дамжсан мессежнүүдийн ялгааг тайлбарлана. Үүнд:

1. ping команд ашиглан илгээсэн Echo request мессежийг задалж, ICMP мессежний type, code хэсгийг тайлбарла.

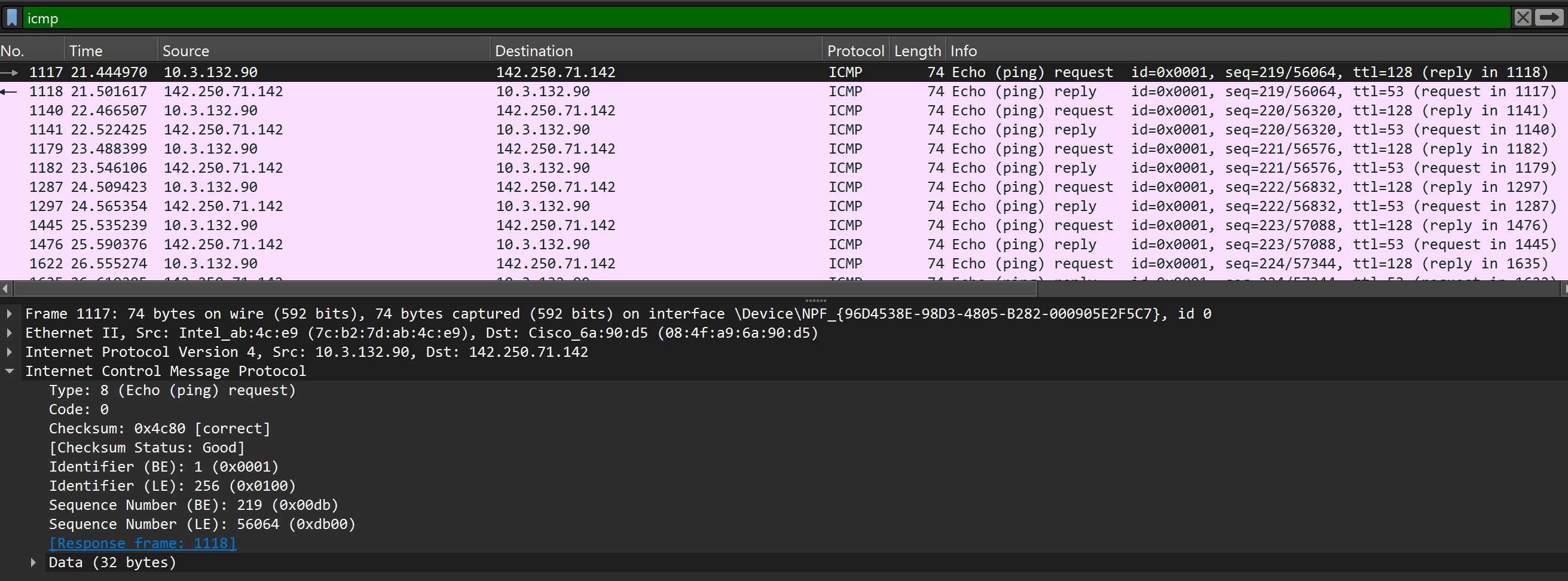


Figure 3 echo request message

Type = 8 энэ нь ICMP echo request-ийг заана.

Code = 0 ямар нэгэн алдаагүйг илэрхийлнэ.

1. tracert команд ашиглан илгээсэн Echo request мессежийг задалж, ICMP мессежний type, code хэсгээс тайлбарла.

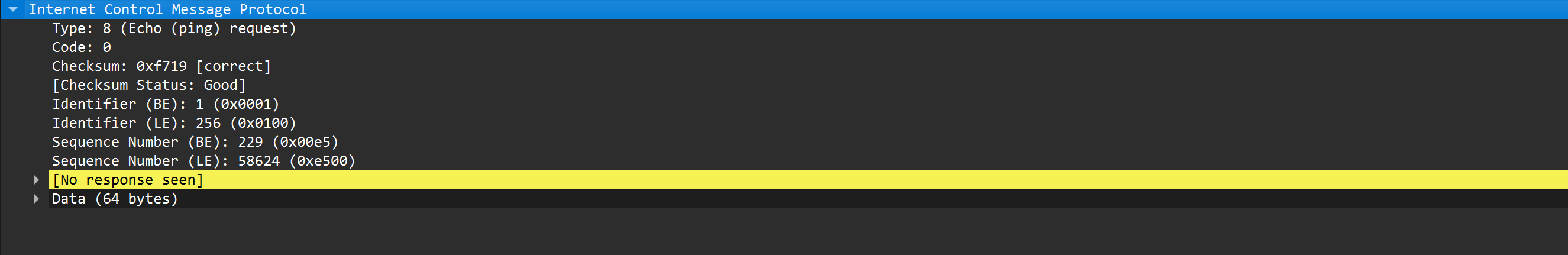


Figure 4 tracert

Type = 8 энэ нь ICMP echo request-ийг заана.

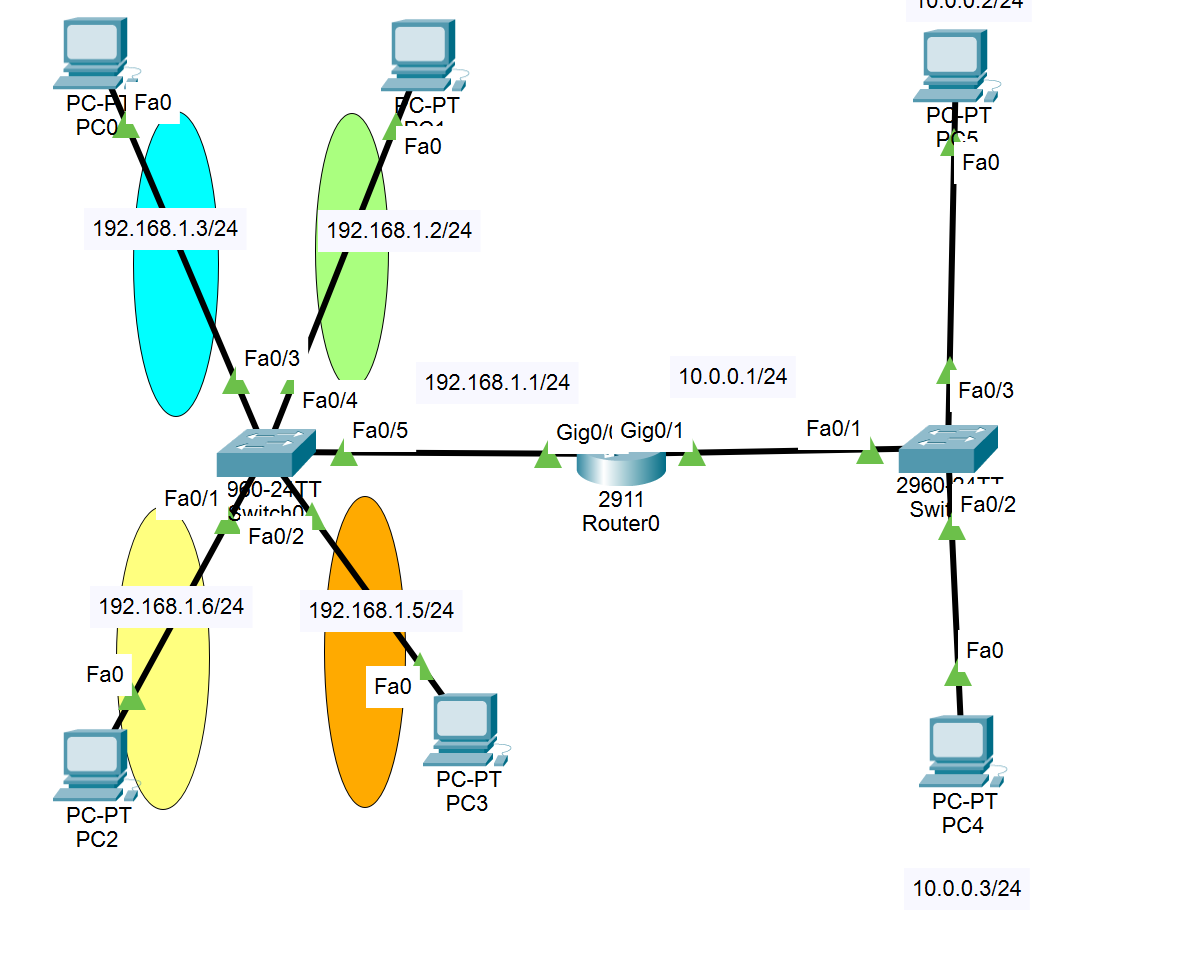
Code = 0 ямар нэгэн алдаагүйг илэрхийлнэ.

1. Дээрх хоёр үр дүнгээс ялгаатай болон ижил зүйл байна уу? тайлбарлана уу.

Type, code, identider нь ижил checksum，sequence number，data нь өөр байсан.

* + 1. ARP протокол

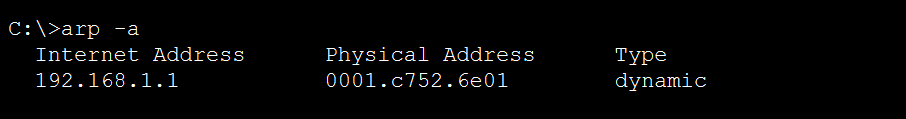
Дотоод сүлжээнд дамжуулж байгаа ARP пакет болон сүлжээ хооронд дамжуулж байгаа ARP пакетыг ажиглан мессеж хэрхэн дамжиж байгааг судална. Зураг 8-5-т харуулсан топологийг байгуулж сүлжээнд харуулсан IP хаягуудаар төхөөрөмжийг хаяглана.



Зураг 8.5 Туршилтын топологи 1

Симуляцийн горимоос Event List Filter-ийг ашиглаад зөвхөн ARP, ICMP протоколуудыг сонгоно. Симуляцийн горимд байх Auto Capture/Play ашиглаад ARP хүсэлтийн мессеж хэрхэн дамжиж байгааг судлаад тайланд оруулна.

Дамжиж буй мессежүүдийг ажиглаад дараах асуултуудад хариулна.

1. PC0-ийн ARP table-д нь IP болон MAC хаягуудын жагсаалтыг ажиглан тайлбарла.

PC0-ийн ARP table -д router-ийн gig0/0 interface -ийн IP, MAC хаяг бичигдсэн байна.

1. Яагаад ARP request-ийг Switch0- ээс broadcast хэлбэрээр илгээж байгаа вэ?

Switch-0 нь хүлээн авагчийн IP хаягтай таарах MAC хаягийг мэдэхгүй байгаа тул бүх төхөөрөмжүүд рүү Broadcast -аар ARP request-ийг илгээж байна.

1. ARP request-ийг сүлжээний ямар төхөөрөмжүүд хүлээн авах вэ?

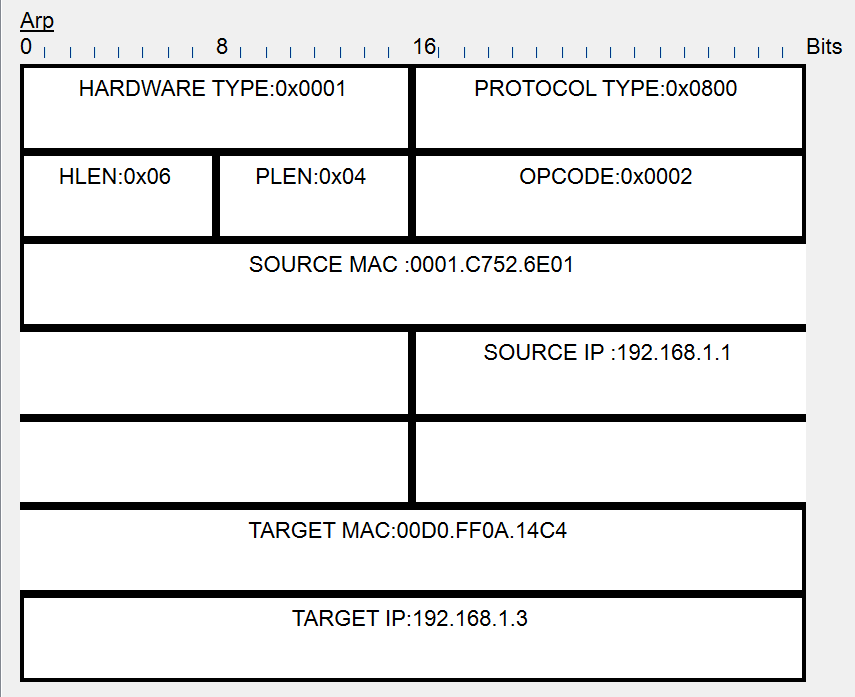
Switch-тэй холбогдсон бүх төхөөрөмжүүдэд ARP request очино, гэхдээ ARP header-ийн target protocol address-тай төхөөрөмж ARP request-ийг хүлээж авна.

1. ARP reply-ийг илгээж байгааг төхөөрөмж хэрхэн мэдэх вэ?

ARP хүсэлтийг хүлээн авсан төхөөрөмжүүд нь өөрийн IP хаягийг ARP хүсэлтэд заасан IP хаягтай харьцуулна. Хэрэв тохирч байвал тухайн төхөөрөмж өөрийн MAC хаягийг ашиглан ARP reply -г unicast-аар илгээнэ. ARP reply гэдгийг ARP header-ийн operation талбараас мэдэх боломжтой.

OPCODE: 0x0002 🡪 ARP Reply

OPCODE: 0x0001 🡪 ARP Request



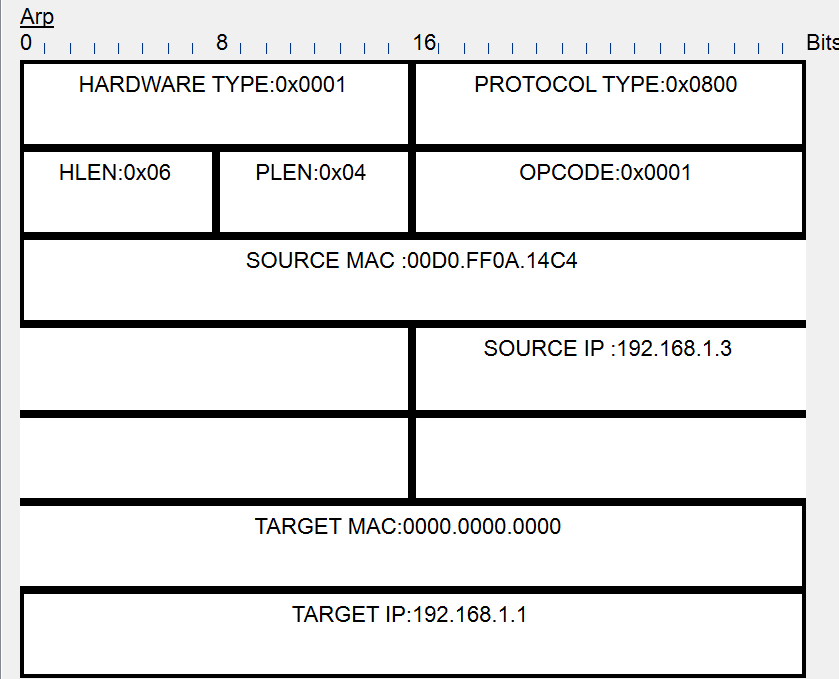
1. Сүлжээний дээрх топологиор пакет дамжуулахад MAC хаягд ямар өөрчлөлт ажиглагдаж байна вэ?

ARP reply ирэх хүртэл source MAC address ARP request илгээгчийн MAC address байж target MAC address нь 0000.0000.0000, ARP reply ирхэд source MAC address нь ARP reply илгээсэн төхөөрөмжийн MAC address болж ARP request илгээсэн төхөөрөмжийн MAC address нь target MAC address болно.

1. Рүтер яагаад ARP request-ийг үүсгэж Gig0/1 портоор дамжуулж байгаа вэ?

Router0 нь өөрийн холбогдсон сүлжээнд байгаа төхөөрөмжүүдийн MAC хаягийг олохын тулд ARP хүсэлт илгээнэ. Жишээлбэл, Router0 нь 10.0.0.2 IP хаягтай PC5-тай харилцах хэрэгтэй бол түүний MAC хаягийг олохын тулд Gig0/1 портоор ARP request илгээнэ.

# Сорих асуулт

1. Дараах мессежүүдийн бүтцийг судлаад тайланд оруулна уу.
   1. ARP Request

Hardware type: 0x0001 🡪 Ethernet-ийг заана.

Protocol type: 0x0008 🡪 IPv4 protocol

Hardware Length: 0x06 🡪 MAC хаягын урт

Protocol Length: 0x04 🡪 IP хаягын урт

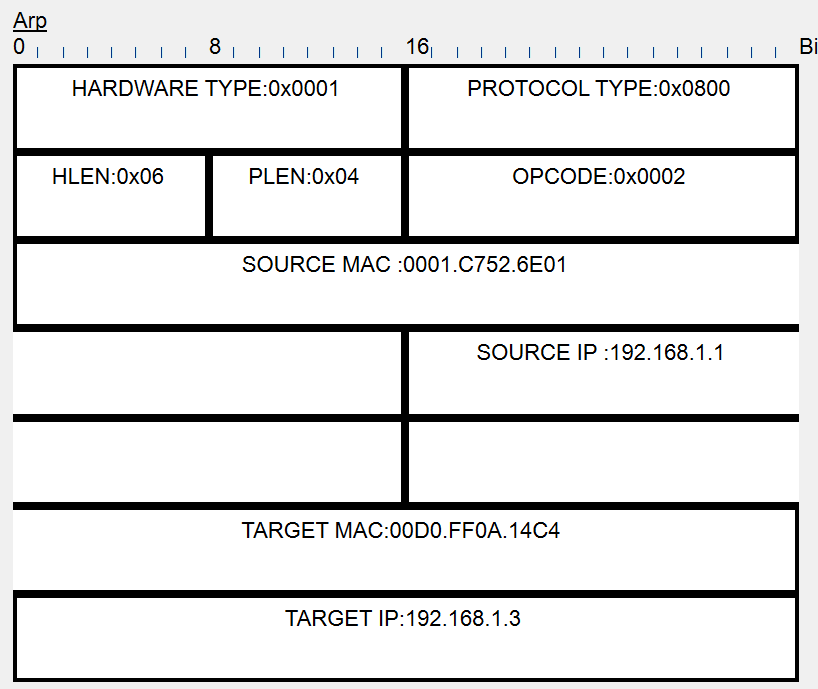
Opcode: 0x0001 🡪 ARP request

Source MAC: ARP request илгээгчийн МАС хаяг

Source IP：ARP request илгээгчийн IP хаяг

Target MAC :0000.0000.0000🡪 broadcast -аар илгээж байна.

Target IP：ARP request хүлээн авагчийн IP хаяг.

* 1.  ARP Reply

Hardware type: 0x0001 🡪 Ethernet-ийг заана.

Protocol type: 0x0008 🡪 IPv4 protocol

Hardware Length: 0x06 🡪 MAC хаягын урт

Protocol Length: 0x04 🡪 IP хаягын урт

Opcode: 0x0002 🡪 ARP reply

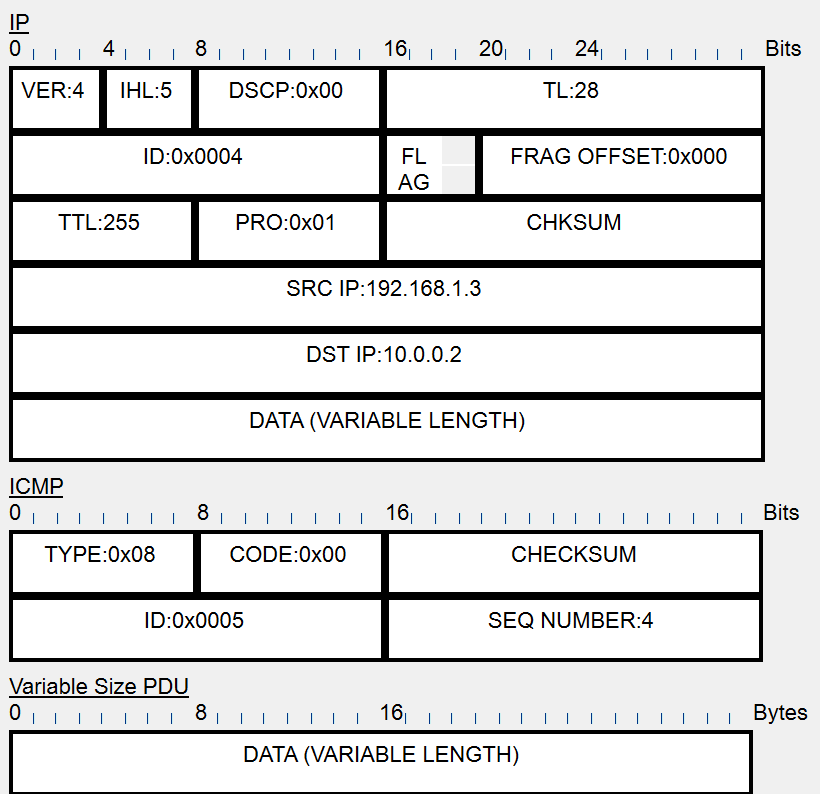
Source MAC: ARP reply илгээгчийн МАС хаяг

Source IP：ARP reply илгээгчийн IP хаяг

Target MAC : ARP reply -г хүлээн авах төхөөрөмжийн MAC хаяг тухайлбал ARP request илгээгчийн MAC хаяг

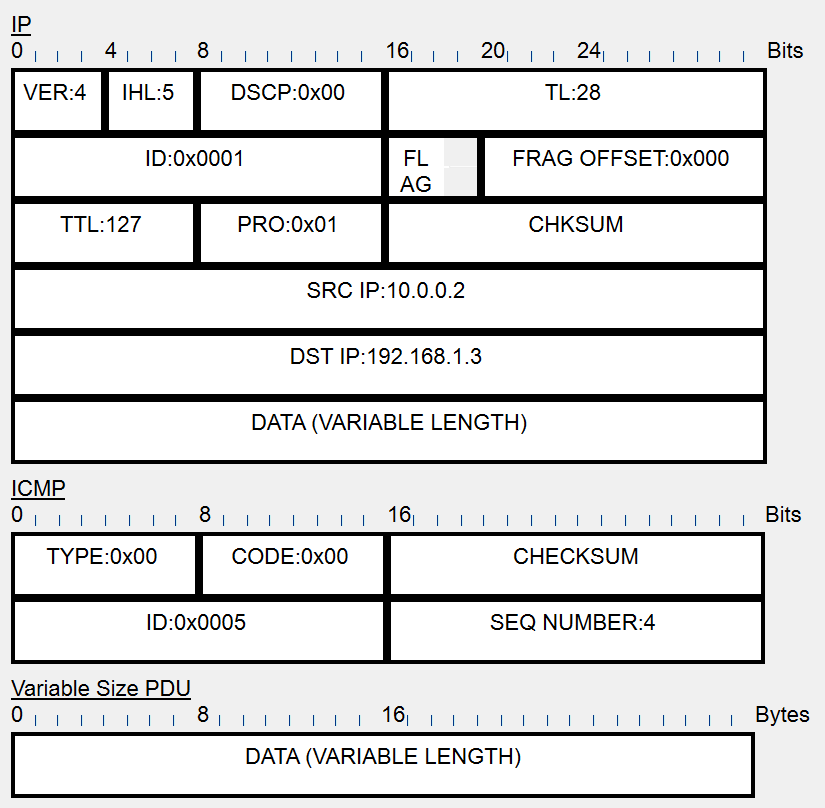
Target IP：ARP reply-г хүлээн авах төхөөрөмжийн IP хаяг.

* 1. ICMP Echo Request (PC0-ээс)



PC0-PC4 руу ICMP echo request илгээж байна.

* 1. ICMP Echo Reply (PC0-ээс)



PC4-ээс РС0 руу ICMP Echo Reply илгээж байна.

1. ARP request-ийн хүлээн авагч MAC хаяг ямар байх вэ?

FFFF.FFFF.FFFF (0000.0000.0000) байсан.

**Дүгнэлт:**

Энэхүү лабораторийн ажлаар ARP болон MAC хаяг хэрхэн ажиллладаг талаар судалж, топологи байгуулан туршилт хийлээ. ARP нь дотоод сүлжээн дэх төхөөрөмжийн MAC хаягийг олж өгдөг. Төхөөрөмж нь сүлжээнд холбогдсон хоёр төхөөрөмж хооронд дамжуулал хийгдэхийн тулд IP хаяг болон МАС хаяг нь хэрэгтэй. Илгээгч хост хүлээн авагч хостын IP хаяг дээр тулгуурлан MAC хаягийг нь тодорхойлдог. ARP нь үндсэн хоёр төрлийн мессежтэй. ARP request, ARP reply. Request нь broadcast- р дамжуулагдана. Reply нь unicast дамжуулалтай