**Модуль 2**

**Дамжуулалтын түвшин**

**Сүлжээний түвшин**

**IP хаягын төлөвлөлт**

**ШУТИС. КТМС. Багш П.Бумдүүрэн / магистр /**

**Гарчиг**

1. Дамжуулалтын түвшин……………………………………………………………. 4

1.1 Дамжуулалтын түвшний протокол, түүний үүрэг……………………... 6

1.2 UDP (найдваргүй дамжуулалттай протокол) гэж юу вэ?

түүний хэрэглээ……………………………………………………………. 8

1.3 Найдвартай дамжуулалтыг дэмжих

TCP (дамжуулалтыг хянах протокол ) механизм, хэрэглээг судлах………… ..11

1.4 SCTP ( Мессэж урсгалын дамжуулалтыг хянах протокол )…………… 17

2. Сүлжээний түвшин………………………………………………………………….22

2.1 Сүлжээний түвшний протокол, түүний үүрэг…………………………. 22

2.2 Рүүтер (Router) ба чиглүүлэлт хийх ……………..……………………… .23

2.3 Статик ба динамик хаяг ………………………………………………….. .27

3. IP хаягын төлөвлөлт ………………………………………………………………...30

3.1 IP хаягийн бүтэц……………………………………………………………. 30

3.2 Тооллын систем, хөрвүүлэлт…………………………………………….. ..32

3.3 Сабнет(Subnet) хаяг.……………………………………………………….. 36

3.4 Өгөгдсөн IP хаягаар дэд сүлжээн дэх төхөөрөмжүүдийн

IP хаягийг тооцоолох………………………………………………………. 38

3.5 Сүлжээний түвшний протоколыг тестлэх, шалгах………………………. 40

4. Лабораторийн ажил 6: Хэрэглээний болон дамжуулалтын түвшний

протоколын уялдаа холбоог судлах………………41

4.1 Даалгавар 1: Топологи тестлэх ба засах………………………………….. 42

4.2 Даалгавар 2: DNS, UDP, HTTP, TCP протоколуудын

уялдаа холбоог судлах……………………………………….43

5. Лабораторын ажил 7: Дамжуулалтын түвшний протоколыг

Wireshark програм дээр анализ хийх …………..…44

5.1 Даалгавар 1: Wireshark програм дээр анализ хийх …………………….. 44

5.2 Даалгавар 2: HTTP сервер програм……………………………………. …..45

* 1. Даалгавар 3: TCP холболт............................................................................. 48

6. Лабораторийн ажил 8: IP пакетийн чиглүүлэлт……………………………………49

6.1 Даалгавар 1: Рүүтерийн интерфейсийг тохируулах................................ 49

6.2 Даалгавар 2: Чиглүүлэлтийн хүснэгтийг судлах..................................... 50

6.3 Даалгавар 3: Статик чиглүүлэлт хийх.....................................................51

6.4 Даалгавар 4: IP пакетийн явах замыг судлах.......................................... 52

7. Лабораторын ажил 9: 2-тын тоон систем, хөрвүүлгэ, IP хаяг…………………. 53

7.1 Даалгавар 1: 2т, 10т-ын тооллын систем………………………………… .53

7.2 Даалгавар 2: IP хаяг, сабнэт маск, сүлжээний хаяг, бродкаст хаяг…….. 5699

7.3 Даалгавар 3: Сабнэт маск………………………………………………….. 58

7.4 Даалгавар 4: РТ симуляц…………………………………………………… 59

8. Лабораторийн ажил 10: IP хаягийн төлөвлөлт……………………………………. 60

8.1 Даалгавар 1: Эх сүлжээг дэд сүлжээнд хуваах,

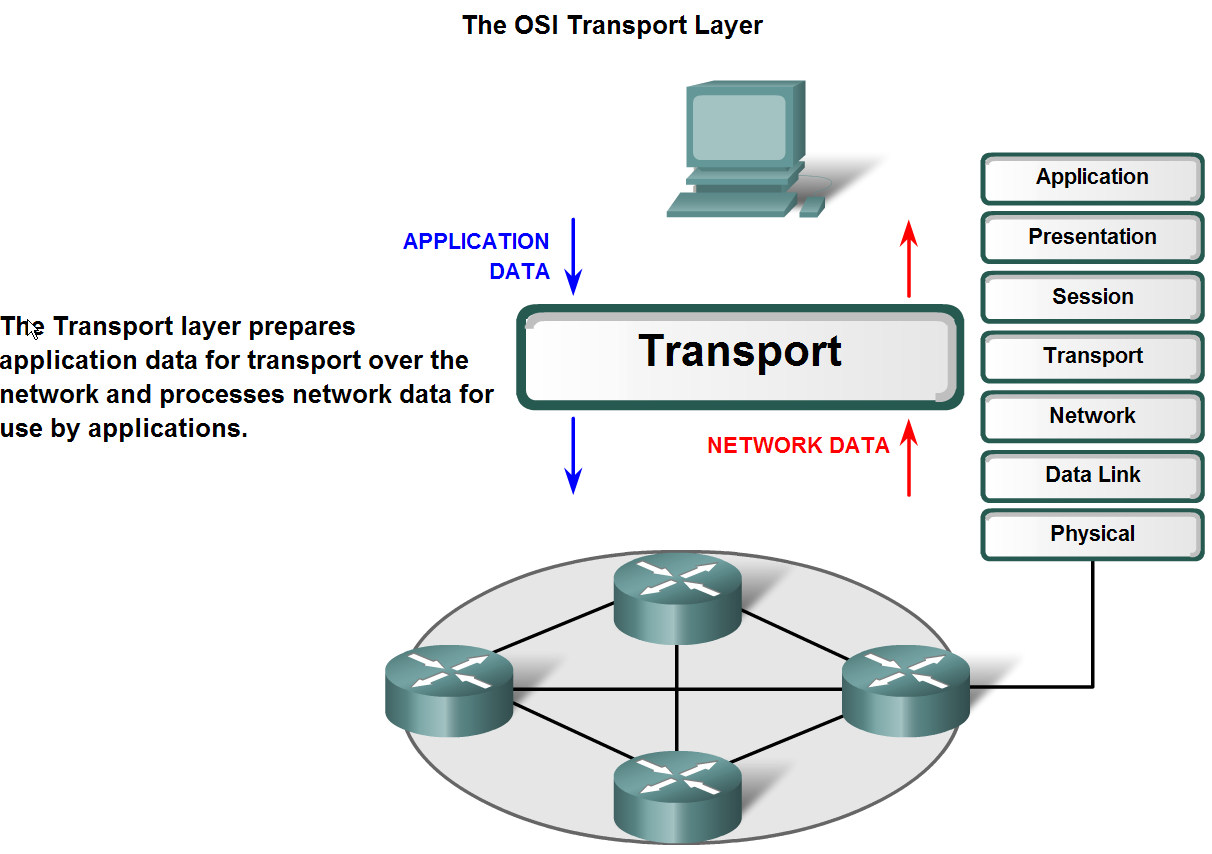
IP хаягийн тооцоо хийх…………………………………….. 62

8.2 Даалгавар 2: Пакет трэйсер (tracer) дээр сүлжээг угсрах.......................... 63

8.3 Даалгавар 3: Сүлжээний тохиргоо хийх.............................................. .....63

8.4 Даалгавар 4: Сүлжээг тестлэх................................................................... 63

1. **Дамжуулалтын түвшин**

****

Зураг 1.1.1 Дамжуулалтын түвшин

Энэ түвшинд мэдээллийн алдагдлыг илрүүлж засах, сүлжээн дээгүүр сегментийг end-to-end буюу эцсийн шатанд хүргэж өгөх үйлчилгээг зохицуулдаг. TCP, UDP протоколууд энэ түвшинд ажилладаг. Сегментийг эцсийн шатанд хүргэхэд 2 төрлийн протокол хэрэглэгддэг.

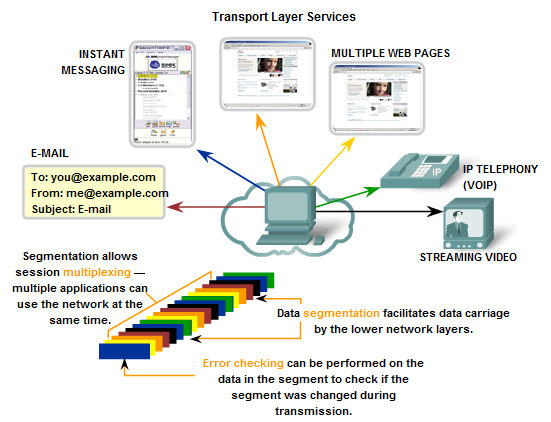
Үүнд:

* Connection-oriented (Холболт хандалтат)
* Connection-less (Холболт хандалтат бус)

гэсэн 2 төрлийн дамжуулалтын протокол байна.

Холболт хандалтат гэдэг нь өгөгдөл солилцохоос өмнө холболт урьдчилан тогтсон байдаг. Хүлээн авагч өгөгдлийг амжилттай хүлээн авснаа илгээгч компьютер руу мессежээр мэдэгдэнэ. Ингэснээр өгөгдлийг найдвартай хүргэх ба хүлээн авдаг. Баталгааны мессежийг илгээгч компьютер хүлээн аваагүй тохиолдолд өгөгдлөө дахин дамжуулдаг.

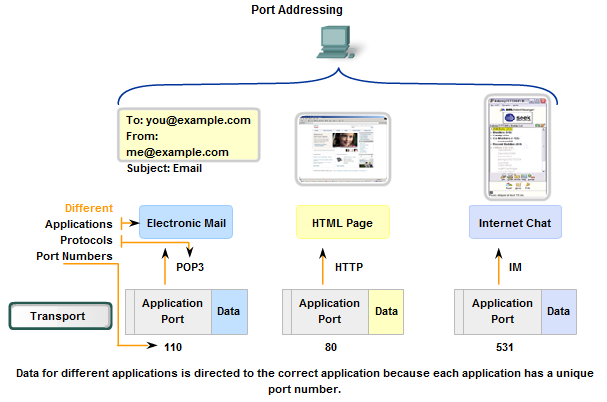
Холболт хандалтат бус гэдэг нь өгөгдөл дамжуулагдахын өмнө холболт тогтдоггүй бөгөөд өгөгдлийг ямар нэгэн баталгаагүйгээр шууд хүлээн авагч уруу дамжуулдаг. UDP нь холболт хандалтат бус протоколын жишээ юм.



Зураг 1.1.2 Дамжуулалтын түвшний сервис

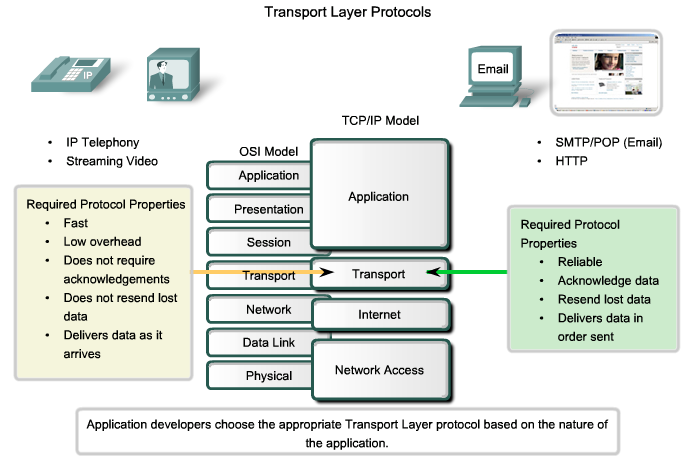
Дамжуулалтын түвшинд тест өгөгдөл, дуу хоолой, видео дүрс гэх мэт мэдээллийг дамжуулахад хэрэглэгддэг апплекэшн ( хэрэглээний програм хангамж ), сервисүүдийг хамгийн үр ашигтайгаар, тохирох протоколууд ашиглан дамжуулдаг бөгөөд хэрэглээний түвшний мессеж өгөгдлийг сегментэд хуваадаг. Өөрөөр хэлбэл дамжуулалтын түвшний PDU-г сегмент гэж нэрлэнэ.

Сүлжээний хост бүр дээр олон төрлийн апплекэшн, хэрэглээний түвшний сервис ажиллаж байдаг ба тэр бүрд тохирох портын дугаараар дамжуулалтын түвшинд ямар апплекэшн , сервис мэдээлэл дамжигдаж байгааг таньдаг.



Зураг 1.1.3 Портын хаяг

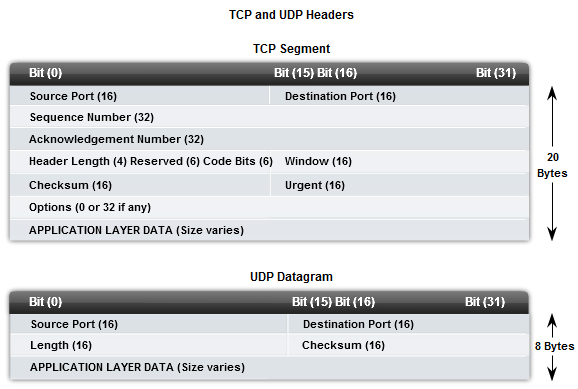
**1.1 Дамжуулалтын түвшний протокол, түүний үүрэг**



Зураг 1.1.2 Дамжуулалтын түвшний протокол

Дамжуулалтын түвшний протоколуудад дамжуулах гэж буй сервисээсээ хамаараад өөр өөр шаардлага тавигддаг. Жишээ нь: видео мэдээллийг яг тухайн агшинд дамжуулдаг учир хурдан, бага протоколын өгөгдлийн нэгжтэй, мессеж дамжсан эсэхийг баталсан баталгааны мессеж шаардлагагүй, алдагдсан мэдээллийг дахин дамжуулах шаардлагагүй байдаг.

Харин эсрэгээр и-мэйл үйлчилгээнд найдвартай, мессеж дамжсан эсэхийг баталсан баталгааны мессежтэй, алдагдсан мэдээллийг дахин дамжуулдаг, мэдээллийг дарааллын дагуу хүргэдэг гэх мэт шаардлагууд тавигддаг.



Зураг 1.1.2 Дамжуулалтын түвшний протоколууд

TCP/IP сүлжээний загварын хамгийн өргөн хэрэглэгддэг дамжуулалтын түвшний протоколууд нь Дамжуулалтыг хянах протокол (TCP) ба өгөгдлийг шууд дамжуулах протокол(UDP) юм. Энэ хоёр протоколын тусламжтай олон төрлийн апплекшэн, сервисүүд (програм , үйлчилгэээ ) сүлжээгээр дамждаг.

**Өгөгдлийг шууд дамжуулах протокол(UDP)**

UDP нь энгийн холболт хандалтат бус протокол юм. Давуу тал нь PDU-ийн хэмжээ бага бөгөөд хурдан.

UDP-г ашигладаг апплекэшн, сервисүүд:

* Domain Name System (DNS)
* Video Streaming
* Voice over IP (VoIP)

**Дамжуулалтыг хянах протокол (TCP)**

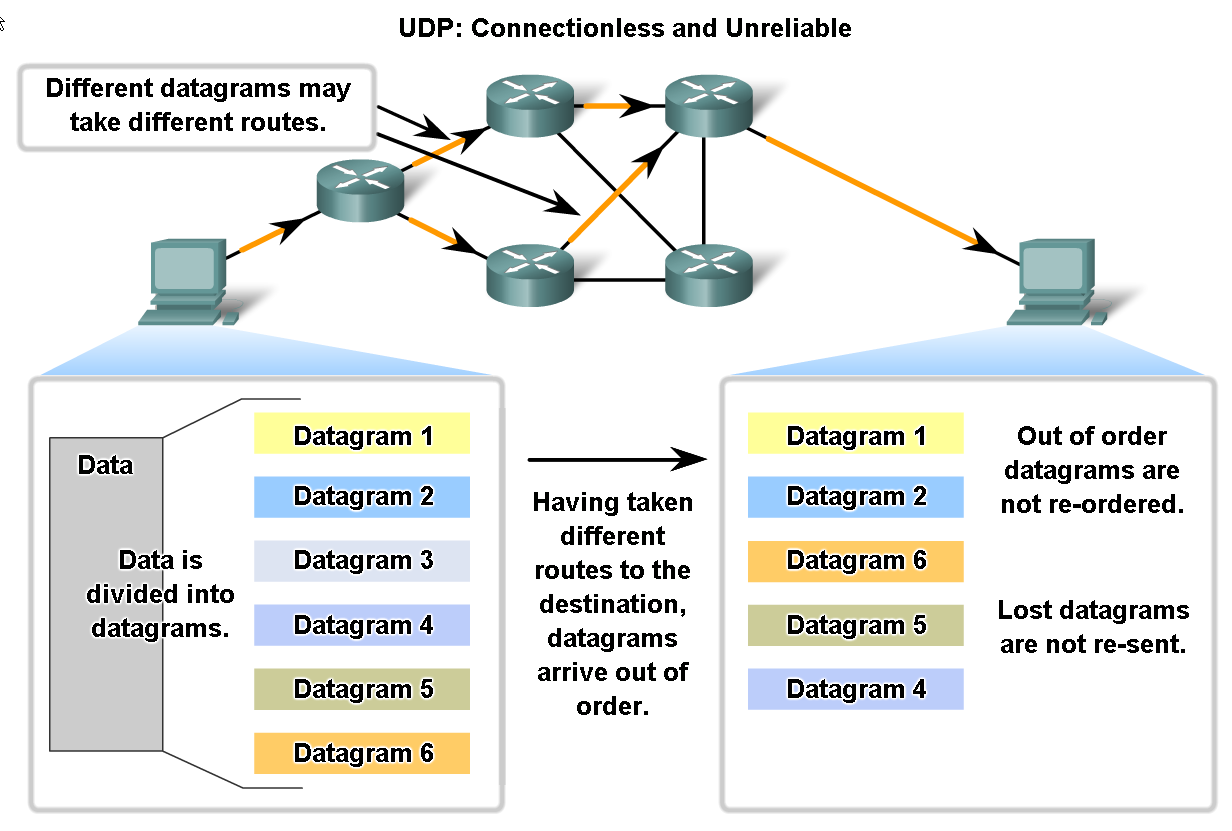
TCP нь холболт хандалтат протокол юм. Давуу тал нь мэдээллийг найдвартай дамжуулдаг, бөгөөд өгөгдлийн урсгалыг хянадаг.

TCP-г ашигладаг апплекэшн, сервисүүд:

* Web Browsers
* E-mail
* File Transfers

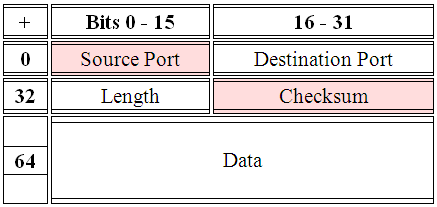
**1.2 Өгөгдлийг шууд дамжуулах протокол**

**User Datagram Protocol (UDP)**



Зураг 1.2.1 UDP протокол

Өгөгдлийг шууд дамжуулах протокол ( UDP ) нь TCP/IP интернэт сүлжээний дамжуулалтын түвшины протокол бөгөөд TCP шиг найдвартай дамжуулалтыг хангадаггүй тиймээс заримдаа Unreliable datagram protocol (өгөгдлийн найдваргүй дамжуулалтын протокол) гэж нэрлэгддэг.



Зураг 1.2.2 UDP сегментийн бүтэц

UDP толгой нь дөрвөн талбарыг агуулсан байна.

Source port – Дамжуулагчийн порт хаяг

Destination Port- Хүлээн авагчийн порт хаяг

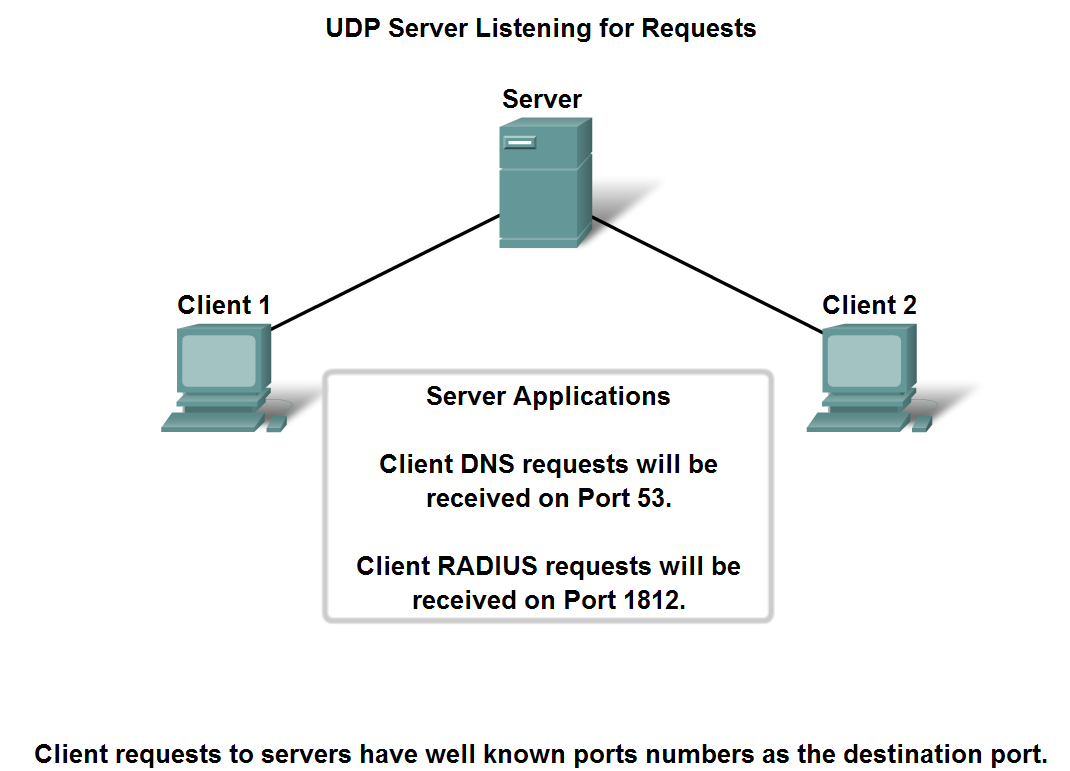
Length- UDP сегментийн ( өгөгдлийн багц) нийт хэмжээ байтаар.

Мин 8 байт. Мах 65535 байт

Checksum- 16 bit урттай энэ талбар нь пакетийн алдааг шалгахад зориулагдсан.

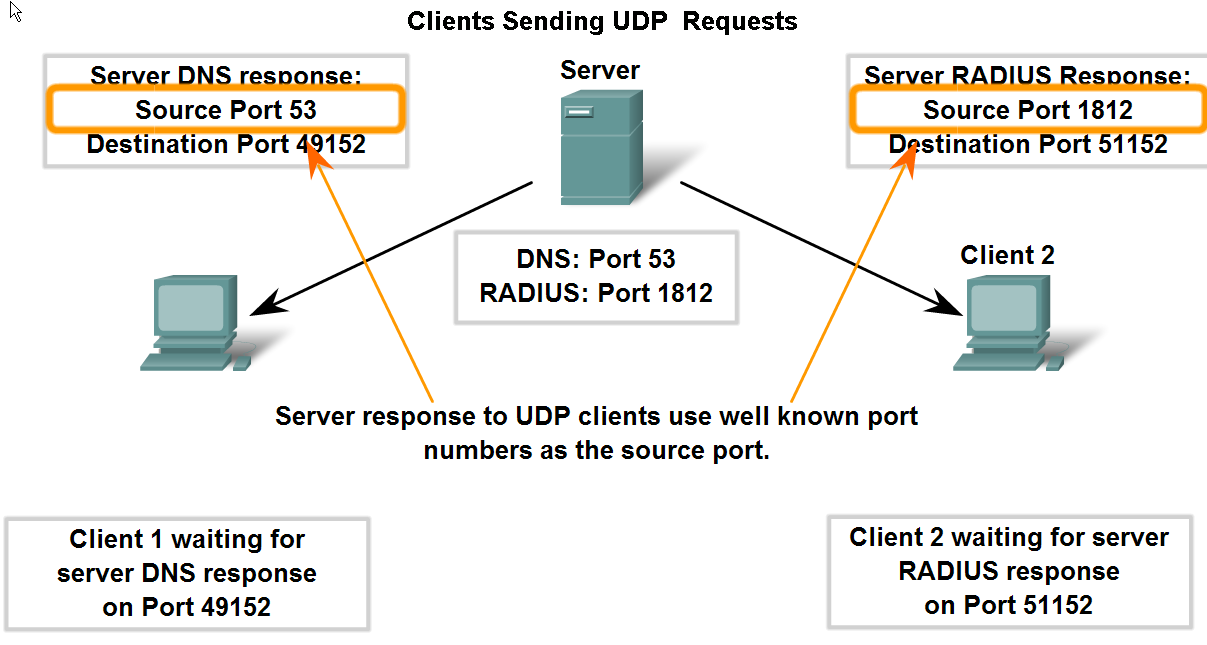
UDP нь дамжуулалтын найдваржилт чухал биш Domain Name System (DNS), Voice over IP (VoIP)- дуу хоолойг интернэтээр дамжуулах протокол, Trivial File Transfer Protocol (TFTP)- файл дамжуулах протокол, online games- интернэт тоглоом зэрэг real time буюу хугацаанаас хамааралтай хэрэглээний программд хэрэглэгддэг.

UDP нь холболт хандалтат бус протокол юм. Холболт хандалтат бус гэдэг нь өгөгдөл дамжуулагдахын өмнө холболт тогтдоггүй бөгөөд өгөгдлийг ямар нэгэн баталгаагүйгээр шууд хүлээн авагч уруу дамжуулдаг. Тиймээс мэдээлэл алдагдах, дахин давтагдах, захиалгын дагуу дамжигдахгүй байж болно. UDP нь мэдээллийг шууд дамжуулдаг учраас TCP-ээс харьцангуй хурдан байдаг.



Зураг 1.2.3 UDP сервер

Зураг 1.2.3-д UDP протокол хэрхэн сервисийг дамжуулж байгааг харуулсан байна. Жишээ нь: Клиентээс сэрвер үрүү DNS хүсэлт илгээхэд UDP протоколоор серверийн 53 гэсэн хаягтай порт уруу дамждаг. Харин сервер дээр RADIUS хүсэлтийг хүлээн авах хаяг нь порт 1812 байна.



Зураг 1.2.4 UDP хүсэлт

Зураг 1.2.4-д Клиент 1, 2 гэсэн 2 компьютерээс хэрхэн UDP хүсэлт илгээж байгааг харуулсан байна. Зурагт харуулснаар клиент 1 нь DNS хүсэлтийн хариуг порт 49152 дээр , клиент 2 нь RADIUS хүсэлтийн хариуг порт 51152 дээр хүлээж авна.

* 1. **TCP ( дамжуулалтыг хянах протокол )**

Дамжуулалтыг хянах протокол (TCP)нь TCP/IP интернэт сүлжээний дамжуулалтын түвшний холболт хандалтат протокол юм. Холболт хандалтат протокол нь өгөгдөл солилцохоос өмнө холболт (виртуал холбоос) урьдчилан тогтсон байдаг.

Хүлээн авагч өгөгдлийг амжилттай хүлээн авснаа илгээгч компьютер руу мессежээр мэдэгдэнэ. Ингэснээр өгөгдлийг найдвартай хүргэх ба хүлээн авдаг. Баталгааны мессежийг илгээгч компьютер хүлээн аваагүй тохиолдолд өгөгдлөө дахин дамжуулдаг.

Хоёр төгсгөлийн цэг нь өөр хоорондоо TCP холболтыг тогтоон өгөгдөл дамжуулдаг. TCP нь дараах боломжуудаар өгөгдлийн найдвартай байдлыг хангадаг.

* Хэрэглээний түвшний өгөгдөл TCP –ийн аль хэсэгт эвдэрснийг илрүүлж түүнийг засахад хамгийн зохистой дахин дамжууллын хэмжээг тодорхойлно.
* TCP сегментийг дамжуулаад хугацаа тоолж эхлэнэ. Энэ хугацаанд эсрэг талаас зөвшөөрсөн хариу ирэхийг хүлээдэг бөгөөд хариу ирээгүй тохиолдолд сегментийг дахин дамжуулна.
* Өгөгдлийн сегментийг хүлээн авсны дараа эсрэг талын төгсгөлийн цэг рүү зөвшөөрсөнөө мэдэгддэг.
* Checksum нь өгөгдлийн толгойд явах бөгөөд дамжуулалтын явцад өгөгдөлд алдаа гарсан эсвэл өгөгдөл өөрчлөгдсөнийг илрүүлнэ.
* Урсгалыг удирдах чадвартай.

TCP нь найдвартай дамжуулалт шаарддаг file transfer protocol, e-mail, world wide web зэрэг хэрэглээг хангахад голчлон хэрэглэгдэнэ .

Бүх TCP сегмент нь илгээж байгаа болон хүлээн авч байгаа хэрэглээг тодорхойлохын тулд илгээгч ба хүлээн авагчийн портуудын дугаарыг агуулдаг. Энэ 2 утга нь илгээгч ба хүлээн авагчийн IP хаягуудын хамтаар тухайн холболтыг цор ганц байдлаар тодорхойлдог.

IP хаяг ба портуудын комбинацыг заримдаа socket гэж нэрлэдэг.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TCP Header ( Толгой ) | | | | | | | | | | | |
| **Bit offset** | **Bits 0–3** | **4–7** | **8–15** | | | | | | | | **16–31** |
| **0** | Source port | | | | | | | | | | Destination port |
| **32** | Sequence number | | | | | | | | | | |
| **64** | Acknowledgment number | | | | | | | | | | |
| **96** | Data offset | Reserved | CWR | ECE | URG | ACK | PSH | RST | SYN | FIN | Window |
| **128** | Checksum | | | | | | | | | | Urgent pointer |
| **160** | Options (optional) | | | | | | | | | | |
| **160/192+** | Data | | | | | | | | | | |

Зураг 1.3.1 TCP сегмэнтийн формат.

Sequence number- дарааллын дугаар нь өгөгдлийн урсгал дахь байтыг илэрхийлдэг.

Acknowledgment number - Хэрэв ACK flag тавигдсан бол энэ дугаар нь хүлээн авагчийн дараагийн хүлээн авах байтын дугаарыг заана.

Data offset- TCP header \*тайлбарлах*\ -ийн хэмжээ

Reserved- нөөцлөгдсөн битүүд 0 утгатай

CWR (Congestion Window Reduced)- Дамжуулагчаас TCP сегмэнтийг хүлээн авсан

илэрхийлж энэ флагийг “1” утгатай болгоно.

ECE (ECN-Echo) (1 bit) – сегмэнт гээгдээгүй болохыг илэрхийлнэ.

URG – urgent (яаралтай) заагч

ACK- acknowledgment талбарт хэрэглэгдэнэ

PSN- push(түлхэх) функц

RST-холболтыг шинээр эхлүүлэх

SYN- дарааллын дугаарын синхронизац

FIN- дамжигдах өгөгдөл дууссаныг мэдэгдэнэ.

WINDOW- хүлээн авагчийн цонхны хэмжээ. Ө.х acknowledgment талбар дахь дарааллын дугаарын байтын тоо

Checksum- өгөгдлийн толгойд явах бөгөөд дамжуулалтын явцад өгөгдөлд алдаа гарсан эсвэл өгөгдөл өөрчлөгдсөнийг илрүүлнэ.

Urgent pointer- Хэрэв Urg флаг тавигдсан бол дарааллын дугаараас шилжсэн хамгийн сүүлийн байтыг заана.

Options (optional)- дээд түвшинээс тодорхойлогдоно.32 бит мэдээлэл байна.

Maximum segment size, Window scale, Selective Acknowledgement ok, Timestamp зэрэг мэдээлэл багтсан байдаг.

Data- TCP сегмэнтийн өгөгдлийн хэсэг буюу хэрэглээний түвшины протокол HTTP, Telnet, SSH,FTP болон TCPг ашигладаг бусад протоколууд.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bit offset** | **Bits 0–3** | **4–7** | **8–15** | **16–31** |
| **0** | Source address | | | |
| **32** | Destination address | | | |
| **64** | Zeros | | Protocol | TCP length |
| **96** | Source port | | | Destination port |
| **128** | Sequence number | | | |
| **160** | Acknowledgement number | | | |
| **192** | Data offset | Reserved | Flags | Window |
| **224** | Checksum | | | Urgent pointer |
| **256** | Options (optional) | | | |
| **256/288+** | Data | | | |

Зураг 1.3.2. TCP pseudo-header (IPv4)

Source address- Илгээгчийн интернэт хаяг

Destination address- Хүлээн авагчийн интернэт хаяг

TCP length- ТСР сегмэнтийн хэмжээ

**ТСР three-way handshaking** \*тайлбарлах*\**зарчмаар холболтыг тогтоодог.**



Зураг 1.3.3. ТСР протоколын холболт тогтоох ба

өгөгдөл дамжуулах процесс

Шинэ холболт тогтсоны дараа SYN флаг тавигдах ба *sequence number* талбар нь энэ холболтонд зориулагдсан *initial sequence number* буюу эхний дарааллын дугаарыг авна. Үүнээс хойш дамжуулагдсан байт бүр *sequence number* талбарын утга дээр тоологдоно.

Байтууд дугаарлагдан дамжуулагдахад эхлэхэд байтыг амжилттай хүлээн авснаа мэдэгдэж илгээгч тал руу *acknowledgement number* талбарт дараагийн байтын дугаарыг явуулна. ТСР холболтонд хийгдэх процессийг ТСР холболтын төлөвийн диаграмд үзүүлэв.

LISTEN -ТСР сервэр алсын клиентээс холболт тогтоох хүсэлт хүлээх төлөв

SYN-SENT -ТСР клиент сервэрлүү холболт тогтоох хүсэлт хүссэн төлөв

SYN-RECEIVED-ТСР сервэр клиентийн холболт тогтоох хүсэлтийг зөвшөөрсөн төлөв

ESTABLISHED-ТСР сервэр болон ТСР клиент хоёрын хооронд холболт тогтсон ба өгөгдөлийг дамжуулж , хүлээн авахад 2 тал бэлэн болсон төлөв.

FIN-WAIT-1-ТСР клиентээс ТСР сервэрт холболт төгсгөх хүсэлтийг хүссэн төлөв

CLOSING-ТСР сервэрээс холболт төгсгөх хүсэлтийг зөвшөөрсөн АСК –ийг

ТСР клиентрүү илгээнэ

FIN-WAIT-2-ТСР клиентээс ТСР сервэрлүү холболт төгссөнийг АСК хийх

CLOSE-WAIT -ТСР сервэрээс холболтыг дуусгах хүсэлтийг хүлээх төлөв

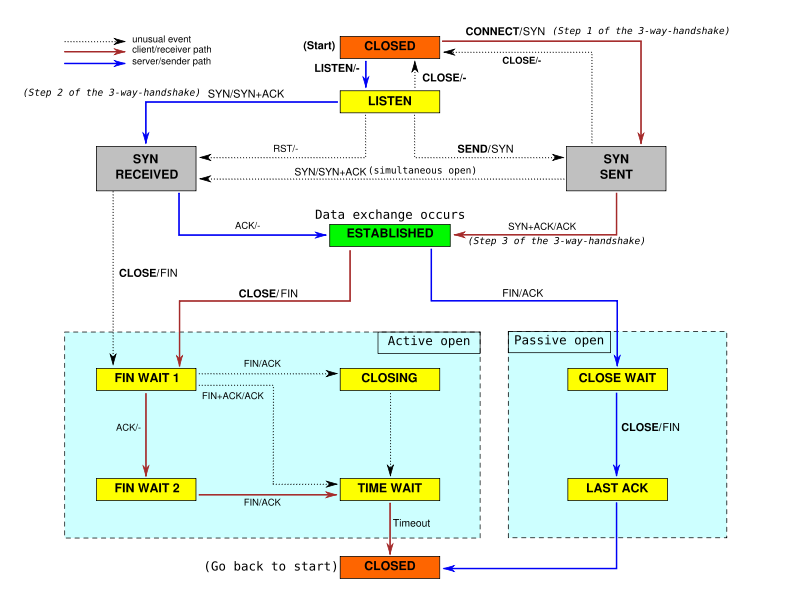
(Идэвхгүй нээлттэй төлөв)

LAST-ACK -ТСР сервэрийн холболт төгсөх АСК –ийг хүлээх төлөв

(Идэвхгүй нээлттэй төлөв)

TIME-WAIT -Холболт төсгөх хүсэлтийг зөвшөөрсөн АСК-ийг ТСР клиент хүлээн авсан эсэхийг хүлээх хугацаах мах 4 мин.

СLOSED-хаалттай төлөв

[](http://upload.wikimedia.org/wikipedia/commons/e/e4/Tcp_state_diagram.svg)

Зураг 1.3.4. ТСР-ын төлөвийн диаграм.

**TCP/UDP портууд**

Бүх TCP сегмент нь илгээж байгаа болон хүлээн авч байгаа хэрэглээг тодорхойлохын тулд *source ба destination* портуудын дугаарыг агуулдаг. Энэ 2 утга нь *source ба destination IP* хаягуудын хамтаар тухайн холболтыг цор ганц байдлаар тодорхойлдог.

IP хаяг ба портуудын комбинацыг заримдаа socket гэж нэрлэдэг. Эдгээр портуудын дугаар нь well-known ( танигдсан ), registered( бүртгэгдсэн ), private/dynamic( хувийн ) гэсэн 3н категорд хуваагддаг.

Well-known (0....1023) порт нь серверийн хэрэглээний программыг ашиглахад зориулагдсан ба сервэр listen буюу сонсох горимд клиентеес холболт тогтоох хүсэлт тавихыг хүлээж байдаг. Жишээ нь FTP(21), ssh(22), TELNET( 23), SMTP(25), HTTP(80) гэх мэт.

Registered порт ( 1024...49151) нь программ хангамжийн компаниудаас гаргасан портуудыг бүртгэхэд зориулагдсан байдаг. Жишээ нь Microsoft SQL(1433), Kaspersky AV Control Center TCP Port (8086). Private/dynamic( 49152.....65535 ) порт нь клиентээс сервэрлүү холбогдоход зориулагдсан temporary( түр зуурын ) порт юм.

**1.4 Мессэж урсгалын дамжуулалтыг хянах протокол**

**SCTP (Stream Control Transmission Protocol)**

SCTP –г анх мессеж хандалтат хэрэглээний дамжуулалтын протоколын зориулалтаар Internet Engineering Task Force (IETF)-ын SIGTRAN группээс эрхлэн гаргасан байна. 2000 оны 10 –р сард SCTP –ын стандарт баримт бичиг болох RFC2960 гаргажээ. SCTP –ын загвар нь *congestion болон flooding, masquerade* дайралтуудаас эсрэг хийгдсэн байна. Түүний TCP –ээс ялгагдах гол ялгаа нь *multihoming ба multistreaming* ойлголт юм. TCP –д урсгал нь байтуудын дараалал хэлбэртэй байдаг бол SCTP –д урсгалыг маш багаас авахуулаад урт хэмжээний мессежүүдийн дараалал хэлбэртэйгээр тусгасан. Checksum болон sequence number (дарааллын дугаар) –ыг ашиглан өгөгдлийн эвдрэлийг илрүүлэх ба өгөгдлийн дахин дамжуулалтын механизм нь зөвхөн эвдэрсэн болон алдагдсан өгөгдлийн хувьд хийгдэнэ. SCTP –ийн холболт нь ерөнхийдөө дараах хэлбэртэй байна. SCTP үйлчилгээ нь TCP болон UDP –ийн нэгэн адил түвшинд ажиллана.



Зураг 1.4.1 SCTP –ийн холболт

SCTP сегмэнт нь common header (толгойн хэсэг) ба chunk (хэлтэрхий) –уудаас тогтоно. Олон chunk –ууд нэг пакет дотор Maximum Transmit Unit (MTU) хүртэл мултифлексорлогдох боломжтой. Chunk нь удирдлагын мэдээлэл ба хэрэглэгчийн өгөгдлийн аль нэгийг агуулна.

**Common header (Толгойн хэсэг)**

Толгойн хэсэг нь 12 байтаас тогтох бөгөөд холболтыг илэрхийлэхийн тулд SCTP нь TCP ба UDP –тэй ижил портыг хэрэглэдэг. SCTP сегмэнт нь Adler-32 алгоритмаар хийгдсэн 32 битийн checksum –аар хамгаалагдана. Түүний тусламжтай дамжуулалтын алдааг илрүүлдэг. Энэ нь TCP ба UDP –ын 16 битийн checksum –аас илүү өргөн юм.

Хэрэв SCTP сегмэнт нь буруу checksum –тай байвал тухайн пакетыг шууд хаядаг. Мөн толгойн хэсэг нь verification tag гэж нэрлэгдэх 32 битийн утгыг агуулна. Verification tag нь тусгайлан холболтонд зориулагдсан бөгөөд түүнийг холболт эхлэхэд төгсгөлийн цэгүүдийн хооронд солилцдог. Иймээс нэг холболтын хувьд 2 өөр verification tag –ын утга хэрэглэгддэг.



Зураг 1.4.2 SCTP пакетын формат

**Chunk**

Chunk гэдэг нь сегмэнт дотор агуулагдах өгөгдлийн хэсгүүдийг агуулсан өгөгдлийн жижиг хэсэг юм. Бүх chunk нь chunk -ын төрөл талбараар эхлэх бөгөөд талбарын утга нь өгөгдлийн chunk болон удирдлагын chunk -ыг ялгахад хэрэглэгдэнэ. Chunk –ууд нь хувьсах урттай учир түүний араас chunk -ын флаг ба chunk –ын урт талбарууд орно. Хүснэгт 1.4.1-д стандарт хэрэглээнд тодорхойлогдсон chunk –уудыг үзүүлэв.

Хүснэгт 1.4.1 Chunk –ын төрлүүд

|  |  |
| --- | --- |
| ID Утга | Chunk -ын төрөл |
| 0 | Payload Data (DATA) |
| 1 | Initiation (INIT) |
| 2 | Initiation Acknowledgement (INIT ACK) |
| 3 | Selective Acknowledgement (SACK) |
| 4 | Heartbeat Request (HEARTBEAT) |
| 5 | Heartbeat Acknowledgement (HEARTBEAT ACK) |
| 6 | Abort (ABORT) |
| 7 | Shutdown (SHUTDOWN) |
| 8 | Shutdown Acknowledgement (SHUTDOWN ACK) |
| 9 | Operation Error (ERROR) |
| 10 | State Cookie (COOKIE ECHO) |
| 11 | Cookie Acknowledgement (COOKIE ACK) |
| 12 | Reserved for Explicit Congestion Notification Echo (ECNE) |
| 13 | Reserved for Congestion Window Reduced (CWR) |
| 14 | Shutdown Complete (SHUTDOWN COMPLETE) |
| 15 to 62 | reserved by IETF |
| 63 | IETF-defined Chunk Extensions |
| 64 to 126 | reserved by IETF |
| 127 | IETF-defined Chunk Extensions |
| 128 to 190 | reserved by IETF |
| 191 | IETF-defined Chunk Extensions |
| 192 to 254 | reserved by IETF |
| 255 | IETF-defined Chunk Extensions |

SCTP нь холболт яаж тогтоодгийг судалж үзье. SCTP холболтын эхэнд хоёр тал 4 мессеж солиллцсоноор дуусгавар болдог. Идэвхигүй буюу холболт тогтоолгож буй талыг сервер, холболт тогтоох хүсэлт тавьж байгаа талыг логикоор клиент гэж нэрлэе. Сервер талд 3 дахь мессеж очиж баталгаажих хүртэл ямар ч нөөц хуваарилагдахгүй. Эндээс холболт тогтоох үйл явцын хүсэлт нь эсрэг талын төгсгөлийн цэгээс бүрэн хамаарах нь харагдаж байна. Холболт тогтох зөв процесс нь сервер ба клиент талууд дээр яаж явагдаж буйг тус бүрд нь тайлбарлая.

**Сервер тал**

Сервер нь ихэнхдээ ХААЛТТАЙ төлвөөс холболт тогтоох хүсэлт INIT chunk –ыг хүлээн авч түүн дотор агуулагдаж буй өгөгдөлд анализ хийнэ. Эндээс холболт тогтооход хэрэгтэй утгуудыг үүсгэн эдгээр утгуудын secure hash ба MD5 эсвэл SHA-1 алгоритмуудаар secret key буюу түлхүүрийг үүсгэнэ.

Дараа нь утгуудыг COOKIE дотор хийж Message Authentication Code (MAC) –ыг гаргана. Энэ COOKIE нь INIT ACK chunk дотор INIT chunk –ыг илгээгч рүү дамжуулагдана. Сервер ХААЛТТАЙ төлөвтөө үлдэж хүлээн авсан бүх INIT chunk –ынхаа тухай мартана.

Сервер нь COOKIE ECHO chunk –ыг хүлээн авна. COOKIE ECHO нь COOKIE –тэй ижил өгөгдлийн бүтэцтэй тул COOKIE –г задалж түүн доторх MAC –ыг шалгана. Хэрэв MAC зөв бол урд нь серверийн үүсгэсэн зөв COOKIE байна гэж ойлгоод түүн доторх өгөгдлийн утгууд нь SCTP instance –г эхлүүлэхэд хэрэглэгдэнэ. Үүний дараа COOKIE ACK chunk –ыг клиент рүү илгээснээр сервер ХОЛБОЛТ ТОГТСОН төлөвт орох бөгөөд өгөгдөл хүлээн авах ба дамжуулахад бэлэн болно.

**Клиент тал**

Дээд түвшнээс холболтыг эхлүүлэхийг хүссэн үед тэрээр API функцийг тодруулбал ASSOCIATE функцийг дуудна. Энэ функц хэрэгтэй өгөгдлүүдийг цуглуулан INIT chunk –ийг байгуулах бөгөөд энэ INIT chunk нь серверийн дамжуулалтын хаяг буюу IP хаяг болон порт руу дамжуулагдана.

Клиент эхний INIT chunk –ыг явуулсны дараа init timer –ыг эхлүүлж COOKIE ХҮЛЭЭХ төлөвт орно. Init timer нь INIT chunk –ын дахин дамжуулалтанд хэрэглэгдэнэ. Тодруулбал init timer нь серверээс INIT ACK chunk ирэхээс өмнө дуусвал дахин дамжуулалт хийгдэнэ.

Хэрэв тодорхой тооны удаа дамжуулалт хийсний дараа ямар ч INIT ACK chunk ирэхгүй бол дээд түвшний протоколд эсрэг талын төгсгөлийн цэг олдсонгүй гэсэн алдааны мэдээллийг буцаана.

COOKIE WAIT төлөвт байгаа клиент нь серверээс INIT ACK chunk –ыг хүлээн авсны дараа init timer –ыг зогсооно. Серверээс хүлээн авсан INIT ACK chunk доторх COOKIE –г авч COOKIE ECHO chunk дотор хийгээд сервер рүү буцаан илгээгээд cookie timer –ыг эхлүүлнэ.

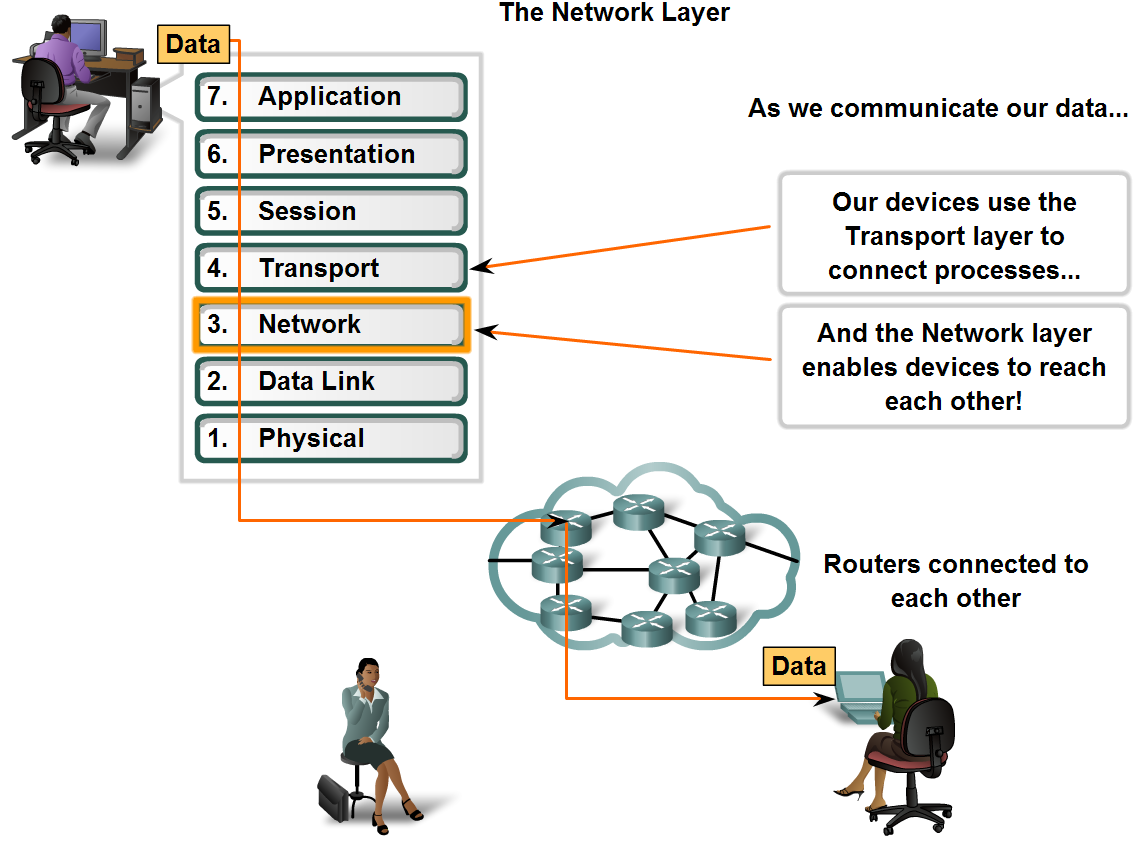
Cookie timer нь COOKIE ACK ирэх хугацааг тоолох бөгөөд COOKIE ECHO –ын дахин дамжуулалтан ашиглагдана. Эхний COOKIE ECHO –г илгээсний дараа COOKIE ECHO –г дамжуулсан төлөвт орно. Хэрэв тодорхой тооны удаа дахин дамжуулалт хийсний дараа COOKIE ACK ирэхгүй бол төгсгөлийн цэг олдоогүйг мэдээлнэ. COOKIE ACK –ыг хүлээн авсны дараа cookie timer –ыг зогсоож ХОЛБОЛТ ТОГТСОН төлөвт шилжинэ.



Зураг1.4.3 SCTP –ын төлвийн диаграм

**2. Сүлжээний түвшин**

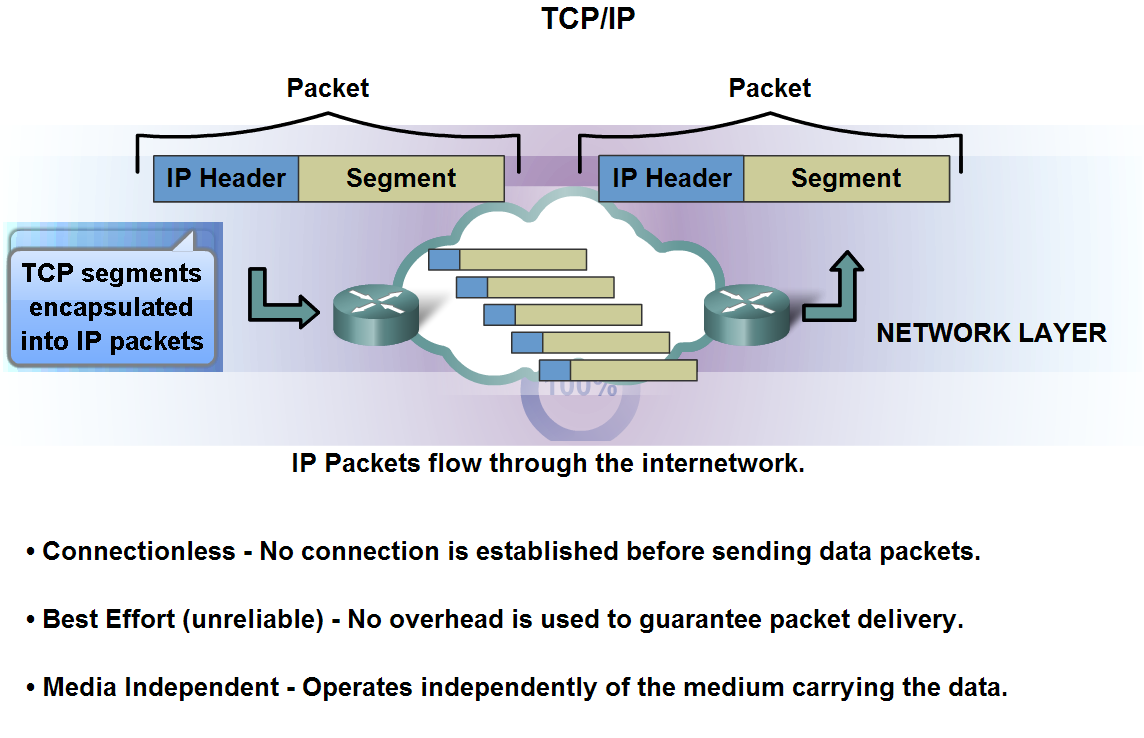
**2.1 Сүлжээний түвшний протокол, түүний үүрэг**



Зураг 2.1.1 Сүлжээний түвшин

Энэ түвшинд сүлжээний төхөөрөмжүүдийн хооронд мэдээлэл хэрхэн дамжуулагддаг, логик хаягаар төхөөрөмж үрүү пакет очих чиглэлийг тодорхойлох арга замыг торхойлдог. Өөрөөр хэлбэл сүлжээний түвшэнд төхөөрөмжүүд логик хаяг буюу IP хаягт тулгуурлан пакетын чиглүүлэлтийг шийддэг. IP version 4 нь 32 битийн урттай аравтын тооллын системд илэрхийлэгдэх 4 тооноос бүрддэг.

Рүүтер нь энэ түвшинд хамаарагдах төхөөрөмж юм. Энэ түвшинд ажилладаг протоколуудад пакетын чиглүүлэлтийг хийдэг, шалгадаг протоколууд орно.



Зураг 2.1.2 сүлжээн дэх IP пакетийн урсгал

**Интернэт протокол**

Холболт хандалтат бус сүлжээний түвшиний протокол. IP нь сүлжээний төхөөрөмжүүдийн хооронд өгөгдөл хэрхэн дамжуулагдах, цор ганц хаягтай төхөөрөмж рүү пакетууд хэрхэн очих маршрут зэрэг тодорхойлдог.

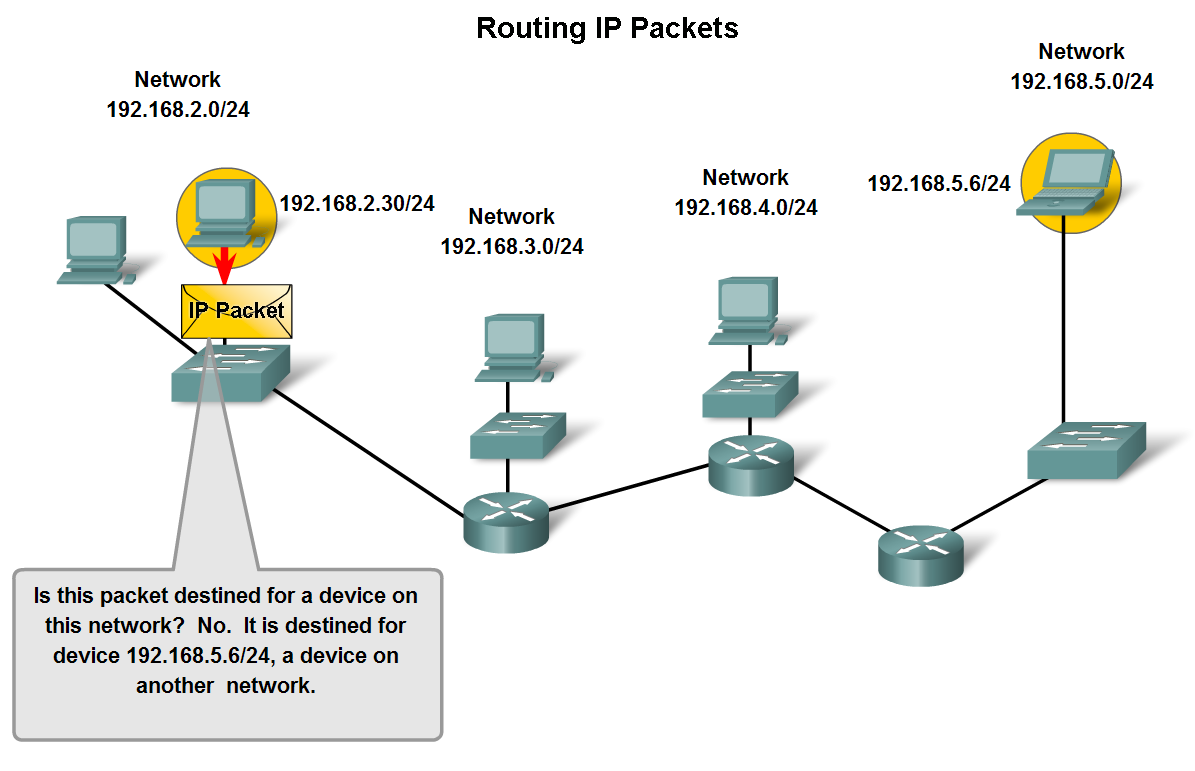
Сүлжээний түвшний төхөөрөмжүүд нь логик хаяг буюу IP хаягт тулгуурлан пакетын чиглүүлэлтийг шийддэг.

Дамжуулалтын түвшний TCP сегмент өгөгдөл дээр дээр IP толгой нэмэх энкапсулэшн үйлдлийг хийснээр сүлжээний түвшний IP пакет үүсдэг. Сүлжээний түвшний протоколууд нь дараах шинж чарантай байна.

Үүнд:

* Холболт хандалтат бус- пакетийг илгээхийн өмнө урьдчилсан холболт тогтдоггүй
* Best effort буюу найдваргүй- пакетийг дамжуулахад нэмэлт толгой шаардагддаггүй
* Сүлжээний орчиноос хамаардаггүй

**2.2 ROUTING ( Чиглүүлэлт)**



Зураг 2.2.1 Чиглүүлэлт хийх

Сүлжээгээр өгөгдөл дамжигдах маршрут (зам) сонгох процесс юм. Чиглүүлэлт нь телефоны сүлжээ, дамжуулалтын сүлжээ, интернэт зэрэг олон төрлийн сүлжээнд хэрэглэгддэг. Чиглүүлэлт хийхэд router, bridge, gateways, firewalls, switches зэрэг төхөөрөмж ашиглан логик хаягтай пакетуудыг илгээгчээс хүлээн авагчруу дамжуулдаг.

Чиглүүлэлтийн 4н төрлийн янзын схем байдаг.

Үүнд:

* Unicast- нэг тусгай зангилааруу мессеж дамжуулна
* Broadcast- сүлжээн дэх бүх зангилаанд мессежийг дамжуулна
* Multicast- нэг групп зангилааруу мессежийг дамжуулна
* Anycast- нэг групп зангилаанаас бусад аль нэгэн зангилааруу дамжуулна

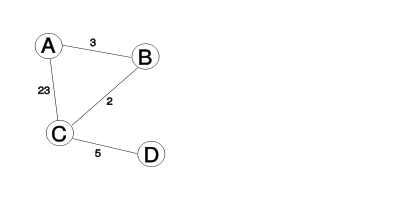
Интернэтийн сүлжээнд unicast routing голчлон ашиглагддаг.

Чиглүүлэх процесс нь routert байрлах Routing Information base ( Чиглэлийн мэдээллийн бааз) дээр үндэслэгдэн хийгдэнэ.

RIB буюу routing table-д сүлжээний чиглэлүүдийн талаархи мэдээллийн жагсаалт байдаг. Чиглүүлэлтийн протокол нь сүлжээн дэх 2 зангилааны хооронд мэдээлэл солилцох хамгийн ойр чиглэлийг сонгох үйлдлийг гүйцэтгэнэ. link-state routing protocols, path vector protocols, distance vector routing protocols гэсэн чиглүүлэлтийн протоколууд байдаг.

Чиглүүлэх протоколын хийх үйлдлийг distance vector routing протоколоор тайлбарлья. Энэ протокол нь Bellman-Ford algorithm-аар хамгийн ойр замыг тооцож гаргадаг.

Жишээ нь: A, B, C, D гэсэн дөрвөн чиглүүлэгчтэй (router) сүлжээг авч үзье

[](http://en.wikipedia.org/wiki/Image:Networkabcd.svg)

Зураг 2.2.2 4н чиглүүлэгчтэй сүлжээ

Хугацааны Т=0 агшинд routing table-ийг дараахи хүснэгтэнд байгуулж харуулав. Энд хамгийн ойр замыг шар өнгөөр дүрслэв.

Хүснэгт 2.2.1 Чиглүүлэлтийн хүснэгт ( Routing table1)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T=0 | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from A** | **via A** | **via B** | **via C** | **via D** | | **to A** |  |  |  |  | | **to B** |  | 3 |  |  | | **to C** |  |  | 23 |  | | **to D** |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from B** | **via A** | **via B** | **via C** | **via D** | | **to A** | 3 |  |  |  | | **to B** |  |  |  |  | | **to C** |  |  | 2 |  | | **to D** |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from C** | **via A** | **via B** | **via C** | **via D** | | **to A** | 23 |  |  |  | | **to B** |  | 2 |  |  | | **to C** |  |  |  |  | | **to D** |  |  |  | 5 | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from D** | **via A** | **via B** | **via C** | **via D** | | **to A** |  |  |  |  | | **to B** |  |  |  |  | | **to C** |  |  | 5 |  | | **to D** |  |  |  |  | |

Сүлжээний бүх зангилаанууд бусад хөрш зангилаануудруу broadcast мессеж буюу өөрийн routing table-ийн мэдээг илгээнэ. Ө.х A зангилаа В,С рүү, В зангилаа А,С рүү, С зангилаа А,В,D рүү , D зангилаа С рүү broadcast мессэжийг явуулна. Энэ broadcast дээр үндэслэн зангилаа бүр шинэ routing table-ийг байгуулдаг.

Эндээс А зангилаанаас Dрүү хүрэх ганц зам л мэдэгдэж байгаа болохоор хүрэх хамгийн ойр замыг А-аас С хүрэх DV=23, С-ээс Dрүү хүрэх DV=5 нийт 28 гэж тооцож гаргана. Энэ мэтчилэн бусад зангилааны хувьд мөн адил тооцож routing table-ийг байгуулана дараахи хүснэгээр харуулав.

Хүснэгт 2.2.2 Routing table2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T=1 | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from A** | **via A** | **via B** | **via C** | **via D** | | **to A** |  |  |  |  | | **to B** |  | 3 | 25 |  | | **to C** |  | 5 | 23 |  | | **to D** |  |  | 28 |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from B** | **via A** | **via B** | **via C** | **via D** | | **to A** | 3 |  | 25 |  | | **to B** |  |  |  |  | | **to C** | 26 |  | 2 |  | | **to D** |  |  | 7 |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from C** | **via A** | **via B** | **via C** | **via D** | | **to A** | 23 | 5 |  |  | | **to B** | 26 | 2 |  |  | | **to C** |  |  |  |  | | **to D** |  |  |  | 5 | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from D** | **via A** | **via B** | **via C** | **via D** | | **to A** |  |  | 28 |  | | **to B** |  |  | 7 |  | | **to C** |  |  | 5 |  | | **to D** |  |  |  |  | |

Мөн түрүүний адилаар шинэчлэгдсэн routing table-ийг хугацааны Т=1 агшинд хөрш зангилаануудруу явуулна. Эндээс А зангилаанаас Dрүү хүрэх ACD, ABCD гэсэн 2 замтай болох ба А-аас В хүрэх DV=3, В-ээс D хүрэх DV=7 нийт DV=10 гэсэн хамгийн богино замыг тооцож гаргана.

Энэ мэт бусад зангилаан дээр бодолд хийгдэн зангилаа бүр дээр хүрэх хамгийн богино замыг харуулсан routing table-ийг шинээр байгуулдаг.

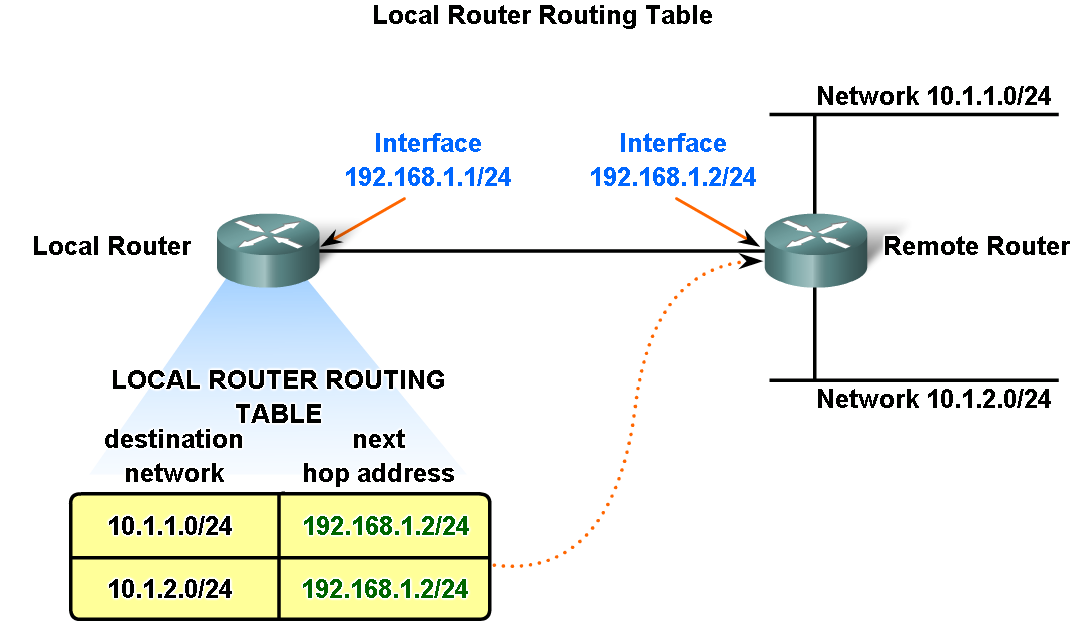
Доорхи хүснэгтэнд үзүүлэв.

үснэгт 2.2.3. Routing table3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T=2 | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from A** | **via A** | **via B** | **via C** | **via D** | | **to A** |  |  |  |  | | **to B** |  | 3 | 25 |  | | **to C** |  | 5 | 23 |  | | **to D** |  | 10 | 28 |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from B** | **via A** | **via B** | **via C** | **via D** | | **to A** | 3 |  | 7 |  | | **to B** |  |  |  |  | | **to C** | 8 |  | 2 |  | | **to D** | 31 |  | 7 |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from C** | **via A** | **via B** | **via C** | **via D** | | **to A** | 23 | 5 |  | 33 | | **to B** | 26 | 2 |  | 12 | | **to C** |  |  |  |  | | **to D** | 51 | 9 |  | 5 | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **from D** | **via A** | **via B** | **via C** | **via D** | | **to A** |  |  | 10 |  | | **to B** |  |  | 7 |  | | **to C** |  |  | 5 |  | | **to D** |  |  |  |  | |

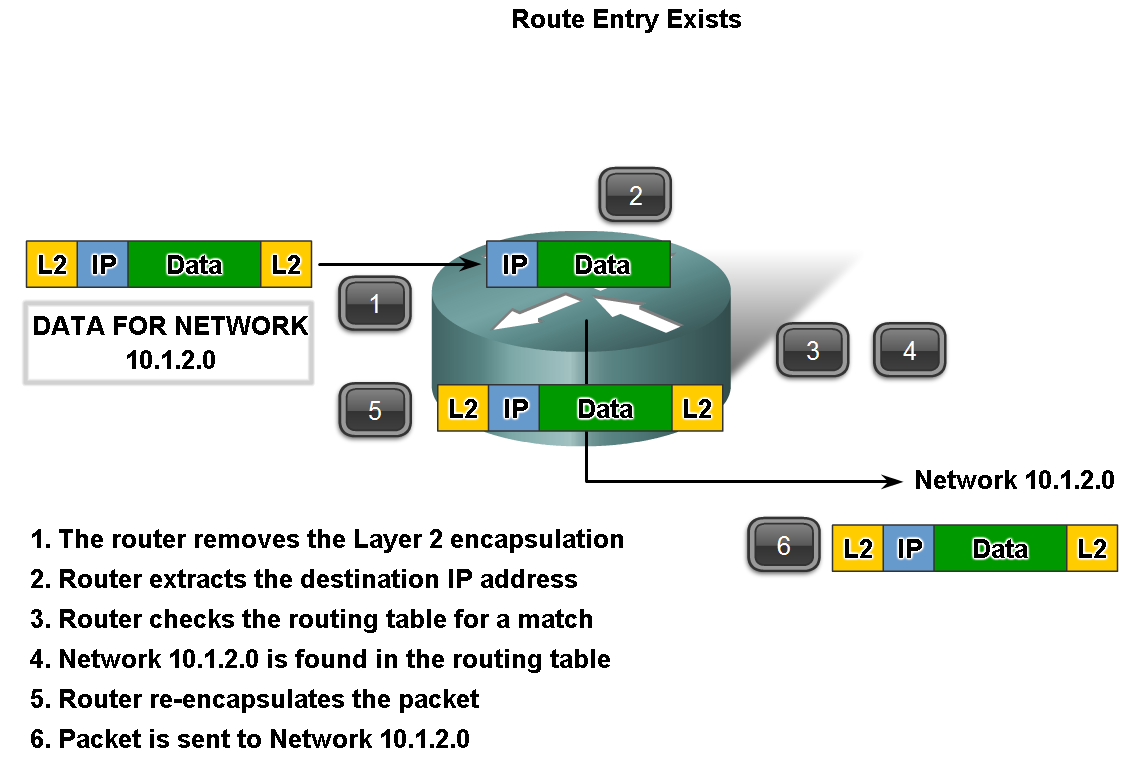
Мөн түрүүний адилаар шинэчлэгдсэн routing table-ийг хугацааны Т=2 агшинд хөрш зангилаануудруу явуулна.

Хамгийн ойр замыг тодорхойлох бодолт хийн шинэ routing table-ийг явуулах боловч энд routing table шинэчлэгдэхгүй ба үүнээс өөр хамгийн ойр зам байхгүй тул алгоритм зогсож хамгийн оновчтой routing table-ийг хугацааны Т=3 агшинд дээрхийн адил байгуулж зангилаа хооронд энэ замаар мэдээлэл дамжина.



Зураг 2.2.3 Рүүтерийн чиглүүлэлтийн хүснэгт

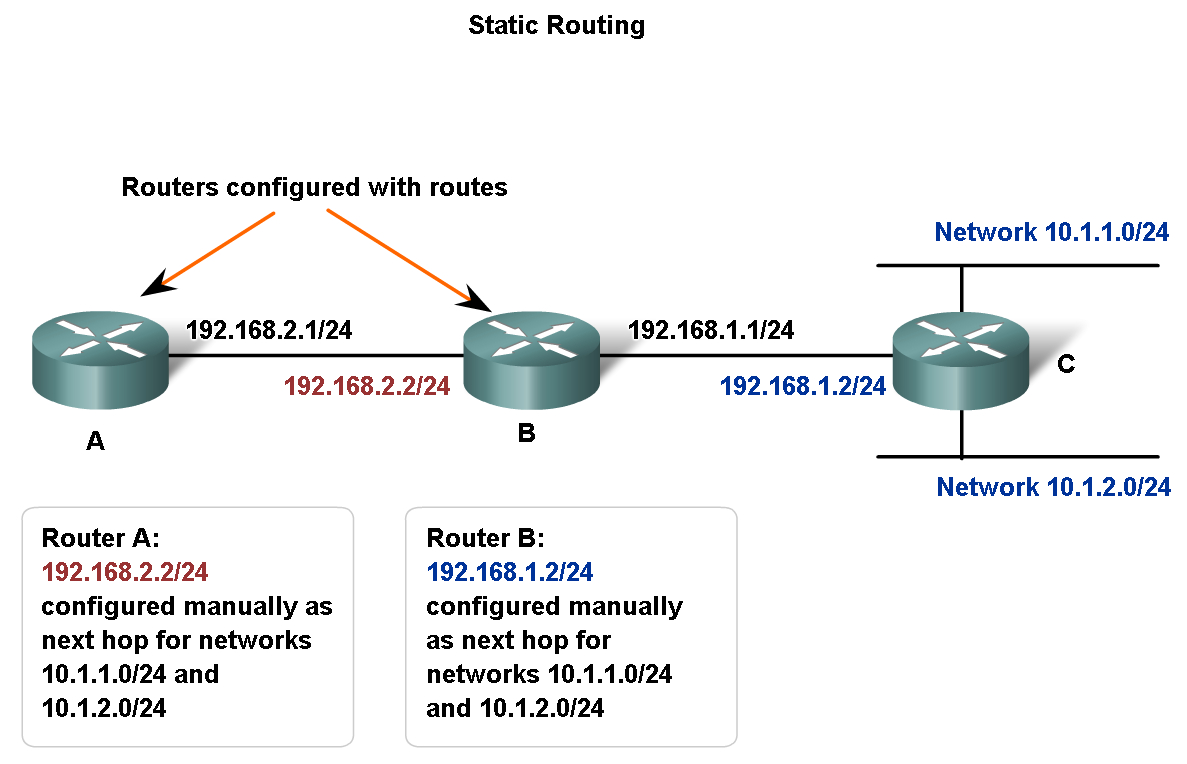
Тухайн рүүтер дээр илгээгчийн хаяг болон дараагийн үсрэх рүүтерийн интерфейсийн хаяг байдаг. Өөрөөр хэлбэл локал рүүтерээс 10.1.1.0/24 болон 10.1.2.0/24 гэсэн сүлжээ үрүү пакетийг чиглүүлэхийн тулд Remote рүүтерээр дамжина гэсэн үг.



Зураг 2.2.4 Рүүтерт чиглүүлэлтийг хийх

1. Рүүтер сувгийн түвшний фреймийг задалж пакет болгоно
2. Рүүтер хүлээн авагчийн IP хаягийг тайлна.
3. Рүүтер чиглүүлэлтийн хүснэгтээс тохирох хүлээн авагчийн IP хаяг байгаа эсэхийг шалгана.
4. 10.1.2.0 сүлжээг чиглүүлэлтийн хүснэгтээс олно
5. Рүүтер пакетийг дахин фрейм болгоно
6. Пакетийг 10.1.2.0 сүлжээ үрүү илгээнэ.

**2.3 Статик ба динамик IP хаяг.**



Зураг 2.2.5 Статик чиглүүлэлт хийх

Тухайн нэг компьютер нь интернэтийн сүлжээнд холбогдох тогтмол нэг IP хаягийг хэрэглэж байвал энэ нь статик IP хаяг юм. Харин dialup холболт болон нэг кабелийг хуваан эзэмшиж байвал IP хаяг нь байнга өөрчлөгдөж байдаг ба энэ нь динамик хаяг юм.

Статик хаяг нь сүлжээний администратор тавьж өгдөг бол динамик хаягийг сервэрээс Dynamic Host Configuration Protocol (DHCP) протокол ашиглан тавьж өгдөг . Динамик хаяглалт нь дотоод сүлжээ болон broadband сүлжээнд хэрэглэгдэнэ.

Динамик хаяг ашигласнаар нэг интернэт хаягийг олон компьютер хуваан эзэмших боломжтой болдог.

Статик хаягийг инфра бүтэцтэй үйлчилгээнд ашиглах ба үүний нэг жишээ нь Domain name service систем юм.

Domain Name System (DNS)нь интернэтийн сүлжээн дэх hostname (domain name) буюу компьютерүүдийн нэрийн жагсаалт ба тэдгээрийг интернэтийн IP хаягруу хөрвүүлэх үйлчилгээ үзүүлж байдаг систем юм.

Мөн mail exchange server-ийн мэдээлэл email (электрон шуудан) очих domain name-үүдийн жагсаалтыг хадгалж байдаг. Internet domain name-үүдийг Internet Corporation for Assigned Names and Numbers (ICANN) байгууллагаас бүртгэдэг. Мөн түүнчлэн Domain name-ийг Web site-ийн Uniform Resource Locator (URL) заагч хаяг гэж бас нэрлэдэг.

Сүлжээний түвшинд компьютерийн hardware( техник хангамж) хаягийг олох Adress Resolution Protocol (ARP) ажилладаг. Энэ протоколын гол үүрэг нь сүлжээний IP хаягийн тусламжтай сувгийн түвшины MAC хаягийг олдог.

Меdia Access Control (MAC) хаяг буюу физик хаяг нь тухайн төхөөрөмжийг илэрхийлэх үл давтагдах 6 байтын урттай тоо байна. Физик хаягийг үйлдвэрлэгчээс тухайн төхөөрөмжин дээр өөрчлөх боломжгүйгээр шарсан байдаг.

2 host ( компьютерийн ) хооронд мэдээлэл солилцох дөрвөн тохиолдолд ARP хэрэлэгддэг.

1. Хоёр компьютер нь нэг сүлжээнд холбогдсон ба өөр хоорондоо мэдээлэл дамжуулах.

2. Хоёр компьютер нь хоёр өөр төрлийн сүлжээнд холбогдсон байх ба gateway/router ( чиглүүлэгч ) ашиглан хоорондоо мэдээлэл дамжуулах

3. Чиглүүлэгч алсын компьютерлүү мэдээллийг(packet) дамжуулахад өөр чиглүүлэгч ашиглахад

4. Нэгэн төрлийн сүлжээнд холбогдсон нэг компьютерээс алсын компьютерт чиглүүлэгч ашиглан мэдээлэл дамжуулах

Нэг компьютерээс нөгөө компьютерлүү мэдээлэл дамжуулахын тулд MAC хаягийг мэдэх хэрэгтэй ба ARP request пакетийг илгээдэг хариуд нь нөгөө компьютерээс өөрийн MAC хаягаа ARP reply пакетаар явуулна.

|  |  |  |  |
| --- | --- | --- | --- |
| **+** | **Bits 0 - 7** | **8 - 15** | **16 – 31** |
| **0** | Hardware type (HTYPE) | | Protocol type (PTYPE) |
| **32** | Hardware length  (HLEN) | Protocol length  (PLEN) | Operation (OPER) |
| **64** | Sender hardware address (SHA) | | |
| **?** | Sender protocol address (SPA) | | |
| **?** | Target hardware address (THA) | | |
| **?** | Target protocol address (TPA) | | |

Зураг 2.1.4 ARP пакетийн бүтэц

Hardware type (HTYPE)-Сувгийн түвшины протоколын (техник хангамжийн) төрөл ,

Жишээ нь Ethernet сүлжээ бол 1.

Protocol type (PTYPE)-Сүлжээний түвшины протоколын (логик хаягийн)төрөл ,

IPv4 бол 0x0800.

Hardware length (HLEN)-Техник хангамжийн хаягийн хэмжээ .

Ethernet сүлжээний хаяг 6 байт урттай.

Protocol length (PLEN)-Логик хаягийн хэмжээ. IPv4 хаяг 4 байт урттай.

Operation-Үйлдлийн төрөл 1 бол request, 2 бол reply.

Sender hardware address (SHA)-Илгээгчийн техник хангамжийн хаяг

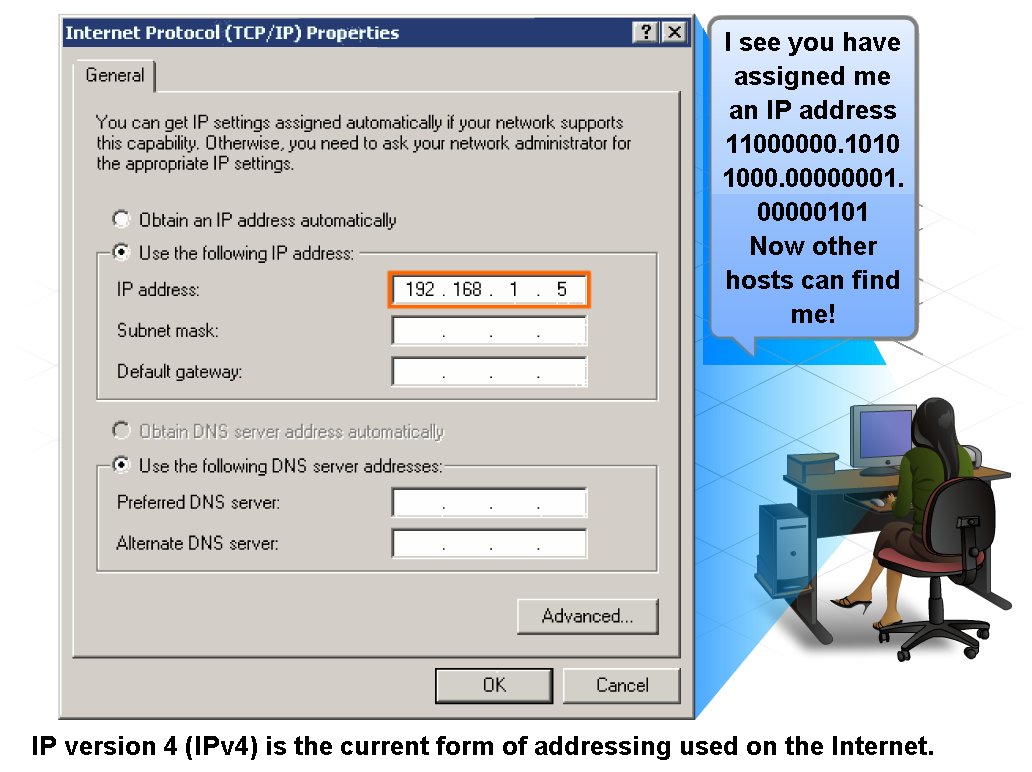
Sender protocol address (SPA)-Илгээгчийн логик хаяг.

Target hardware address (THA)-Хүлээн авагчийн техник хангамжийн хаяг

Target protocol address (TPA)-Хүлээн авагчийн логик хаяг.

1. **IP хаягын төлөвлөлт**

**3.1 IP хаягийн бүтэц**



Зураг 3.1.1 IPv4 хаяг

Сүлжээний түвшний хаяглалт нь ижил сүлжээнд болон өөр сүлжээнд байгаа

хостуудын хооронд өгөгдөл солилцох боломжийг хангадаг. Бид энэ зорилгоор Интернэт протоколын хувилбар 4 (IPv4)-ийг судална.

Энэ бүлэгт IPv4 хаягийн бүтэц болон эх сүлжээг дэд сүлжээнд хуваах талаарх ойлголтуудыг судлах болно.

Үүнд:

* IP хаягийн бүтэц болон 8 бит 2тын тоог 10т тооллын системд хөрвүүлж сурах
* Өгөгдсөн IPv4 хаягийг ангилах, сүлжээнд хэрхэн ашиглагдахыг тодорхойлох.
* Хаягийг администратор болон ISP-аас хэрхэн тодорхойлдог болох
* Сүлжээний хэсэг болон хостийн хэсэг гэж юу вэ? эх сүлжээг дэд сүлжээнд хуваах сабнет маскийн үүргийг торхойлох
* Өгөгдсөн IPv4 хаягийн мэдээллийг ашиглан хаягийн бүрэлдэхүүн хэсгүүдийг тодорхойлох, тооцоолох.
* Сүлжээний холболтийг тестлэх, шалгах,хост дээрх IP протоколын стекийн үйл ажиллагааг судална.

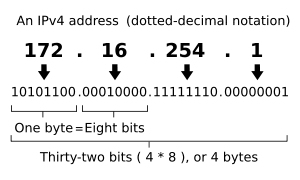
**IP хаяг (интернэт хаяг)**

IP хаяг нь компьютерийн сүлжээнд интернэт протокол ашиглан өөр хоорондоо мэдээлэл солилцох төхөөрөмжүүдийн таних тэмдэг болох цор ганц хаяг ба IP төхөөрөмжүүдийн локатор буюу заагчийн үүрэг гүйцэтгэнэ.

IP хаягийг Internet Assigned Numbers Authority (IANA)-аас олгодог.

IANA нь глобал IP хаяг , DNS( domain name system) root zone management , интернэт протоколын үүрэг зэрэгийг тодорхойлдог. IANA-г ICANN (Internet Corporation for Assigned Names and Numbers)байгууллага хэрэгжүүлдэг.

IP version 4 IP хаяг нь 32 битийн урттай 10 –тын тооллын системд илэрхийлэгдэх 4 тооноос бүрддэг.

[](http://en.wikipedia.org/wiki/Image:Ipv4_address.svg)

Зураг 3.1.2 IPv4 хаягийн формат

IPv4 хаяг нь цэгээр тусгаарлагдсан дөрвөн байт урттай.

IP хаягийн эхний байтаас хамаарч сүлжээг А,В,С ангилалд хуваадаг.

Хүснэгт 3.1.1 IP хаягийн ангилал

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ass | Range of first octet | Network ID | Host ID | Possible number of networks | Possible number of hosts |
| A | 1 – 126 | A | b.c.d | 126 = (27 - 2) | 16,777,214 = (224 - 2) |
| B | 128 – 191 | a.b | c.d | 16,384 = (214) | 65,534 = (216 - 2) |
| C | 192 – 223 | a.b.c | d | 2,097,151 = (221 - 1) | 254 = (28 - 2) |

Хүснэгт 3.1.2 Дотоод сүлжээнд зориулсан IPv4 хаяг

|  |  |  |  |
| --- | --- | --- | --- |
| IANA Reserved Private Network Ranges | Class | Start of range | End of range |
| The 24-bit Block | A | 10.0.0.0 | 10.255.255.255 |
| The 20-bit Block | B | 172.16.0.0 | 172.31.255.255 |
| The 16-bit Block | C | 192.168.0.0 | 192.168.255.255 |

**3.2 Тооллын систем**

Хоёртын тооллын систем (Binary representation )

0, 1 – 2 цифр

Аравтын тооллын систем (Decimal representation)

0,1,2,3,4,5,6,7,8,9 – 10 цифр

Арван зургаатын тооллын систем (Hexadecimal representation)

0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F – 16 цифр тус тус хэрэглэгдэнэ.

Тухайн тооллын системийн хамгийн их цифр дээр нэгийг нэмье:

1 + 1 = 102 = 10b (binary)

9 + 1 = 1010 = 10 (decimal)

F + 1 = 1016 = 10h эсвэл 0x10 (hexadecimal)

Дээрх тооллын системүүдийн цифрүүдийг ашиглан ямар нэг тоо бичие:

1001011b – 2-тын тоо

1211d - 10-тын тоо

01A3E h буюу 0х1A3E - 16-тын тоо

**Нэг тооллын системээс нөгөө тооллын системд хөрвүүлэх**

Тоог янз бүрийн тооллын системд бичих жишээ болгох зорилгоор 0–ээс 16 хүртэлх тоог 10-т, 2-т, 16-тын тооллын системд бичье.Энд дэс дараалсан тоо байгаа учир өмнөх тоон дээр нэгийг нэмэх замаар дараах тоог нь олж бичнэ.

|  |  |  |
| --- | --- | --- |
| 10-т | 2-т | 16-т |
| 0 | 0 | 0 |
| **1** | **1** | 1 |
| **2** | **10** | 2 |
| 3 | 11 | 3 |
| **4** | **100** | 4 |
| 5 | 101 | 5 |
| 6 | 110 | 6 |
| 7 | 111 | 7 |
| **8** | **1000** | 8 |
| 9 | 1001 | 9 |
| 10 | 1010 | A |
| 11 | 1011 | B |
| 12 | 1100 | C |
| 13 | 1101 | D |
| 14 | 1110 | E |
| 15 | 1111 | F |
| **16** | **10000** | 10 |

Хүснэгтээс 10-тын системд хоёрын зэрэгтэй тэнцүү байх тоог 2-тын системд шууд хөрвүүлэн бичиж болж байна.

|  |  |
| --- | --- |
| 10-т | 2-т |
| 1=20 | 1 |
| 2=21 | 10 |
| 4=22 | 100 |
| 8=23 | 1000 |
| 16=24 | 10000 |
| M=2n | 1  n |

Энэхүү шинжийг ашиглан аравтын ямар ч тоог 2-тын систем рүү хялбархан хөрвүүлж болно. Жишээ нь: Аравтын 291 гэсэн тоог хоёрт руу хөрвүүлье.

291 = 256 + 32 + 2 + 1 = 100000000b + 100000b + 10b + 1b= 100100011b буюу

291 = 100100011b болно.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

Дээрх хоёртоор нэмэх үйлдлийг дараах байдлаар хийж болно. Эхлээд 256-д харгалзах 1 –ийг бичээд нийлбэрт 128, 64 байхгүй учир хоёр 0, 32 байгаа тул 1 нэг , 16, 8, 4 байхгүй тул гурван тэг, 2, 1 байгаа тул хоёр нэг бичнэ.

Иймд 291 = 256 + 32 + 2 + 1 = 28 + 25+21+ 1 = 100100011b болно.

Харин тоог 2 –тын системээс 10 –тын систем рүү хөрвүүлэхэд энэ аргыг урвуугаар нь хэрэглэж бас болно.

Жишээлбэл: 10011110110b = *20*+**21**+**22**+*23*+**24**+**25**+**26**+**27**+*28*+*29*+**210** =1270 болно. Энд хоёртын тоог хойноос нь эхлэн харгалзах хоёртын зэрэгтүүдийн нийлбэрт задлах ба тухайн байрлалд 0 байвал 0 –ийг, харин 1 байвал тухайн байрлалд харгалзах хоёртын зэрэгтийг нэмэх замаар харгалзах аравтын тоог гаргана.

Зарим тохиолдолд b = 1 – 1 = 2n – 1 байх шинжийг ашиглавал илүү хялбар байх тохиолдолд байна.

Жишээлбэл: 111111b = **20**+**21**+**22**+**23**+**24**+**25** = 26-1= 63

Хоёрт ба 16-тын системийн сууриуд 16=24 гэсэн холбоотой учир тэдгээрийн хооронд тоог шууд хөрвүүлж болдог. Ингэхдээ хоёртын тоог араас нь дөрөв дөрвөн оронгоор нь бүлэглэн тухайн хоёртын тоонд харгалзах 16 –тын тоог тавина. Жишээлбэл:

010011110110 = ‘0100’1111’0110 = 4’F’6h

0011’1111’0111b = 3’F’7h

Арванзургаатын тооллын системээс хоёрт руу хөрвүүлэхдээ мөн адил хөрвүүлнэ.

1ABCh = 1’A’B’C’h = 0001’1010’1011’1100b

321Fh = 0011’0010’0001’1111b

Аравтын системээс 16-тын систем рүү хөрвүүлэхдээ аравтын тоог 16 - д хуваана. Жишээ нь:

1783 гэсэн аравтын тоог 16-тын тооллын систем рүү хөрвүүлье.

|  |  |  |  |
| --- | --- | --- | --- |
| Тайлбар | Хуваалт | Бүхэл хэсэг | Үлдэгдэл буюу  16 –тын тоо |
|  | 1783/16 | 111 | **7** |
| Бүхэл хэсэг 16-аас их тул дахин хуваана. | 111/16 | 6 | **15 буюу F** |
| Бүхэл хэсэг 16-аас бага тул 6-г үлдэгдэл гэж тооцно | 6/16 | 0 | **6** |

Эндээс 1783 = буюу **6F7h** болно.

16-тын системээс 10 –тын систем рүү хөрвүүлэх.

1A7h = =423

42BCh = = 17084

2-тын тооллын системд арифметик +, - үйлдэл гүйцэтгэх

Тус бүр нэг бит (bi*nary* *digi*t) байх хоёртын хоёр тоон арифметик нэмэх хасах үйлдлийг хийе

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| x | Y | x+y | x | y | x-y |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 10 | 1 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 10 | 1 | 1 | 0 |

Дээрх дүрмийг ашиглан хоёртын тооллын системд хоёр тоог нэмж, хасъя.

+ + + - - -

**Логик үйлдлүүд**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| X | Y | X or Y | X nor Y | X and Y | X nand Y | not X | X xor Y |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |

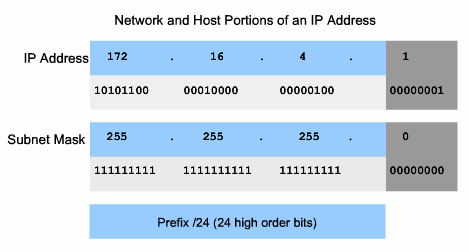
Жишээ болгон дараах хоёртын тоонууд дээр логик үйлдлүүд хийж үзье.

or nor and nand xor

**3.3 Сабнет хаяг**

Сүлжээний администратор блокийг subnetүүд болгон хуваадаг. Жишээ нь : home routers хаягын 192.168.0.0- 192.168.0.255 интервалын хооронд автоматаар default хаягийг авдаг.

Subnet гэдэг нь тухайн дотоод сүлжээн дэх төхөөрөмжүүдийн логик хаяг. Home routers буюу home gateway нь тухайн дотоод сүлжээг интернэттэй холбох төхөөрөмж ба тухайн дотоод сүлжээн дэх компьютерүүд интернэтийн нэг IP хаягийг хуваан эзэмших боломжоор хангана.



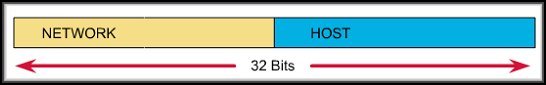
Зураг 3.3.1 IP хаягийн сүлжээний ба хостийн хэсэг

Энэ зурагт үзүүлсэн цэнхэр өнгөөр дүрслэгдсэн IP хаягийн эхний гурван аравтын тоо нь сүлжээний хэсэг гэж нэрлэгдэх буюу сүлжээний хаягийг заана. Хамгийн сүүлийн аравтын орон нь хостийн тоог илэрхийлдэг. Ташуу зураасын ард байрлах тоо нь сүлжээний орны тоо буюу хэдэн ширхэг нэг байгааг заадаг.

IP хаяг, сабнэт маск, сүлжээний хаяг, бродкаст хаяг

IP хаяг = сабнэт маск = 32 бит

IP хаяг дотор сүлжээний, хостын гэсэн хоёр хэсэг багтдаг.

****

Хаагуураа зааглагдаж байгааг сабнэтмаск зааж өгнө.

Сабнэт маск нь мөн 32 бит бөгөөд 1-ийн цуваагаар эхлээд 0-ийн цуваагаар дууссан хэлбэртэй байна. 1-ийн болон 0-ийн цувааны урт хэд ч байж болдог.

172.89.12.1

255.255.255.0 гэж байвал сүлжээний хаяг нь 172.89.12 хостын хэсэг нь .1 болно.

**Дүрэм:**

Тухайн IP хаягийг сабнэт масктай нь AND хийвэл сүлжээний хаяг гарна. Өөрөөр хэлбэл сүлжээний оронг хэвээр үлдээгээд хостын оронг тэг болгохтой ижил үйлдэл юм. Жнь: дээрх хаягны хувьд сүлжээний хаяг нь 172.89.12.0 болно.

Тухайн IP хаягийг сабнэт маскын урвуутай OR хийвэл броад каст хаяг гарч ирнэ. Өөрөөр хэлбэл сүлжээний оронг хэвээр үлдээгээд хостын оронг дан нэгээр дүүргэхтэй ижил үйлдэл юм. Жнь: дээрх хаягны хувьд сүлжээний хаяг нь 172.89.12.255 болно.

Сүлжээний хаяг броадкаст хаяг хоёрыг хостыг хаяглахад ашиглахгүй бөгөөд энэ хоёроос бусад хаягаар хостыг хаяглаж болно. Тэдгээр хаягуудыг ашиглаж болох хостын хаяг гэж ярьдаг. Жишээ: 192.168.2.165

255.255.255.0

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP хаяг | 192 | 168 | 2 | 165 |
| Сабнэт маск | 255 | 255 | 255 | 0 |
|  |  |  |  |  |
| IP хаяг | 11000000 | 10101000 | 00000010 | 10100101 |
| Сабнэт маск | 11111111 | 11111111 | 11111111 | 00000000 |
| Cүлжээний хаяг | 11000000 | 10101000 | 00000010 | 00000000 |
| Бродкаст хаяг | 11000000 | 10101000 | 00000010 | 11111111 |
|  |  |  |  |  |
| Cүлжээний хаяг | 192 | 168 | 2 | 0 |
| Бродкаст хаяг | 192 | 168 | 2 | 255 |
| Хамгийн эхний ашиглаж болох хостын хаяг | 192 | 168 | 2 | 1 |
| Хамгийн сүүлийн ашиглаж болох хостын хаяг | 192 | 168 | 2 | 254 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP хаяг | 10 | 254 | 189 | 65 |
| Сабнэт маск | 255 | 255 | 240 | 0 |
| IP хаяг | 00001010 | 11111110 | 10111101 | 01000001 |
| Сабнэт маск | 11111111 | 11111111 | 11110000 | 00000000 |
| Cүлжээний хаяг | 00001010 | 11111110 | 10110000 | 00000000 |
| Бродкаст хаяг | 00001010 | 11111110 | 10111111 | 11111111 |
| Cүлжээний хаяг | 10 | 254 | 176 | 0 |
| Бродкаст хаяг | 10 | 254 | 191 | 255 |
| Хамгийн эхний ашиглаж болох хостын хаяг | 10 | 254 | 176 | 1 |
| Хамгийн сүүлийн ашиглаж болох хостын хаяг | 10 | 254 | 191 | 154 |

**3.4 IP хаягийг тооцоолох**

IPv4 хаягийн хүрэлцээ бага болсноор нэг том сүлжээнээс дэд сүлжээ үүсгэх аргыг бий болгожээ. Дэд сүлжээнд хувааснаар тухайн сүлжээний ашиглагдахгүй хаягийн тоо багасдаг байна. Жишээ нь:



Зураг 3.3.2 Эх хаягийг дэд сүлжээнд хуваах

Хэлбэртэй сүлжээ өгөгдсөн бол ашиглахгүй хаягийн хэмжээг хамгийн бага байлгахын тулд : A cүлжээнд 32 хосттой

Б cүлжээнд 512 хосттой

В cүлжээнд 16 хосттой

Г cүлжээнд 128 хосттой

Дэд сүлжээ үүсгэж өгөх шаардлагатай болж байна. Гэвч уг байгууллага 172.31.0.0/16 гэсэн нэг л сүлжээний мужийг ашигладаг бол уг сүлжээгээ дээрх 4 тусдаа жижиг сүлжээнд ашиглахын тулд хуваах хэрэгтэй болно.

**Дүрэм:**

Дэд сүлжээний хэрэгцээг хангах сүлжээний хаягийн мужийн уртыг тодорхойлно.

* Уртаар нь эрэмбэлэнэ.
* Эх сүлжээний эхлэлээс сүлжээний хаягийн уртаар тасдана.
* Сабнэт маскуудыг бодож гаргана.

Жишээ: Дээрх өгөгдөл дээр сүлжээг хэрхэн хуваахыг харъя.

A сүлжээ 24 хосттой бол 32 хаягтай сүлжээ хувааж өгнө.

Б сүлжээ 400 хосттой бол 512 хаягтай сүлжээ хувааж өгнө

В сүлжээ 10 хосттой бол 16 хаягтай сүлжээ хувааж өгнө

Г сүлжээ 70 хосттой бол 128 хаягтай сүлжээ хувааж өгнө

Одоо сүлжээнүүдээ хаягийн тоогоор нь эрэмбэлнэ.

Б – 512

Г – 128

А – 32

В – 16

Дараа нь хуваалтаа хийнэ

Б – 512 - 172.31.0.0 – 172.31.1.255 (Энэ хооронд нийт 512 хаяг байгаа)

Г – 128 172.31.2.0 – 172.31.2.127 (Энэ хооронд нийт 128 хаяг байгаа)

А – 32 - 172.31.2.128 – 172.31.2.159 (Энэ хооронд нийт 32 хаяг байгаа)

В – 16 - 172.31.2.160 – 172.31.2.175 (Энэ хооронд нийт 16 хаяг байгаа)

Хамгийн сүүлд сүлжээ тус бүрийн сабнэт маскийг бодож гаргана. Сабнэт маскын тоо нь сүлжээний оронгийн тоогоор шууд илэрхийлэгддэг.

IP хаяг 32 бит = Сүлжээний орон + Хостын орон

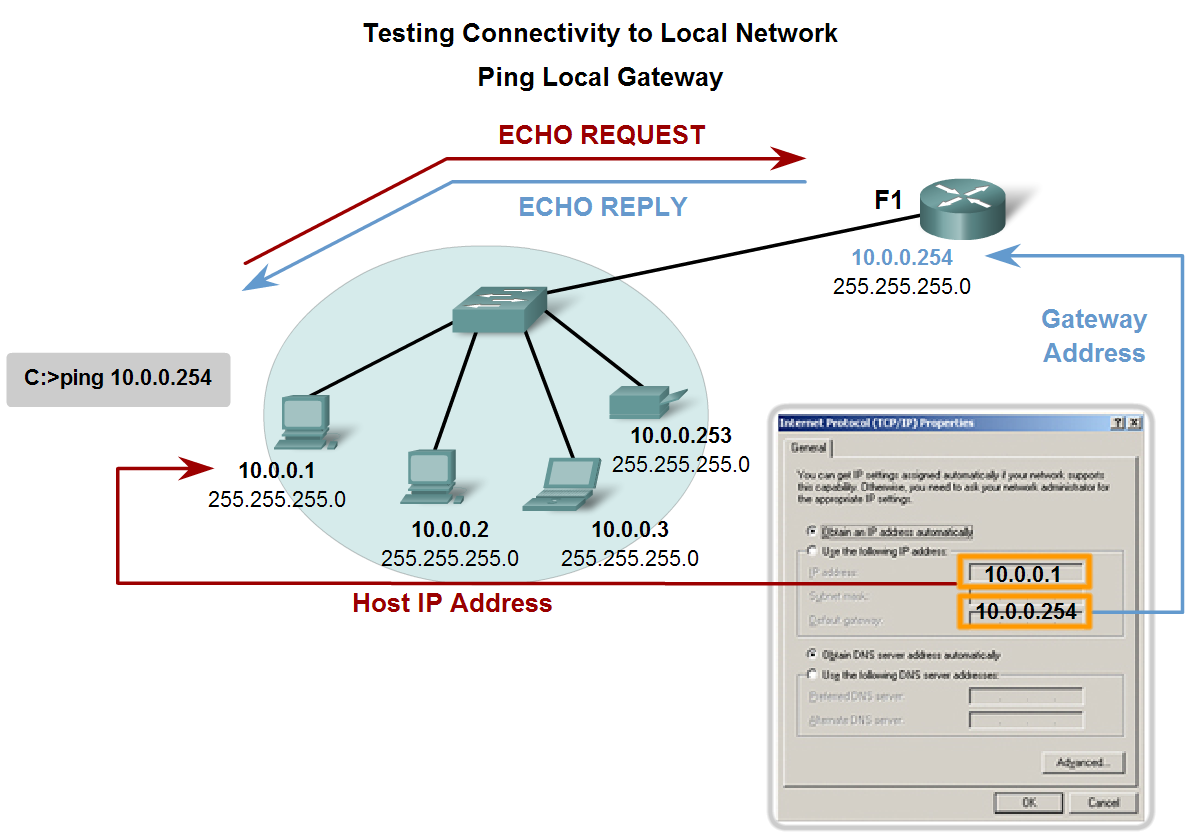
Б – 512 - 172.31.0.0 – 172.31.1.255 /23

Г – 128 172.31.2.0 – 172.31.2.127 /25

А – 32 - 172.31.2.128 – 172.31.2.159 /27

В – 16 - 172.31.2.160 – 172.31.2.175 /28

**3.5 Сүлжээний түвшний протоколыг шалгах, тестлэх**

****

Зураг 3.5.1 Ping команд

Ping бол хостуудын хооронд холболт тогтсон эсэхийг шалгадаг команд юм. Ping тодорхой нэг хаягруу хариу хүссэн хүсэлтийг илгээдэг. Ping командыг TCP/IP сүлжээний 3-р түвшний Internet Control Message Protocol (ICMP) протоколд ашиглагддаг. Ping ICMP Echo Request өгөгдлийг илгээдэг.

Хэрэв тодорхой хаягтай хост Echo request-ийг хүлээж авбал түүнд ICMP Echo Reply гэсэн хариу өгөгдөл илгээдэг. Илгээгдсэн пакет бүрд , ping хариулт өгөгхөд шаардагдах хугацааг хэмждэг.

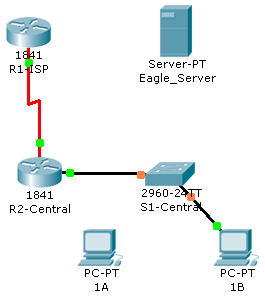
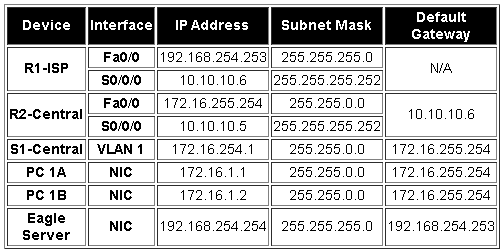
Ping дэлгэцэнд дамжигдсан болон хариу өгсөн хугацааг дэлгэцэнд харуулж байдаг. Энэ нь сүлжээний гүйцэтгэлийн хугацаа юм. Хэрэв Ping командын явцад хариу өгөгдөл ирэхгүй бол дэлгэцэнд timeout гэсэн мэдээлэл гарах ба хостуудын хооронд өгөгдөл дамжихгүй ба холболтын ямар нэг алдаа байгаа гэсэн үг юм.

Ping (127.0.0.1) гэсэн командаар тухайн хост сүлжээнд холбогдсон эсхийг шалгаж болдог. Хэрэв энэ командыг ажиллуулахад алдаа зааж байж байвал хаяг, маск, гэйтвэй дээр ямар нэг тохиргоо буруу байна гэсэн үг болно

**4. Лабораторийн ажил 6: Хэрэглээний болон дамжуулалтын**

**түвшний протоколын уялдаа холбоог судлах**

**Топологи диаграм:**



Зураг 4.1 сүлжээний топологи диаграм ба хаягийн схем

**Судлах зүйлс:**

1. Хост ба сервисийг тохируулах
   * Тус лабораторийн ажлаар дээрх сүлжээний загвар топологийг судлана. Хост ба сервисийн тохиргоог хийж, төхөөрөмжүүдийг холбох
2. DNS, HTTP, UDP, TCP протоколууд хэрхэн хамтарч ажиллахыг судлах
   * Simulation горимд DNS, UDP, HTTP, ба TCP-ийн үйлдлийг харах.

**Товч мэдээлэл:**

Та энэхүү модуль сургалтын турш пакет трэйсерийн стандарт лабораторийн ажлуудыг хийж бодит компьютер, сервер, рүүтер, свич зэрэг сүлжээний ойлголтуудыг судлах болно.

Энэ лабораторийн ажлаар Пакет трэйсерийн тусламжтай хэд хэдэн протоколуудын үйл ажиллагааг мэддэг болно.

**4.1 Даалгавар 1: Топологи тестлэх ба засах**

Серверийг асааж дараах тохиргоог хийх: IP хаяг 192.168.254.254, Сабнет маск 255.255.255.0, Интернэтийн гарц Гэйтвэй 192.168.254.253, DNS-ийг идэвхжүүлж ,

eagle-server.example.com гэж бичээд серверийн IP хаягийг оруул , HTTP идэвхжүүл. Eagle Сервер-ийн Fa0/0 портыг R1-ISP рүүтертэй crossover ( хөндлөн ) кабелиар холбох.

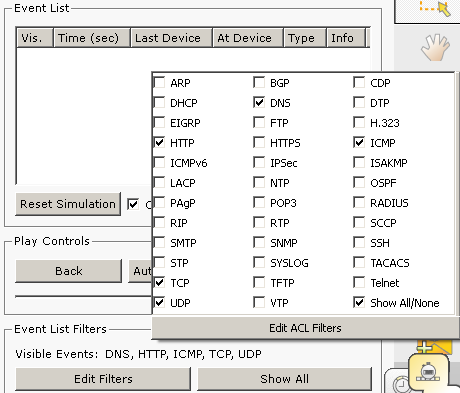
PC 1A компьютерийн тохиргоо хийх: IP хаяг 172.16.1.1, Сабнет маск 255.255.0.0, Интернэтийн гарц Гэйтвэй 172.16.255.254, DNS Сервер 192.168.254.254. PC 1A компьютерийг S1-Central свичийн Fa0/1 порт уруу straight-through ( шулуун ) кабелиар холбох.

Өөрийн хийсэн ажлын үр дүнг  **Check Results** товч дараад  **Assessment Items** цонхыг сонгон шалга. Холболтыг realtime горимд ADD SIMPLE PDU ашиглан PC 1A болон Eagle Сервер хоёрын хооронд тест мессеж дамжуулж шалга.

Энгийн PDU-г нэмэхэд PDU List буюу пакет хэрхэн дамжигдсан тухай мэдээлэл дэлгэцийн Scenario 0 гэсэн хэсэгт гарна. Эхний удаа нэг ping хийхэд **Failed ( алдсан )** гэсэн мэдээлэл гарна. Учир нь ARP процесстой холбоотой, энэ процессийг дараа тайлбарлана. PDU List цонхон дахь "Fire" товчин дээр маузаар 2 удаа товшоод тест мессежийг хоёр дахь удаагаа дамжуулбал **Successful ( амжилттай )** гэсэн мэдээлэл гарч 2 төхөөрөмжийн хооронд мэдээлэл бүрэн дамжигдсаныг илтгэнэ.

Өөр тест пакетийг **New** товчийг дарж шалгаж болно. Жишээ нь: **New** товчийг дарахад Scenario 1 үүсэх бөгөөд PC 1B болон рүүтерийн хооронд пакет дамжих процессийг шалгаж болно. Бүх тест пакетийг устгахдаа  **Delete** товчийг ашиглана.

**4.2 Даалгавар 2: DNS, UDP, HTTP, TCP протоколуудын уялдаа холбоог судлах**



Зураг 4.2 Протоколыг идэвхжүүлэх

Бодит хугацааны ( Realtime) горимоос симуляцийн ( Simulation ) горимд шилжүүл. Event Filter цонхны DNS, UDP, HTTP, TCP, болон ICMP идэвхжүүлнэ. PC 1A компьютерийн веб браузерийг нээж, eagle-server.example.com гэж бичээд Enter дар, дараа нь **Event List** цонхны **Capture / Forward** товчоор DNS, UDP, HTTP ,TCP протоколуудыг барьж авч судал.

PC 1A болон Eagle Server дээрх пакетийн **PDU-г** event listцонхны өнгөтэй дөрвөлжин дээр маузаар дарж  **PDU Information** цонхонд гарах  **Inbound PDU Details** ( орж байгаа протоколийн өгөгдлийн нэгжийн үзүүлэлт)**, Outbound PDU Details** ( гарч байгаа протоколийн өгөгдлийн нэгжийн үзүүлэлт)-г харж болно. Хэрэв "Buffer Full" ( буфер дүүрэн ) мессеж гарч ирвэл, **View Previous Events** товчийг дарна.

**PDU Information** цонхонд гарах эдгээр мэдээллийн тусламжтай DNS, UDP, HTTP, TCP протоколууд хэрхэн хамтран ажиллаж байгааг харж болно.

1. **Лабораторын ажил 7:** **Транспорт түвшний протоколыг**

**Wireshark програм дээр анализ хийх**

**Судлах зүйлс**:

OSI болон TCP/IP загварын транспорт төвшин, Wireshark програм дээр анализ хийх, сүлжээний командууд, чиглүүлэгч төхөөрөмжийн тохиргоо.

**Товч мэдээлэл:**

Хэрэглэгчийн програмаас өгөгдөл гараад үйлдлийн системийн мэдэлд очно. Үйлдлийн систем дамжуулалтын(transport), сүлжээний (network) төвшнүүдийг өөртөө агуулдаг. Энэ удаад бид транспорт төвшнийг судлах гэж байна.

Транспорт төвшинд өгөгдөл TCP, UDP гэсэн хоёр үндсэн протоколоор хувирна. Дээрх 2 протоколын гол үүрэг нь портын дугаараар хаяглах, өөрөөр хэлбэл тухайн өгөгдөл аль програм хангамжид хамаарч байгааг заах юм.

|  |  |  |
| --- | --- | --- |
|  | OSI Model | TCP/IP model |
| USER INTERFACE | APPLICATION | APPLICATION |
| Presentation |
| Session |
| **OPERATION SYSTEM** | **Transport** | **TRANSPORT** |
| Network | INTERNET |
| HARDWARE | Datalink | NETWORK ACCESS |
| Physic |

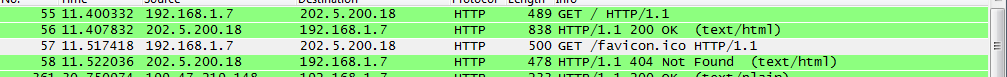
Лабораторын ажлаар бид аппликэшн төвшний HTTP, FTP, DHCP, DNS сэрвэр програмууд транспорт төвшинд ямар протокол ашигладагийг судлаж тэдгээрийн портын дугааруудыг илрүүлнэ.

**5.1 Даалгавар 1:**

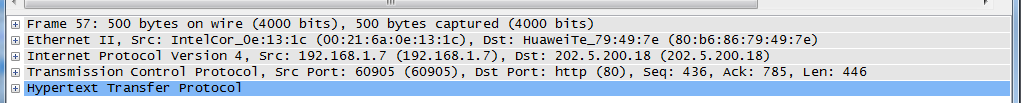
Дээрх аппликэшн төвшний протоколуудыг wireshark ашиглан хялбархан судалж болно. Wireshark ажиллуулаад хэд хэдэн вэбрүү ханд.

**Filter** дээр НТТР гэж бичээд **apply** дар. Ямар нэгэн HTTP протоколтой пакетыг сонгоод TCP, UDP 2-н алийг ашигласан байгааг хар. Эхний зураг дээр сонгогдсон байгаа пакет HTTP протоколыг ашигласан байна.

Тухайн пакетийн дэлгэрэнгүй задаргаа нь доод талын зураг дээр харагдаж байна.



Зураг 5.1



Зураг 5.2

Хоёрдох зурагны доороосоо хоёрдох мөрөнд **Transmission Control Protocol (ТСР)**гэсэн байна. Энэ бол манай вэб өгөгдлийн хувьд транспорт төвшинд TCP протокол ашигласан байгааг харуулж байна.

Мөн уг мөрнөөс хүлээн авагчийн портын дугаар 80 байгааг харж болно. Үүгээр HTTP сэрвэр програм 80 гэсэн портын дугаар ашиглаж байгаа нь харагдана.

Асуулт: Аппликэшн төвшний DNS, FTP, DHCP протоколуудын хувьд транспорт төвшинд ямар протокол ашигладаг болон портын дугаар хэд байна вэ?

Зөвлөмж: тухайн протоколоор шүүлтүүр тавьж түүнийг ашиглан өгөгдөл дамжих нөхцөл бүрдүүл. Жишээ нь бид вэб хуудасруу хандаж байгаа нь HTTP протоколоор өгөгдөл дамжих нөхцөл үүсгэж байна.

**5.2 Даалгавар 2**: **HTTP сервер програм**

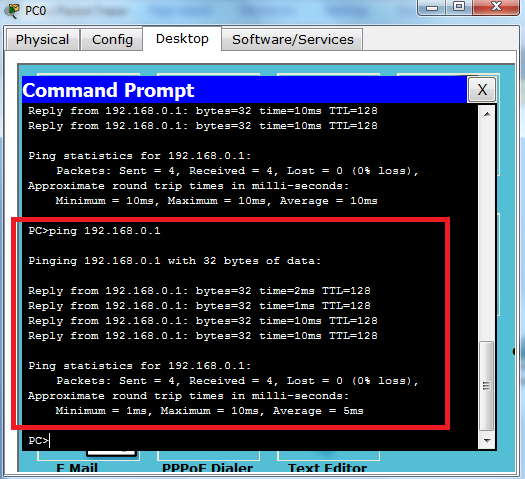
Түрүүчийн хичээл дээр бид HTTP протокол хэрхэн өгөгдөл дамжуулж байгааг аппликэшн төвшинд РТ болон бодит сүлжээг ашиглан судалсан. Энэ удаад аппликэшн төвшний уг протокол транспорт төвшинд ямар протокол ашиглан ямар үйлдэл хийдгийг эхлээд РТ ашиглан хийсвэрээр судална.



Зураг 5.3 Сүлжээний топологи

Зураг 5.3 дээрх сүлжээг байгуулаад төхөөрөмжүүдэд оноосон нэрийг өг. subnet mask нь 255.255.0.0 байх ямар нэгэн сүлжээний хаяг зохиож төхөөрөмжүүдийн IP хаягийг тохируул.

Төхөөрөмж бүхэн өөр хоорондоо өгөгдөл дамжуулах бололцоотой болсныг ping коммандаар шалга. Ping командыг PC1🡪 Desktop 🡪 Command Prompt гэж ороод [ping 192.168.0.1] гэх хэлбэртэй бичнэ.



Зураг 5.4

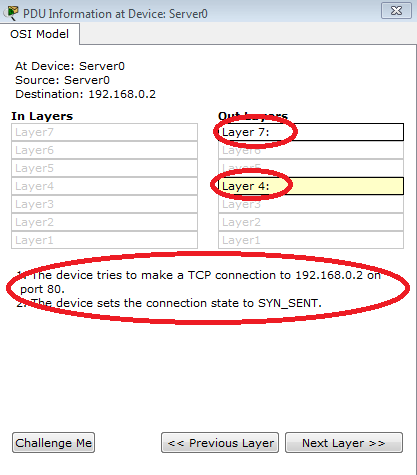
Дэлгэц дээрх 4 мөр нь ping комманд амжилттай болсныг илтгэж байна. Хэрэв бүх төхөөрөмж чинь хоорондоо холбоотой болсон бол цааш явна уу.

Өмнөх хичээлийн мэдлэг дээр үндэслэн HTTP, DNS сэрвэрүүдийг тохируул. HTTP сэрвэр дээр [www.surgalt.com](http://www.surgalt.com) нэртэй вэб хуудас байрлана.

Төхөөрөмжүүдэд DNS хаяг зааж өг. PC1 дээрээс үүсгэсэн вэб хуудасруугаа хандаж байгаа эсэхийг шалга.

Хэрэв вэб хуудас ачаалагдаж байгаа бол РТ симуляци дээр тавиад EDIT FILTER дотор HTTP, DNS, TCP, UDP протоколуудыг үлдээж өгөгдөл хаанаас хаашаа яаж дамжиж байгааг хар.

Асуулт: Доорх зургийн дагуу пакетууд дамжих бөгөөд дамжиж байгаа пакет тус бүрийн утгыг тэмдэглэ.



Зураг 5.5



Зураг 5.6

**5.3 Даалгавар 3: TCP connection**

TCP протокол нь connection oriented буюу холболт дээр суурилдаг протокол юм. Filter хэсэгт хаалтгүйгээр [ТСР] гэж бичээд Apply дар.

Энэ тохиолдолд дан ТСР болон ТСР-ийг ашигладаг бүх аппликэшн төвшний протоколууд хамтдаа баригдана.

Зөвлөмж: туршилтыг эхлэхийн өмнө restart товчийг дарвал цуглуулсан пакетын тоо цөөрч та хүссэн өгөгдлөө таньж барьж авахад дөхөм болно.

Мөн өгөгдөл дамжуулалт дуусмагц stop товчийг дарвал сүлжээн дээрх өгөгдлүүд ар араасаа нэмэгдэлгүй харахад хялбар болдог.

Зөвөлгөөг заавал дагах албагүй.

Одоо вэб браузер ажиллуулаад [www.cisco.edu.mn](http://www.cisco.edu.mn) хаягруу ханд .



Яг зураг дээр харагдаж байгаа шиг гурван пакетыг ол. Дээрх гурван пакетыг ТСР холболт үүсгэж байгаа handshake гэж нэрлэдэг.



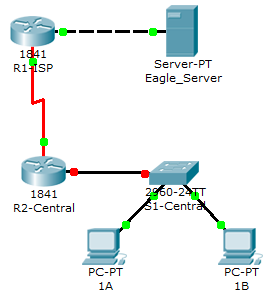
Зураг 5.7

Өөр нэг вэб хаягруу хандаад дээрх үйлдэл хийгдэж байгаа эсэхийг шалга.

Асуулт: Яагаад эхний 2 пакет 62 байт, 3дах пакет 54 байт урттай байгааг пакетын задаргааг судалж үзээд тогтоо.

1. **Лабораторийн ажил 8: IP пакетийн чиглүүлэлт**

**Топологи диаграм:**



Зураг 6.1 Сүлжээний топологи ба хаягийн схем

**Судлах зүйлс:**

1. Рүүтерийн интерфейсийг тохируулах.
2. Чиглүүлэлтийн хүснэгтийг судлах.
3. Статик чиглүүлэлт хийх.
4. IP пакетийг чиглүүлэх.

**Товч мэдээлэл:**

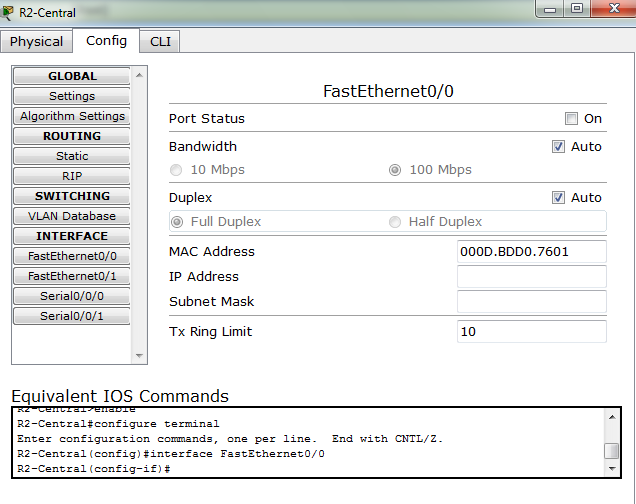
Бид өмнөх лабораторийн ажлаар хэрэглээний түвшний протоколууд болох DNS, HTTP, TFTP, DHCP, Telnet, мөн дамжуулалтын түвшний протокол болох TCP, UDP-г судалсан билээ.

Бидний судалснаар **Inbound** болон **Outbound PDU Details** –д байгаа мэдээлэл нь сүлжээгээр дамжигдаж байгаа IP пакетууд түвшин бүрийн протоколоор дамжихдаа protocol data unit encapsulation буюу протоколын өгөгдлийн нэгжийг багцлалт гэж нэрлэдэх үйлдэл хийгдэж байгааг судалсан билээ.

Энэ лабораторийн ажлаар сүлжээний түвшний голлох протокол болох интернэт протоколыг судлах бөгөөд энгийн IP пакетийн чиглүүлэлтийг хийж сурна.

**6.1 Даалгавар 1: Рүүтерийн интерфейсийг тохируулах.**

Дотоод сүлжээнд дараах асуудал гардаг: PC 1A-ээс Eagle Сервер уруу өгөгдөл дамжуулж болдоггүй (Бодит хугацааны ( Realtime ) горимд шалга). Учир нь рүүтер дээр тохиргоо хийгдээгүй байна гэсэн үг.



Зураг 6.2 Рүүтерийн тохиргоо

Маузыг R2-Central рүүтер дээр аваачихад, Fa0/0 интефейсийн холболтийн талаархи мэдээлэл гарна. Fa0/0 интефейс нь IP хаяг, сабнет масктай ба ассан байх ёстой бөгөөд дотоод сүлжээний Интернэтийн гарц Гэйтвэйгийн үүргийг гүйцэтгэдэг.

Маузны зүүн товчоор R2-Central рүүтерийг сонгож  **Config** цонх уруу орно. **Config** цонхны **INTERFACE, FastEthernet0/0** цэсийг сонгосноор Fa0/0 интефейсийн тохиргоог хийнэ.

IP хаяг 172.16.255.254-ийг IP Address гэсэн мөрөнд оруулах ба сабнет маск 255.255.0.0-г Subnet Mask мөрөнд оруулна , мөн портыг асаахын тулд Port Status-ийн On дөрвөлжинг чагтална.

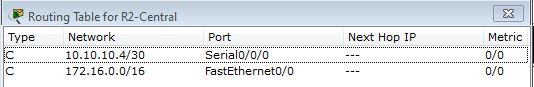
Рүүтерийн цонхыг хаагаад маузаар рүүтерийн интерфейс дээр аваачин ажиллаж байгаа эсэхийг шалга.

Eagle Сервер уруу өгөгдөл дамжуулах гэж оролд. Хэрэв алдаа гарвал ямар асуудал гарсныг тайлбарлана.

**6.2 Даалгавар 2: Чиглүүлэлтийн хүснэгтийг судлах.**

Дэлгэцийн баруун талд байрлах **Inspect Tool** дотроос (томруулдаг шил)-ийг  ашиглан R2-Central рүүтерийн чиглүүлэлтийн хүснэгтийг харж болно. С ( соnnected ) буюу холбогдсон гэсэн үг.

Хэдийгээр та сүлжээнд рүүтер холбогдсон байгааг харах боловч Eagle Сервер уруу өгөгдөл дамжуулж чадахгүй. Учир нь статик эсвэл динамик чиглүүлэлт хийгдээгүй байна гэсэн үг юм.



Зураг 6.3 Чиглүүлэлтийн хүснэгт

**6.3 Даалгавар 3: Статик чиглүүлэлт хийх.**



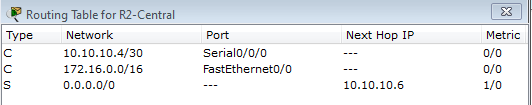
Зураг 6.4 Статик чиглүүлэлт

R2-Central рүүтерийг сонгон **Config** цонхны **ROUTING, Static** цонхыг нээснээр статик чиглүүлэлтийг хийх боломжтой болно.

Тохиргоог хийхдээ default статик чиглүүлэлтийг ашиглана. Network мөрөнд 0.0.0.0 гэсэн хаяг бичнэ, mask мөрөнд 0.0.0.0 гэсэн хаяг бичнэ, next hop ( дараагийн үсрэх хаяг ) мөрөнд 10.10.10.6 ( Энэ хаяг нь R1-ISP рүүтерийн S0/0/0 интерфейсийн IP хаяг юм. ) гэсэн хаяг бичээд **Add** товчийг дарснаар статик чиглүүлэлт хийгдэх бөгөөд энэ чиглүүлэлтийн дагуу 172.16.0.0 /16 Дотоод сүлжээнээс (LAN) ирэх пакетууд R1-ISP рүүтерээр дамжин цааш өөр дотоод сүлжээнд хүрнэ.

**GLOBAL, Settings -**ийн **Save** товчийг дарж статик чиглүүлэлт болон интефейсийн тохиргоог NVRAM-д хадгална. Одоо та чиглүүлэлтийн хүснэгтээс статик чиглүүлэлт хийгдсэн болохыг харж болно.

Дэлгэцийн баруун талд байрлах **Inspect Tool** (томруулдаг шил)-ийг  ашиглан R2-Central рүүтерийн чиглүүлэлтийн хүснэгтийг хар. S үсэг нь static буюу статик чиглүүлэлт гэсэн үг.



Зураг 6.5 Чиглүүлэлтийн хүснэгт

Өөрийн хийсэн ажлын үр дүнг  **Check Results-**ийн **Assessment Items-**ийг маузаар сонгон шалгана .

Add Simple PDU гэсэн  дүрсийн тусламжтай тест мессежийг компьютер1B болон Eagle Серверийн хооронд дамжуулж шалга. Энгийн PDU-г нэмэхэд PDU List буюу пакет хэрхэн дамжигдсан тухай мэдээлэл дэлгэцийн Scenario 0 гэсэн хэсэгт гарна.

Эхний удаа нэг ping хийхэд **Failed ( алдсан )** гэсэн мэдээлэл гарна. Учир нь ARP процесстой холбоотой, энэ процессийг дараа тайлбарлана.

PDU List цонхон дахь "Fire" товчин дээр маузаар 2 удаа товшоод тест мессежийг хоёр дахь удаагаа дамжуулбал **Successful ( амжилттай )** гэсэн мэдээлэл гарч 2 төхөөрөмжийн хооронд мэдээлэл бүрэн дамжигдсаныг илтгэнэ.  
  
**6.4 Даалгавар 4: IP пакетийн явах замыг судлах.**

Симуляцийн ( Simulation ) горимд шилжих. Даалгавар 3-д үүсгэсэн PDU-г ашиглан **Capture / Forward** товчийн тусламжтай пакетийг PC 1A –аас Eagle Сервер үрүү дамжуулж.

Ажлын талбай дахь дугтуй эсвэл Event List цонхны Info багананд байгаа өнгөтэй дөрвөлжин дээр маузаар дарж пакетийн алхам бүрийг судал.

**7. Лабораторын ажил 9: 2-тын тоон систем, хөрвүүлгэ, IP хаяг.**

**Судлах зүйлс**:

2-тын тоон систем дээр үйлдэл хийх, IP хаяг сабнэт маск хоёроос сүлжээний хаяг, броадкаст хаягуудыг бодох, чиглүүлэгч төхөөрөмжийн энгийн тохиргоог сурах.

**Товч мэдээлэл:**

Тухайн нэг төхөөрөмжийн хаягийг IP хаяг сабнэт маск хоёр нийлж байж бүрэн тодорхойлж чаддаг. Өөрөөр хэлбэл уг хоёр хаягийн дундаас тухайн төхөөрөмжийг ямар сүлжээнд харъялагдаж байгааг илэрхийлнэ.

Өмнө нь бид сабнэт маскийг 255.255.255.0 гэсэн ганцхан тохиолдолд ашиглаж байсан бол угтаа 0.0.0.0 – 255.255.255.252 хүртэл сабнэт маск байж болдог.

Тооцооллыг 2тын тоон системд and, or үйлдэл, 2тоос 10труу, 10таас 2труу шилжүүлэх үйлдлүүдээр хийнэ.

Лабораторын ажлаар IP хаяг дээр үйлдэл хийх аргыг эзэмшиж чиглүүлэгч төхөөрөмжийн анхан шатны тохиргоонуудыг туршина.

**7.1 Даалгавар 1: 2т, 10т-ын тооллын систем**

|  |  |  |
| --- | --- | --- |
| 2тын тооллын систем | 10тын тооллын систем | 16тын тооллын систем |
| 0b 0000 | 0 | 0x 0 |
| 0b 0001 | 1 | 0x 1 |
| 0b 0010 | 2 | 0x 2 |
| 0b 0011 | 3 | 0x 3 |
| 0b 0100 | 4 | 0x 4 |
| 0b 0101 | 5 | 0x 5 |
| 0b 0110 | 6 | 0x 6 |
| 0b 0111 | 7 | 0x 7 |
| 0b 1000 | 8 | 0x 8 |
| 0b 1001 | 9 | 0x 9 |
| 0b 1010 | 10 | 0x A |
| 0b 1011 | 11 | 0x B |
| 0b 1100 | 12 | 0x C |
| 0b 1101 | 13 | 0x D |
| 0b 1110 | 14 | 0x E |
| 0b 1111 | 15 | 0x F |

2тоос 10труу хөрвүүлэх:

**AND**

|  |  |  |
| --- | --- | --- |
| **A** | **B** | **C** |
| **0** | **0** | **0** |
| **0** | **1** | **0** |
| **1** | **0** | **0** |
| **1** | **1** | **1** |

0b 11010011 and 0b 00110010 = 0b 00010010

0xd3 and 0x32 = 0x12

**OR**

|  |  |  |
| --- | --- | --- |
| **A** | **B** | **C** |
| **0** | **0** | **0** |
| **0** | **1** | **1** |
| **1** | **0** | **1** |
| **1** | **1** | **1** |

0b11010011 or 0b00110010 = 0b 11110011

0xd3 or 0x32 = 0xf3

Асуулт:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AND** | 0x87 | 0x36 | 0xf7 | 0xa7 | 0xac |
| 0xb8 |  |  |  |  |  |
| 0xad |  |  |  |  |  |
| 0x0f |  |  |  |  |  |
| 0x1b |  |  |  |  |  |
| 0xb4 |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OR** | 0x87 | 0x36 | 0xf7 | 0xa7 | 0xac |
| 0xb8 |  |  |  |  |  |
| 0xad |  |  |  |  |  |
| 0x0f |  |  |  |  |  |
| 0x1b |  |  |  |  |  |
| 0xb4 |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AND** | 0x5687 | 0xf536 | 0x4af7 | 0xa3a7 | 0x65ac |
| 0x5cb8 |  |  |  |  |  |
| 0xd7ad |  |  |  |  |  |
| 0x140f |  |  |  |  |  |
| 0x7c1b |  |  |  |  |  |
| 0x4ab4 |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OR** | 0x5687 | 0xf536 | 0x4af7 | 0xa3a7 | 0x65ac |
| 0x5cb8 |  |  |  |  |  |
| 0xd7ad |  |  |  |  |  |
| 0x140f |  |  |  |  |  |
| 0x7c1b |  |  |  |  |  |
| 0x4ab4 |  |  |  |  |  |

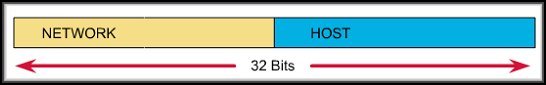
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AND** | 43 | 76 | 87 | 187 | 200 |
| 0 |  |  |  |  |  |
| 58 |  |  |  |  |  |
| 97 |  |  |  |  |  |
| 135 |  |  |  |  |  |
| 253 |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OR** | 43 | 76 | 87 | 187 | 200 |
| 0 |  |  |  |  |  |
| 58 |  |  |  |  |  |
| 97 |  |  |  |  |  |
| 135 |  |  |  |  |  |
| 253 |  |  |  |  |  |

**7.2 Даалгавар 2: IP хаяг, сабнэт маск, сүлжээний хаяг, бродкаст хаяг**

IP хаяг = сабнэт маск = 32 бит

IP хаяг дотор сүлжээний, хостын гэсэн хоёр хэсэг багтдаг.

****

Хаагуураа зааглагдаж байгааг сабнэтмаск зааж өгнө.

Сабнэт маск нь мөн 32 бит бөгөөд 1-ийн цуваагаар эхлээд 0-ийн цуваагаар дууссан хэлбэртэй байна. 1-ийн болон 0-ийн цувааны урт хэд ч байж болдог.

172.89.12.1

255.255.255.0 гэж байвал сүлжээний хаяг нь 172.89.12 хостын хэсэг нь .1 болно.

**Дүрэм:**

Тухайн IP хаягийг сабнэт масктай нь AND хийвэл сүлжээний хаяг гарна. Өөрөөр хэлбэл сүлжээний оронг хэвээр үлдээгээд хостын оронг тэг болгохтой ижил үйлдэл юм. Жнь: дээрх хаягны хувьд сүлжээний хаяг нь 172.89.12.0 болно.

Тухайн IP хаягийг сабнэт маскын урвуутай OR хийвэл броад каст хаяг гарч ирнэ. Өөрөөр хэлбэл сүлжээний оронг хэвээр үлдээгээд хостын оронг дан нэгээр дүүргэхтэй ижил үйлдэл юм. Жнь: дээрх хаягны хувьд сүлжээний хаяг нь 172.89.12.255 болно.Сүлжээний хаяг броадкаст хаяг хоёрыг хостыг хаяглахад ашиглахгүй бөгөөд энэ хоёроос бусад хаягаар хостыг хаяглаж болно. Тэдгээр хаягуудыг ашиглаж болох хостын хаяг гэж ярьдаг.

Жишээ:

192.168.2.165

255.255.255.0

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP хаяг | 192 | 168 | 2 | 165 |
| Сабнэт маск | 255 | 255 | 255 | 0 |
|  |  |  |  |  |
| IP хаяг | 11000000 | 10101000 | 00000010 | 10100101 |
| Сабнэт маск | 11111111 | 11111111 | 11111111 | 00000000 |
| Cүлжээний хаяг | 11000000 | 10101000 | 00000010 | 00000000 |
| Бродкаст хаяг | 11000000 | 10101000 | 00000010 | 11111111 |
|  |  |  |  |  |
| Cүлжээний хаяг | 192 | 168 | 2 | 0 |
| Бродкаст хаяг | 192 | 168 | 2 | 255 |
| Хамгийн эхний ашиглаж болох хостын хаяг | 192 | 168 | 2 | 1 |
| Хамгийн сүүлийн ашиглаж болох хостын хаяг | 192 | 168 | 2 | 254 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP хаяг | 10 | 254 | 189 | 65 |
| Сабнэт маск | 255 | 255 | 240 | 0 |
|  |  |  |  |  |
| IP хаяг | 00001010 | 11111110 | 10111101 | 01000001 |
| Сабнэт маск | 11111111 | 11111111 | 11110000 | 00000000 |
| Cүлжээний хаяг | 00001010 | 11111110 | 10110000 | 00000000 |
| Бродкаст хаяг | 00001010 | 11111110 | 10111111 | 11111111 |
|  |  |  |  |  |
| Cүлжээний хаяг | 10 | 254 | 176 | 0 |
| Бродкаст хаяг | 10 | 254 | 191 | 255 |
| Хамгийн эхний ашиглаж болох хостын хаяг | 10 | 254 | 176 | 1 |
| Хамгийн сүүлийн ашиглаж болох хостын хаяг | 10 | 254 | 191 | 154 |

Асуулт: Дараах хаягуудын сүлжээний хаяг, бродкаст хаяг, ашиглаж болох хамгийн эхний хостын хаяг, ашиглаж болох хамгийн сүүлийн хостын хаягуудыг ол.

65.78.214.24 - 255.255.192.0

156.52.123.76 - 255.255.255.128

123.24.255.90 - 255.255.255.0

241.251.209.9 - 255.224.0.0

87.128.200.170 - 255.255.248.0

234.170.67.93 - 252.0.0.0

35.84.38.4 - 255.255.254.0

4.74.37.170 - 255.255.224.0

64.27.109.3 - 240.0.0.0

74.43.148.26 - 255.255.0.0

**7.3 Даалгавар 3: сабнэт маск**

Сабнэт маск нь 1-ийн цуваагаар эхлээд 0-ийн цуваагаар дууссан тоо байх ёстой. Жнь:

11111111.11111000.00000000.00000000 эсвэл 11111111.11111111.11000000.00000000

Гэх мэт.

Сабнэт маскын 1-тэй хэсэг нь түүнд харгалзах IP хаягийнхаа сүлжээний орны тоо 0-тэй хэсэг нь хостын орны тоог заадаг болохыг мэдэж авлаа. Сабнэт маскыг бичиг баримт дээр тэмдэглэхэд төвөггүй, зай бага эзлүүлэх зорилгоор богиносгож бичих хувилбар байдаг.

**Дүрэм:**

Сабнэт маскыг богиноор бичихдээ түүнд байгаа 1-ийн цувааны уртыг бичнэ.

Жишээ:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 255 | 255 | 240 | 0 | /20 |
| 11111111 | 11111111 | 11110000 | 00000000 | 20 ширхэг 1 байна |

255.255.240.0 = /20 Үүнийг IP хаягтай нь хамт бичихдээ 87.234.9.123/20 гэж бичнэ.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 255 | 255 | 0 | 0 | /16 |
| 11111111 | 11111111 | 00000000 | 00000000 | 16 ширхэг 1 байна |

255.255.0.0 = /16 Үүнийг IP хаягтай нь хамт бичихдээ 87.234.9.123/16 гэж бичнэ.

Асуулт:

Даалгавар 2 дээр гарсан бүх сабнэт маскуудыг богино хэлбэрт оруулж бич.

**7.4 Даалгавар 4: РТ симуляц**



Зурагт өгсөн хэлбэртэй сүлжээг РТ програм дээр байгуул. Өмнөх лабуудаас ялгаатай нь компьютерууд маань сэрвэрүүдээс ялгаатай сүлжээнд орж байна.

Шар өнгийн сүлжээнд 255.255.224.0 сабнэт масктай, улаан өнгийн сүлжээнд 255.255.255.248 сабнэт масктай IP сүлжээний хаяг сонгон авч түүн дотроос ашиглагдаж болох хаягуудаар PC1, PC2, HTTP server, DNS server, чиглүүлэгч төхөөрөмжийн хоёр талын интерфэйсүүд буюу бүгд 6 хостод зохих IP хаягийг олгож өг. DNS server дээрх вэб сэрвисийг зогсоож ганцхан DNS сэрвисийг асаалттай үлдээ.

HTTP server дээр ганцхан HTTP сэрвисийг асаалттай үлдээ.

Тохиргоо хийж дууссаны дараа компьютеруудаас HTTP SERVER дээрх вэб хуудсруу [www.surgalt.com](http://www.surgalt.com) хаягаар хандах боломжтой байх ёстой.

**8. Лабораторийн ажил 10: IP хаягийн төлөвлөлт**

**Товч мэдээлэл:**

Компьютерийн сүлжээн дэх тухайн төхөөрөмжийг бусад төхөөрөмжөөс ялгаж өгдөг логик хаягийг IP хаяг гэж нэрлэдэг. IP хаягийг үйлдлийн системд зааж өгөх ба сүлжээний түвшинд ашиглагдана.

IP хаяг төхөөрөмжийг орон зайн байрлалаар хаана оршиж байгааг зааж чаддаг. Чиглүүлэгч төхөөрөмж дээр ирсэн пакетаас очих төхөөрөмжийн IP хаягийг уншаад цааш дамжигдвал зохих сүлжээний интерфэйсээр урагшлуулдаг.

Пакет эхлэлийн цэгээс эцсийн цэгтээ хүртэл олон сүлжээний төхөөрөмжөөр дамжих боловч сүлжээний түвшинд анх байсан өгөгдлийн хэлбэрээ огт өөрчилдөггүй. Лабораторын ажлаар IP хаягуудыг дэд сүлжээ болгон хуваах, чиглүүлэгч төхөөрөмжүүдийг тохируулах ажил хийнэ.

**Дасгал 1: IP хаяг дээр тооцоо хийх**

Өмнө үзсэн онолын мэдлэг дээр үндэслэн дараах IP хаягуудын сүлжээний хаяг, бродкаст хаягуудыг бодож гаргаад тухайн сүлжээ нийт хэдэн хаягтай, тэдгээрээс хэд нь хостыг хаягладаг хаяг (боломжит хостын тоо гэж ярьдаг) болохыг тогтоо. Сүлжээний хаяг бродкаст хаяг хоёроор хост хаягладаггүй.

172.20.0.9/23

78.65.200.23/14

202.5.192.8/27

**Дасгал 2: Сүлжээг дэд сүлжээнд хуваах**

IPv4 хаягийн хүрэлцээ бага болсноор нэг том сүлжээнээс дэд сүлжээ үүсгэх аргыг бий болгожээ. Дэд сүлжээнд хувааснаар тухайн сүлжээний ашиглагдахгүй хаягийн тоо багасдаг байна. Жишээ нь:



Хэлбэртэй сүлжээ өгөгдсөн бол ашиглахгүй хаягийн хэмжээг хамгийн бага байлгахын тулд

A cүлжээнд 32 хосттой

Б cүлжээнд 512 хосттой

В cүлжээнд 16 хосттой

Г cүлжээнд 128 хосттой

Дэд сүлжээ үүсгэж өгөх шаардлагатай болж байна. Гэвч уг байгууллага 172.31.0.0/16 гэсэн нэг л сүлжээний мужийг ашигладаг бол уг сүлжээгээ дээрх 4 тусдаа жижиг сүлжээнд ашиглахын тулд хуваах хэрэгтэй болно.

**Дүрэм:**

* Дэд сүлжээний хэрэгцээг хангах сүлжээний хаягийн мужийн уртыг тодорхойлно.
* Уртаар нь эрэмбэлэнэ.
* Эх сүлжээний эхлэлээс сүлжээний хаягийн уртаар тасдана.
* Сабнэт маскуудыг бодож гаргана.

Жишээ:Дээрх өгөгдөл дээр сүлжээг хэрхэн хуваахыг харъя.

A сүлжээ 24 хосттой бол 32 хаягтай сүлжээ хувааж өгнө.

Б сүлжээ 400 хосттой бол 512 хаягтай сүлжээ хувааж өгнө

В сүлжээ 10 хосттой бол 16 хаягтай сүлжээ хувааж өгнө

Г сүлжээ 70 хосттой бол 128 хаягтай сүлжээ хувааж өгнө

Одоо сүлжээнүүдээ хаягийн тоогоор нь эрэмбэлнэ.

Б – 512

Г – 128

А – 32

В – 16

Дараа нь хуваалтаа хийнэ

Б – 512 172.31.0.0 – 172.31.1.255 (Энэ хооронд нийт 512 хаяг байгаа)

Г – 128 172.31.2.0 – 172.31.2.127 (Энэ хооронд нийт 128 хаяг байгаа)

А – 32 172.31.2.128 – 172.31.2.159 (Энэ хооронд нийт 32 хаяг байгаа)

В – 16 172.31.2.160 – 172.31.2.175 (Энэ хооронд нийт 16 хаяг байгаа)

Хамгийн сүүлд сүлжээ тус бүрийн сабнэт маскийг бодож гаргана. Сабнэт маскын тоо нь сүлжээний оронгийн тоогоор шууд илэрхийлэгддэг.

IP хаяг 32 бит = Сүлжээний орон + Хостын орон

Б – 512 172.31.0.0 – 172.31.1.255 /23 32-9=23

255.255.254.0

Г – 128 172.31.2.0 – 172.31.2.127/25 32-7=25

255.255.255.128

А – 32 172.31.2.128 – 172.31.2.159 /27 32-5=27

255.255.255.224

В – 16 172.31.2.160 – 172.31.2.175 /28 32-4=28

255.255.255.240

Асуулт: доорх эх сүлжээнүүдийг өгсөн шаардлагын дагуу дэд сүлжээнд хуваа.

Эх сүлжээ - 172.30.0.0/16

А сүлжээ - 26 хосттой

Б сүлжээ - 250 хосттой

В сүлжээ - 100 хосттой

Г сүлжээ - 2 хосттой

Эх сүлжээ - 10.0.0.0/12

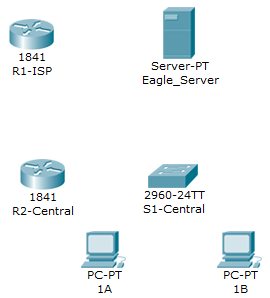
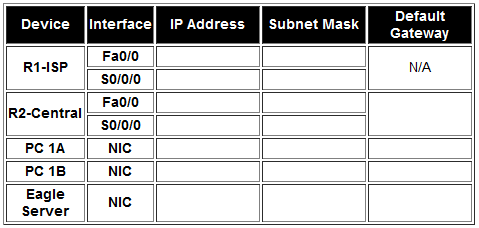
А сүлжээ - 40 хосттой

Б сүлжээ - 50 хосттой

В сүлжээ - 2 хосттой

Г сүлжээ - 2 хосттой

**Топологи диаграм:**



Зураг 8.1 Сүлжээний топологи диаграм ба хаягийн схем

**Судлах зүйлс:**

1. Дэд сүлжээг төлөвлөх
   * Дэд сүлжээг төлөвлөх дасгал ажиллах.
2. Сүлжээг байгуулах.
   * Төхөөрөмжүүдийг этернэт болон сериал кабелиар холбох.
3. Сүлжээг тохируулах.
   * Сервер, компьютер, рүүтерийн интерфейсийг дэд сүлжээний төлөвлөлтийн схемийн дагуу хаяглах, сервисүүдийг тохируулах, статик чиглүүлэлт хийх.
4. Сүлжээг тестлэх.
   * ping, trace, веб траффик, **Inspect** хэрэгслийг ашиглах

**8.1 Даалгавар 1: Эх сүлжээг дэд сүлжээнд хуваах, IP хаягийн тооцоо хийх**

192.168.23.0 /24 IP хаягтай эх сүлжээ өгөгдсөн бөгөөд доорх дэд сүлжээнд хуваа.

**Дэд сүлжээнүүд:**

* 1-р дэд сүлжээ , одоо байгаа student LAN сүлжээ ( R2-Central рүүтерээр дамжиж гадаад сүлжээнд холбогдоно), 60 хосттой ;
* 2-р дэд сүлжээ, ирээдүйд шинээр байгуулах future student LAN сүлжээ, 28 хосттой;
* 3-р дэд сүлжээ, одоо байгаа ISP ( интернэтийн сервес үзүүлэгч байгууллага) LAN сүлжээ, 12 хосттой;
* 4-р дэд сүлжээ, ирээдүйд шинээр байгуулах ISP LAN сүлжээ, 8 хосттой;
* 5-р дэд сүлжээ, одоо байгаа WAN, цэгээс цэгрүү холболт;
* 6-р дэд сүлжээ, ирээдүйд шинээр байгуулах WAN, цэгээс цэгрүү холболт;
* 7-р дэд сүлжээ, ирээдүйд шинээр байгуулах WAN, цэгээс цэгрүү холболт;

**Интерфейсийн IP хаяг:**

* Серверийн IP хаягт одоо байгаа ISP LAN сүлжээний хамгийн сүүлээсээ 2 дахь боломжит хостийн хаягийг олгоно.
* R1-ISP's Fa0/0 интерфейсд одоо байгаа ISP LAN сүлжээний хамгийн сүүлийн боломжит хостийн хаягийг олгоно.
* R1-ISP's S0/0/0 интерфейсд одоо байгаа WAN сүлжээний хамгийн сүүлийн боломжит хостийн хаягийг олгоно.
* R2-Central's S0/0/0 интерфейсд одоо байгаа WAN сүлжээний хамгийн эхний боломжит хостийн хаягийг олгоно.
* R2-Central's Fa0/0 интерфейсд одоо байгаа student LAN сүлжээний хамгийн сүүлийн боломжит хостийн хаягийг олгоно.
* Компьютер 1A ба 1B-д одоо байгаа student LAN сүлжээний хамгийн эхний 2 боломжит хостийн хаягийг олгоно.

**Нэмэлт тохиргоо:**

* Компьютер 1A ба 1B-д DNS сервисийн IP хаягийг олгоно.
* Сервер дээр DNS сервисийг идэвхжүүлнэ, домэйн нэр нь eagle-server.example.com, бас HTTP сервисийг идэвхжүүл.
* R1-ISP рүүтерийн цуваа интерфейсд клокын хэмжээг 64000-аар тохируул.

(цуваа холболтын төгсөгөл буюу DCE тал дээр хугацааны механизм ажилладаг)

* R2-Central-ийн цуваа интерфейс буюу DTE тал дээр клокын хэмжээ хэрэггүй байдаг.

**8.2 Даалгавар 2: Пакет трэйсер дээр сүлжээг угсрах.**

* R1-ISP S0/0/0-ийн цуваа DCE кабелийг R2-Central S0/0/0-тай холбо.
* Компьютер PC 1A-ийг S1-Central свичийн хамгийн эхний FastEthernet порттой холбо.
* Компьютер PC 1B-ийг S1-Central свичийн хоёр дахь FastEthernet порттой холбо.
* R2-Central рүүтерийн Fa0/0 интерфейсийг S1-Central свичийн хамгийн сүүлийн FastEthernet порттой холбо.
* Бүх төхөөрөмж болон төхөөрөмж дээрх тэжээлийг залгасан байна.

**8.3 Даалгавар 3: Сүлжээний тохиргоо хийх.**

Сервер, 2 рүүтер, 2 компьютерийг тохируулахдаа IOS CLI-ийг ашиглах шаардлагагүй ба свичийг тохируулахгүй. Статик чиглүүлэлт болон интерфейсийг GUI дээр тохируулахаас бусад тохиргоо хийгдсэн болно. R1-ISP дээр хийгдэх статик чиглүүлэлтэнд R2-Central рүүтерийн цуваа интерфейсийн IP хаягийг өгөх ба R2-Central дээр хийгдэх статик чиглүүлэлтэнд R1-ISP рүүтерийн цуваа интерфейсийн IP хаягийг өгнө.

**8.4 Даалгавар 4: Сүлжээг тестлэх.**

Ping, trace командууд, веб траффик, **Inspect** хэрэгслийг ашигла. Пакетийн урсгалыг HTTP, DNS, TCP, UDP, ба ICMP протоколуудыг идэвхжүүлэн тестлэн сүлжээг дэх процессийг судал.