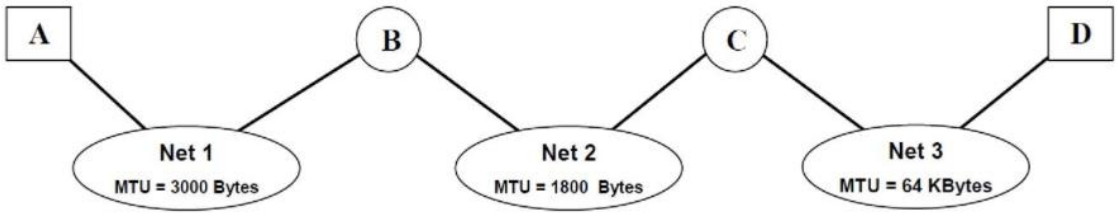
| |
|---|
| **نام و نام‌خانوادگی:** |
| **شماره دانشجویی:** |

توضیحات:

- مهلت تحویل تمرین **۲۵ ام خرداد** در نظر گرفته شده است.
- پاسخ به تمرین ها به صورت انفرادی باشد و اگر تقلب یافت شود نمره تمرین **صفر** خواهد شد.
- نظم و خوانایی تمرین از اهمیت بالایی برخوردار می باشد.
- خواهش می شود تمرین خود را در قالب یک فایل PDF با نام **"HW1_FirstnameLastName_StdudentNumber"** مانند؛ "HW4_ParsaAliEsfahani_ 9631052.pdf" و در مهلت یاد شده در سایت بارگزاری فرمایید.
- پرسش های خود درباره این تمرین را می توانید از راه ایمیل های **autcnta@gmail.com** بیان کنید.

۱. فرض کنید گره A می خواهد بسته ای به اندازه ی 4000 بایت (شامل سرآیند) را برای گره D ارسال کند. اطلاعات fragment های دریافت شده توسط گره C مربوط به این بسته را مطابق جدول زیر مشخص کنید




| | Total Length | Identification | MF | Fragment offset |
|---|---|---|---|---|
| Original packet | 4000 = 3980 + 20 | ID | | |
| #1 | 1796 = 1776 + 20 | ID | 1 | 0 |
| #2 | 1796 = 1776 + 20 | ID | 1 | 1776/8 = 222 |
| #3 | 448 = 428 + 20 | ID | 0 | 444 |

در این جا در هر Net با توجه به مقدار MTU بسته fragment می شود و به گره بعدی ارسال می شود، هر گره بعد از سر هم بندی قطعه ها، مجدد بر اساس ظرفیت Net بعدی عمل قطعه بندی را انجام می دهد، بنابراین می توان فرض کرد گره B بسته ای به اندازه ی 4000 بایت را به سمت گره C ارسال می کند و به اینصورت fragment های دریافتی آن را بررسی می کنیم.

Total Length = Payload + Header Length

۲. قالب HEADER بسته های پروتکل IPv4 را با رسم شکل بیان کنید، سپس به سوالات زیر در رابطه به IPv4 پاسخ دهید.

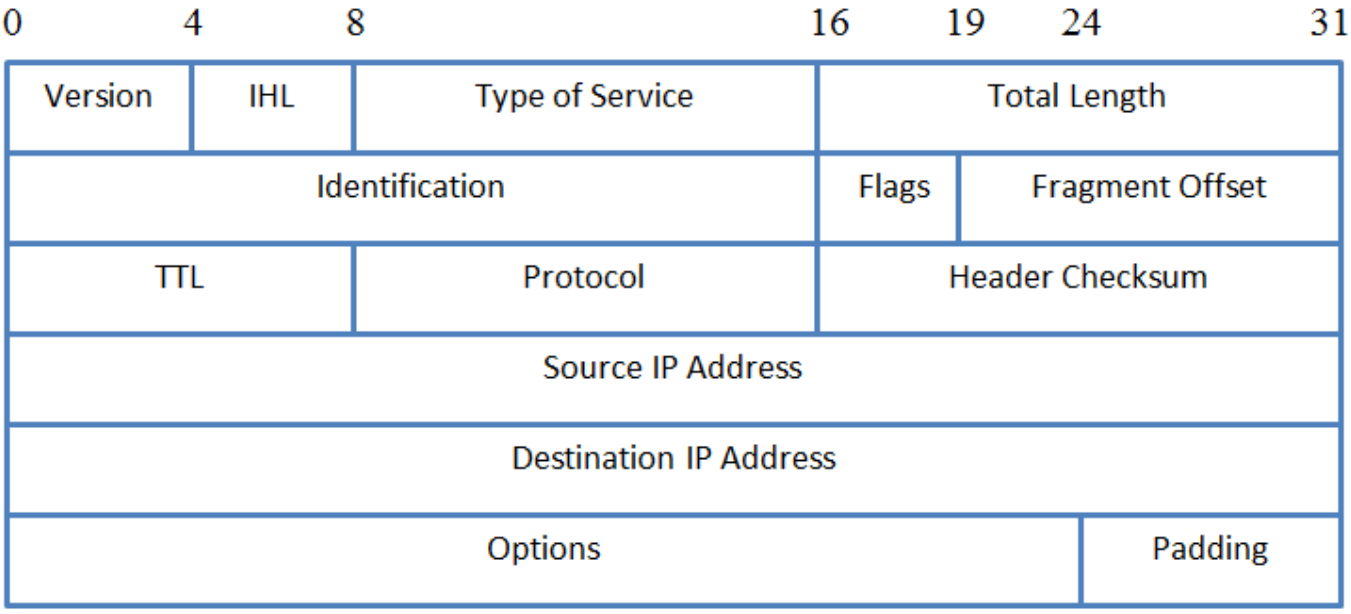



Fig: IPv4 Frame Format

- در بست های IPv4 مقدار فیلد PROTOCOL چیست؟ و چه مقادیری می تواند داشته باشد؟

این فیلد ۸ بیتی شامل یک عدد است که نوع پروتکلی که داده (payload) با آن ارسال شده است را مشخص می کند. این اعداد برای پروتکل های پر کاربرد TCP و UDP به ترتیب برابر با ۶ و ۱۷ است. تعداد دیگری از این اعداد در جدول زیر آمده است.

# TCP/IP Protocol Numbers

**Table 1-1** TCP/IP protocol numbers

| Number | Acronym | Protocol Name |
|---|---|---|
| 0 | HOPOPT | IPv6 Hop-by-Hop Option |
| 1 | ICMP | Internet Control Message |
| 2 | IGMP | Internet Group Management |
| 3 | GGP | Gateway-to-Gateway Protocol |
| 4 | IP | IP in IP (**encapsulation**) |
| 5 | ST | Stream |
| 6 | TCP | Transmission Control Protocol |
| 7 | UCL | User Control List |
| 8 | EGP | Exterior Gateway Protocol |
| 9 | IGP | Any private interior gateway |
| 10 | BBN-RCC-MON | BBN RCC Monitoring |
| 11 | NVP-II | Network Voice Protocol |
| 12 | PUP | Peripheral Update Protocol |
| 13 | ARGUS | ARGUS protocol |
| 14 | EMCON | Emergency Condition |
| 15 | XNET | Cross Net Debugger |
| 16 | CHAOS | Chaos protocol |
| 17 | UDP | User Datagram Protocol |
| 18 | MUX | Multiplexing |
| 19 | DCN-MEAS | DCN Measurement Subsystems |
| 20 | HMP | Host Monitoring Protocol |

- فرض کنید در یک بسته ی IPv4 مقدار بیت M برابر با صفر باشد، header length (IHL) =10، total length = 400 و fragment offset = 300 باشد. در این صورت موقعیت بسته، و نقطه ی شروع و پایان payload را مشخص کنید. (منظور از موقعیت بسته آن است که بعد از قطعه بندی و ارسال بسته ها، بسته ی فعلی جزو بسته های ابتدایی، میانی یا انتهایی است؟)

بیت M (More Fragment) برابر با صفر است، بدان معناست که قطعه ی دیگری برای ارسال نیست بنابراین بسته ی فعلی **آخرین** بسته می باشد.

IHL یک فیلد ۴ بیتی است که تعداد بلوک های ۳۲ بیتی (یا ۴ بایتی) Header را تعیین می کند. از آنجایی که تعداد بلوک ها برابر با ۱۰ است بنابراین اندازه ی Header بر حسب بایت برابر است با:

Header Length = 10*4 = 40 bytes
Payload = Total Length – Header Length = 400 – 40 = 360 bytes

به کمک fragment offset می توانیم حجم داده ای که تا کنون ارسال شده است را محاسبه کنیم (یا در واقع شروع محدوده ی payload بسته ی فعلی):

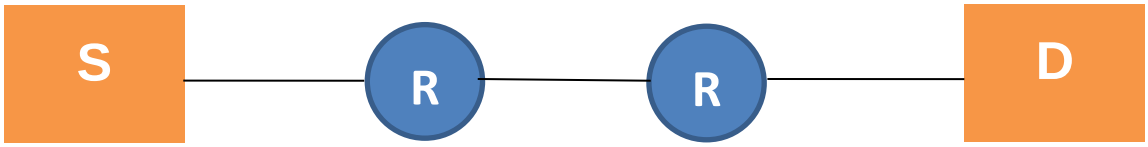
Fragment offset * 8 = 300 * 8 = 2400 bytes

با توجه به اندازه ی payload این بسته و اینکه index از صفر شروع می شود، پایان محدوده برابر است با:

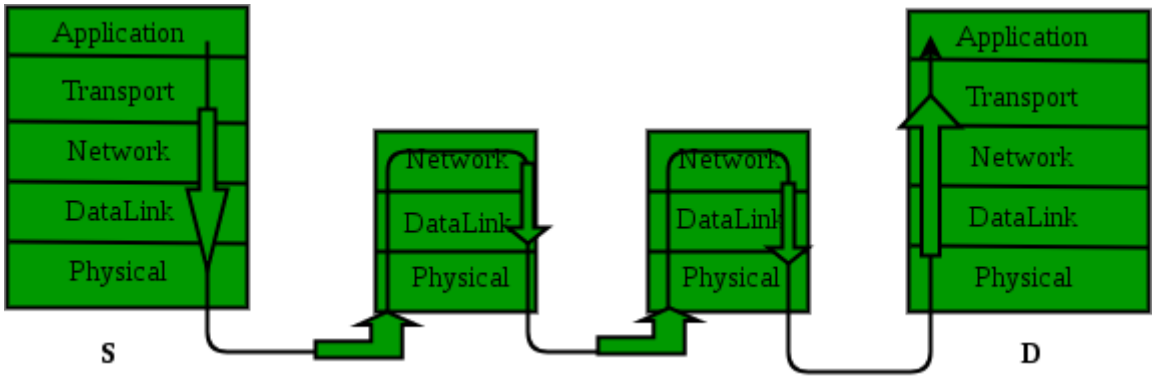
2400 + 360 - 1 = 2759 bytes

۳. به سوالات زیر پاسخ دهید و دلیل خود را به صورت خلاصه ذکر کنید.

الف_ در شکل زیر مبدا را گره S و مقصد را گره D در نظر بگیرید که این دو توسط دو روتر (R) بهم مرتبط اند. مشخص کنید هر بسته در انتقال از S به D چند بار از لایه ی شبکه عبور می کند؟




روتر ها دستگاه هایی هستند که وظیفه ی مسیر یابی را بر عهده دارند، بنابراین می توان گفت هر بسته با عبور از هر روتر یکبار از لایه ی شبکه عبور کرده است. در کل همانطور که در شکل زیر مشخص است در **مجموع ۴ بار** از لایه ی شبکه عبور می کند.



ب- یکی از فیلدهای هدر بسته های IP، TTL می باشد. کدام یک از گزینه های زیر بهترین توصیف را از نیاز به این field ارائه می دهد؟ (علت انتخاب خود را مختصر توضیح دهید)

a. برای اولویت بندی بسته ها
b. برای کاهش تاخیر
c. برای بهبود برون دهی
d. برای جلوگیری از ایجاد حلقه در فرآیند ارسال (packet looping)

پاسخ صحیح گزینه ی d می باشد. با کمک TTL می توان کران بالایی برای تعداد دفعاتی که بسته از گره ها گذر می کند تعیین کرد و از ایجاد حلقه جلوگیری کرد.

ج- هنگام ارسال یک بسته ی IP، از Host A به Host B با فرض آنکه خطایی رخ نداده است، احتمال تغییر هر یک از فیلد های زیر را برای بسته ی مذکور بررسی کنید.

a. TTL در هر hop یک واحد از مقدار TTL کم می شود.
b. Checksum مقدار checksum در هر گره مجدد محاسبه می شود و به دلیل تغییر TTL، تغییر می کند.
c. Fragment offset اگر در یک لینک ارتباطی اندازه ی بسته از MTU آن واسط بزرگ تر باشد، fragmentation اتفاق می افتد بنابراین ممکن است مقدار fragment offset هم تغییر کند.

د- جدول زیر یک forwarding table برای یک IP router نشان می دهد (برای سادگی آدرس ها 8 بیتی در نظر گرفته شده اند).

اگر بسته ای با آدرس مقصد 0101 0011 به ورودی روتر برسد، به کدام خروجی فرستاده می شود و آدرس Hop بعدی که آن را دریافت می کند کدام خواهد بود؟

| prefix | next hop | |
|---|---|---|
| | output | address |
| 101* | 2 | 1010 1111 |
| 0100* | 4 | 0100 0110 |
| 0010 0* | 6 | - |
| 1010 1* | 7 | - |
| 0101 0* | 5 | 0101 0011 |
| 1011 00* | 3 | 1011 0000 |
| 0101 11* | 1 | 0101 1100 |
| 0010 01* | 9 | - |

5, 0101 0011 زیرا آدرس ورودی بیشترین match را با سطر پنجم دارد.

۴. الف- وظایف اصلی لایه ی شبکه را شرح دهید.

Forwarding (هدایت): زمانی که بسته وارد یک روتر می شود، باید آن را به سمت پورت خروجی مناسب هدایت کند.

Routing (مسیریابی): لایه ی شبکه باید مسیری که هر بسته از مبدا تا مقصد طی می کند را مشخص کند که این کار یا به صورت static در جداول مسیریابی میسر می شود یا با کمک الگوریتم های مسیریابی.

ب- روش های انتقال بسته بین روتر ها را نام ببرید.

۱- روش سنتی (*traditional routing algorithms*)

۲- روش SDN (*software-defined networking*)

ج- روش های قسمت ب را با یکدیگر مقایسه کنید.

الگوریتم های مسیریابی در روش اول در روتر ها و در روش دوم در سرور های مرکزی و دورتر از شبکه (cloud) پیاده سازی می شود.

در روش اول تک تک روتر ها با control plane تعامل دارند در حالی که در روش دوم یک کنترلر remote با گره های محلی در ارتباط است.

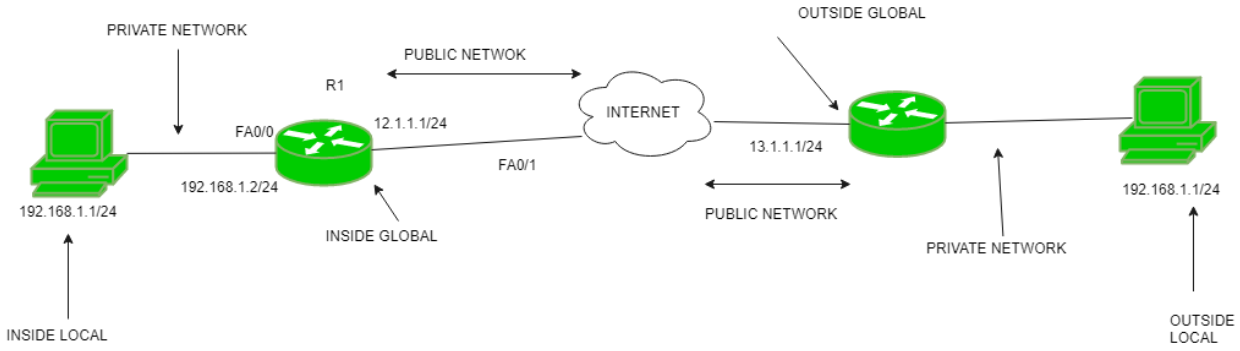
در روش سنتی، مسیریابی فقط بر مبنای آدرس مقصد انجام می شود و اگر دو مسیر با longest prefix matching معرفی شود نهایتا مسیری که هزینه ی کمتری دارد انتخاب می شود، در حالی که در SDN علاوه بر آدرس، فیلتر هایی در لایه ی network، data link و transport پردازش و انتخاب مسیر را بر عهده دارند.

در روش سنتی فقط عمل forwarding انجام می شود، در مقابل سرور ها توانایی Block کردن بسته، load balancing، تغییر اطلاعات بسته های NAT و ... را دارند.

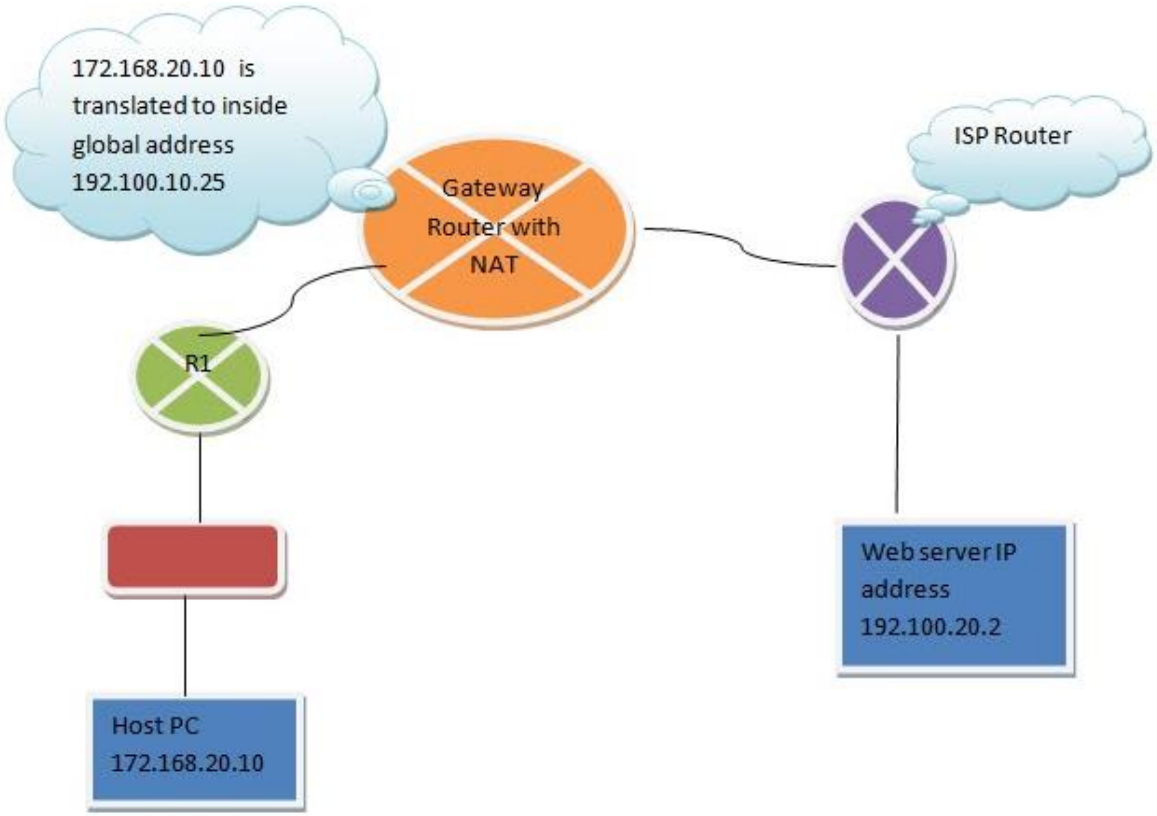
۵. با توجه به شکل الف ابتدا توضیحی از مفاهیم زیر ارائه دهید سپس سناریو شکل ب را شرح دهید.

الف.

- Inside local address آدرس IP که به یک host در شبکه ی محلی آن اختصاص داده شده است (آدرس خصوصی) و از خارج شبکه ی محلی قابل مشاهده نیست. این آدرس توسط ISP ها تعیین نمی شود.
- Inside global address آدرس IP که یک تا تعداد بیشتری Inside local address را به شبکه ی خارجی معرفی می کند.
- Outside local address آدرس IP واقعی host مقصد در شبکه ی محلی بعد از ترجمه می باشد.
- Outside global address آدرس IP مقصد قبل از ترجمه و بیرون از شبکه ی محلی مقصد می باشد.




ب. با توجه به شکل زیر، برقراری ارتباط بین PC و web server را در شبکه ای که NAT فعال است، توضیح دهید.




در این مثال، host 172.168.20.10 قصد دارد با دنیای بیرونی و web server 192.100.20.2 ارتباط برقرار کند.
برای این منظور بسته ای را به gateway router می فرستد که قابلیت ترجمه ی آدرس های NAT را دارد.
gateway router تمام دستگاه هایی که برای آدرس های پنهان (NAT) احراز شده اند را نگه می دارد، بنابراین بعد از شناسایی آدرس مبدا بسته ها در پورت ورودی بررسی می کند آیا شرایط ترجمه را دارند یا خیر. اگر شرایط برقرار بود Inside local address را به inside global IP address (که در اینجا برابر است با 192.100.10.25) ترجمه می کند سپس آن را در جدول NAT ذخیره کرده و به مقصد می فرستد.

بعد از اینکه web server پاسخ این درخواست را می دهد، آدرس مجددا به global IP address 192.100.10.25 بر می گردد و در gateway router به local IP address 172.168.20.10 ترجمه می شود و اگر با آدرس های جدول NAT تطبیق نخورد از بسته صرف نظر می شود.

۶. شکل زیر شبکه ای با سه روتر را نشان می دهد که به کمک سوئیچ های اترنت به هم متصل شده اند (6ضلعی ها روتر هستند). Forwarding table برای روتر سمت چپ نشان داده شده است.

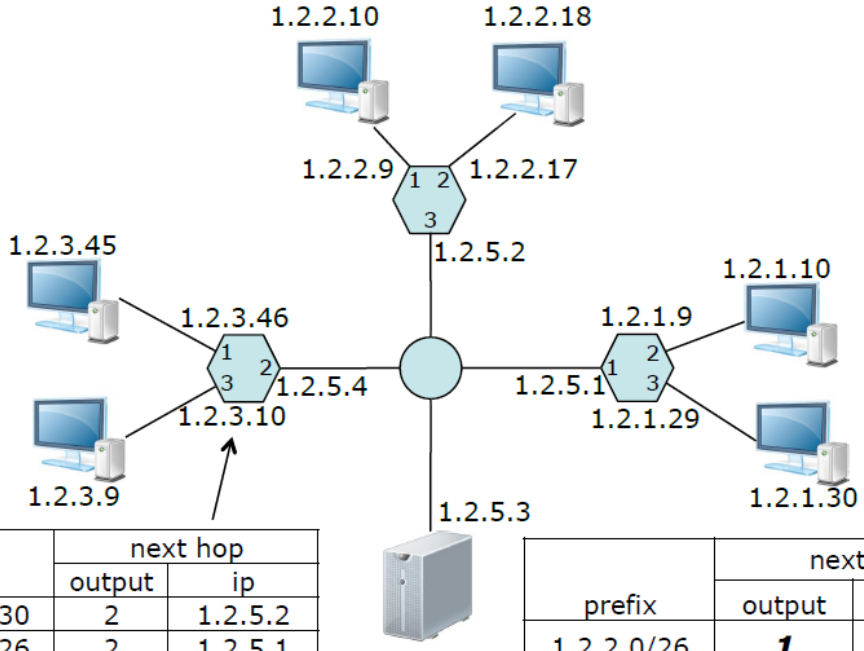
الف. Forwarding table روتر سمت راست را به گونه ای پر کنید که بسته ها به شیوه مناسبی ارسال شوند.

ب. توضیح دهید آیا همه‌ی ورودی های روتر سمت چپ ضروری هستند؟ اگر نه توضیح دهید چگونه ورودی ها را تغییر دهیم بدون اینکه تغییری در مسیر ها ایجاد شود؟

خیر، دو ورودی 1.2.2.8/30 و 1.2.2.16/30 می توانند با یک ورودی جایگزین شوند که 1.2.2.0/27 را به مقصد 2:1.2.5.2 نگاشت می کند.

ج. فرض کنید می خواهیم تغییراتی در روتر سمت چپ اعمال کنیم. به این صورت که پورت 1 را به یک سوئیچ وصل کرده و 10 میزبان تازه به شبکه بیافزاییم (host فعلی به جای اتصال به روتر به سوئیچ متصل می شود). در نتیجه این تغییرات کدام ورودی های جدول نیاز به تغییر دارد؟ ورودی های جدید را تعیین کنید.

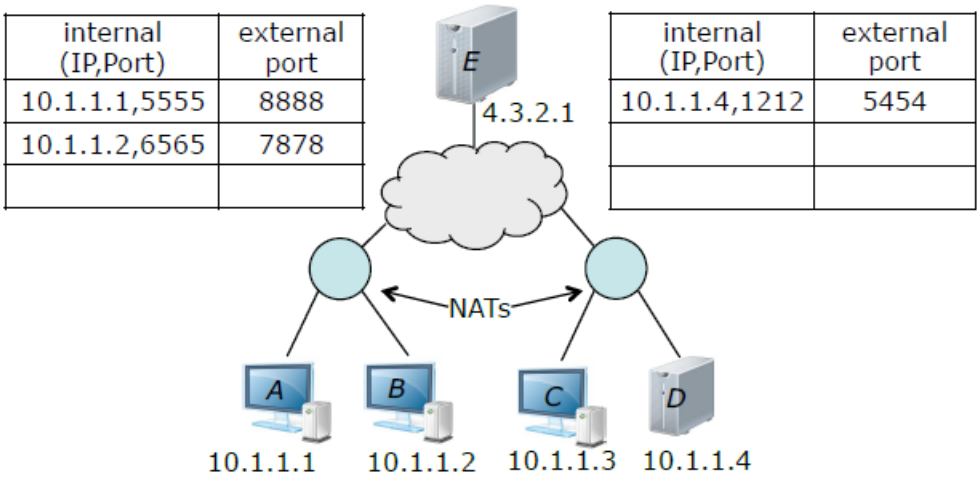
در حال حاضر پورت 1 روتر سمت چپ 30/ را ساپورت می کند یعنی قابلیت نگاشت به 4 میزبان را دارد. با این تغییرات حداقل نیاز به 12 IP address دارد. در این صورت subnet ما باید 28/ تغییر کند تا این تعداد را ساپورت کند. بنابراین مسیر با پیشوند 1.2.3.44/30 باید به 1.2.3.32/28 تغییر می کند.




| prefix | next hop | |
|---|---|---|
| | output | ip |
| 1.2.2.8/30 | 2 | 1.2.5.2 |
| 1.2.1.0/26 | 2 | 1.2.5.1 |
| 1.2.5.0/24 | 2 | - |
| 1.2.2.16/30 | 2 | 1.2.5.2 |
| 1.2.3.44/30 | 1 | - |
| 1.2.3.8/30 | 3 | - |

| prefix | next hop | |
|---|---|---|
| | output | ip |
| 1.2.2.0/26 | ***1*** | ***1.2.5.2*** |
| 1.2.3.0/26 | ***1*** | ***1.2.5.4*** |
| 1.2.5.0/24 | ***1*** | **-** |
| 1.2.1.28/30 | ***3*** | **-** |
| 1.2.1.8/30 | ***2*** | **-** |

۷. شکل زیر دو شبکه ی خانگی ، روتر هایی که NAT را پیاده سازی می کنند و یک سرور ریموت با آدرس عمومی (public internet address) را نشان می دهد .




الف. شکل زیر هدر بسته ای را نشان می دهد که از شبکه ی سمت چپ به سمت سرور ارسال می شود. هدر بالایی، مربوط به زمانی است که بسته وارد روتر می شود و هدر پایینی مربوط به زمانی است که بسته از روتر خارج می شود. ورودی های جدول NAT روتر سمت چپ را به گونه ای پر کنید که با هدر بسته های زیر هم خوانی داشته باشد. آدرس IP عمومی روتر سمت چپ چیست؟ *3.7.5.7*

| src adr | dest adr | src port | dest port |
|---|---|---|---|
| 10.1.1.1 | 4.3.2.1 | 5555 | 3333 |
| 3.7.5.7 | 4.3.2.1 | 8888 | 3333 |

ب. سه هدر زیر مربوط به بسته ایست که از شبکه ی سمت راست به شبکه ی سمت چپ ارسال می شود. ابتدا هدر ها را کامل کنید، سپس ورودی های هر دو جدول NAT را به گونه ای کامل کنید که با هدر بسته های زیر هم خوانی داشته باشد. آدرس IP عمومی روتر سمت راست چیست؟ *5.3.5.2*

| src adr | dest adr | src port | dest port |
|---|---|---|---|
| 10.1.1.4 | 3.7.5.7 | 1212 | 7878 |
| 5.3.5.2 | 3.7.5.7 | 5454 | 7878 |
| 5.3.5.2 | 10.1.1.2 | 5454 | 6565 |

ج. فیلد های هدر بسته ای که به عنوان پاسخ از شبکه ی سمت چپ به شبکه ی سمت راست ارسال شده است را کامل کنید.

| src adr | dest adr | src port | dest port |
|---|---|---|---|
| 10.1.1.2 | 5.3.5.2 | 6565 | 5454 |
| 3.7.5.7 | 5.3.5.2 | 7878 | 5454 |
| 3.7.5.7 | 10.1.1.4 | 7878 | 1212 |

۸. فرض کنید دو بسته همزمان به دو پورت ورودی متفاوت از یک روتر برسند و بسته ی دیگری درون روتر نیست.

أ) فرض کنید که این دو بسته به دو پورت خروجی متفاوت ارسال میشوند، آیا میتوان دو بسته را به صورت همزمان از راه switch fabric که از shared-bus بهره میبرد، ارسال کرد؟

نه, در هر لحظه فقط میتوان یک بسته را از راه shared-bus منتقل کرد.

ب) فرض کنید که این دو بسته به دو پورت خروجی متفاوت ارسال میشوند، آیا میتوان دو بسته را به صورت همزمان از راه switch fabric که از crossbar بهره میبرد، ارسال کرد؟

بله تا زمانی که دو بسته از bus ورودی و خروجی متفاوتی استفاده کنند, میتوانند به صورت موازی فرستاده شوند.

پ) فرض کنید که این دو بسته به دو پورت خروجی یکسانارسال میشوند، آیا میتوان دو بسته را به صورت همزمان از راه switch fabric که از crossbar بهره میبرد، ارسال کرد؟

نه, فرستادن دو بسته با bus خروجی یکسان به صورت همزمان امکان پذیر نیست.

۹. آ) همانجور که در درس فراگرفتید پروتکل IPV6 عملیات fragmentation را تنها در مبدا انجام میدهد. تحقیق کنید که کوچک ترین MTU مسیر را چگونه شناسایی میکند و در صورتی که fragmentation انجام شود, مقصد چگونه از آن آگاه خواهد شد.

در این حالت هاست مبدا تلاش می‌کند در یک فرآیند MTU discovery مینیمم MTU را بدست آورد. هاست مبدا یک بسته با اندازه مشخص و با آپشن don't fragment می‌فرستد .در صورتی که یک پیغام ICMPv6 با محتوای Too big دریافت کند باید سایز بسته را کاهش دهد تا جایی که بسته به مقصد برسد در این حالت کمترین مقدار MTU بدست می‌آید.

ب) سه مورد از بخش هایی که در سرآیند IPV4 بودند اما در IPV6 نیستند را نام برده و درباره هرکدام توضیح دهید.

- Fragmentation/reassembly

برای فرستادن بسته بر روی لینک‌های مختلف بدلیل وجود MTU های متفاوت گاهی مجبور به قطعه کردن بسته بودیم اما در ورژن ۶ این قطعه بندی تنها در مبدا انجام می‌شود.

- Header checksum

به دلیل پیشرفت تجهیزات فرض شده است که خطایی در ارسال بسته‌های IP صورت نمی‌گیرد و در صورت خطا نیز می‌توان دیتاگرام را دوباره ارسال کرد.

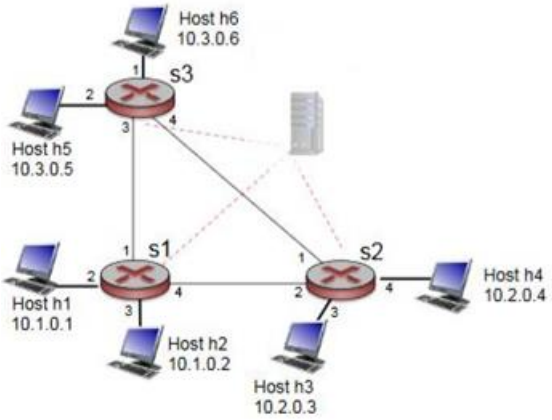
- Options

این بخش شامل موارد اضافی است که در نسخه ۶ در بخش payload قرار می‌گیرد.

۱۰. شبکه SDN زیر را که از پروتکل Openflow بهره میبرد در نظر بگیرید. فرض کنید رفتار مطلوب با رسیدن دیتاگرام از میزبان های h3 و h4 به s2 به این شکل است:

- هر دیتاگرامی که از h3 با مقصد h5,h2,h1 یا h6 می‌رسد باید در جهت عقربه های ساعت درون شبکه فرستاده شود.
- هر دیتاگرامی که از h4 با مقصد h5,h2,h1 یا h6 می‌رسد باید در خلاف جهت عقربه های ساعت درون شبکه فرستاده شود.

سطر های جدول جریان s2 را که رفتار بالا برای جلورانی را پیاده سازی میکنند مشخص کنید.




| جدول جریان سوییچ ۲S | | |
|---|---|---|
| Match | | Action |
| Interface Src = 3 | IP.Dest=10.1.*.* | Forward(2) |
| Interface Src = 3 | IP.Dest=10.3.*.* | Forward(2) |
| Interface Src = 4 | IP.Dest=10.1.*.* | Forward(1) |
| Interface Src = 4 | IP.Dest=10.3.*.* | Forward(1) |