



# شبکه‌های کامپیوتری

تمرین دوم

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی شریف

نیم سال دوم ۹۹-۰۰

---

استاد:

جناب آقای دکتر جعفری

نام و نام خانوادگی:

امیرمهدی نامجو - ۹۷۱۰۷۲۱۲



# ۱ سوال اول

توجه: امکان زوم بر روی تمامی تصاویری که در متن قرار دارند وجود دارد.

۱. وضعیت درخواست‌های DNS رد و بدل شده برای فیسبوک به صورت زیر است:

184	1.848091	192.168.1.100	192.168.1.1	DNS	72 Standard query 0x1529 A facebook.com
185	1.848098	192.168.1.100	192.168.1.1	DNS	76 Standard query 0xd3ff A www.facebook.com
186	1.848099	192.168.1.100	192.168.1.1	DNS	79 Standard query 0xb0bd A static.xx.fbcdn.net
192	1.887890	192.168.1.1	192.168.1.100	DNS	88 Standard query response 0x1529 A facebook.com A 10.10.34.36
194	1.893267	192.168.1.1	192.168.1.100	DNS	92 Standard query response 0xd3ff A www.facebook.com A 10.10.34.36
195	1.893267	192.168.1.1	192.168.1.100	DNS	79 Standard query response 0xb0bd Server failure A static.xx.fbcdn.net

سه درخواست اول از کامپیوتر من به روتر رفته‌اند و سه مورد بعدی جواب‌هایی هستند که از روتر به کامپیوتر من برگشته‌اند. مشاهده می‌کنیم آدرس آی‌پی که برای فیسبوک برگشته است 10.10.34.36 است.

این آدرس آی‌پی جزو دسته آی‌پی‌های رزرو شده است که بین 10.0.0.0 تا 10.255.255.255 قرار دارد. این آدرس آی‌پی‌ها مربوط به شبکه‌های خصوصی هستند و عملاً به سایت خاصی در اینترنت نگاشت نشده‌اند. این یعنی DNS سرور، آدرسی را برای سایت Facebook برگردانده که عملاً مربوط به شبکه عمومی اینترنت نمی‌شود و یک آدرس در شبکه خصوصی است که عملاً در کامپیوتر من وجود نداشته و نتیجتاً کروم با خطای This site can't be reached و ERR\_CONNECTION\_TIMED\_OUT متوقف می‌شود.

با بررسی تنظیمات مودم متوجه شدم که DNS-Server پیش‌فرض آن به صورت 46.224.1.220 است که با IpLookup کردن آن، متوجه می‌شویم که این آی‌پی متعلق به ns5.hiweb.ir یعنی Nameserver «های‌وب» در ایران است و منطقی است که فیلترینگ روی این Nameserver داخلی اعمال شده باشد و در نتیجه DNS به آن نتیجه نامعتبری برای facebook.com که یک سایت فیلتر شده است برگرداند.

۲. وضعیت درخواست DNS برای سایت اوراکل به صورت زیر است:

262	8.178533	192.168.1.100	192.168.1.1	DNS	74 Standard query 0x35ed A www.oracle.com
263	8.219834	192.168.1.1	192.168.1.100	DNS	169 Standard query response 0x35ed A www.oracle.com CNAME ds-www.oracle.com.edgekey.net CNAME e2581.dscx.akamaiedge.net A 23.14.117.40

وضعیت خروجی برگردانده شده برای آن به صورت زیر است:

## Answers

www.oracle.com: type CNAME, class IN,

cname ds-www.oracle.com.edgekey.net

Name: www.oracle.com

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 497 (8 minutes, 17 seconds)

Data length: 31



```

CNAME: ds-www.oracle.com.edgekey.net
ds-www.oracle.com.edgekey.net: type CNAME, class IN,
  cname e2581.dscx.akamaiedge.net
Name: ds-www.oracle.com.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 451 (7 minutes, 31 seconds)
Data length: 24
CNAME: e2581.dscx.akamaiedge.net
e2581.dscx.akamaiedge.net: type A, class IN, addr 23.14.117.40
Name: e2581.dscx.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 497 (8 minutes, 17 seconds)
Data length: 4
Address: 23.14.117.40

```

جواب اول مشخص می کند که `www.oracle.com` در اصل یک Alias برای یک آدرس دیگر است.

جواب دوم مشخص می کند که آدرس مشخص شده بعدی یعنی

`ds-www.oracle.com.edgekey.net`

هم یک Alias برای آدرس دیگری است. آدرس نهایی یعنی `e2581.dscx.akamaiedge.net` به یک آدرس آی پی واقعی مپ شده است. این آدرس آی پی یعنی `23.14.117.40` مربوط به یکی از CDN های شرکت Akamai است. این CDN در ترکیه واقع شده است و براساس موقعیت مکانی من که ایران بوده، نزدیک ترین CDN تشخیص داده شده مربوط به کشور ترکیه بوده است. با این وجود در نهایت شاهد این هستیم که سایت Oracle باز نمی شود و با خطاهای `This site can't be reached` و `ERR_CONNECTION_TIMED_OUT` مواجه می شویم. این خطاها این بار به خاطر فیلترینگ نیستند بلکه به خاطر تحریم است.

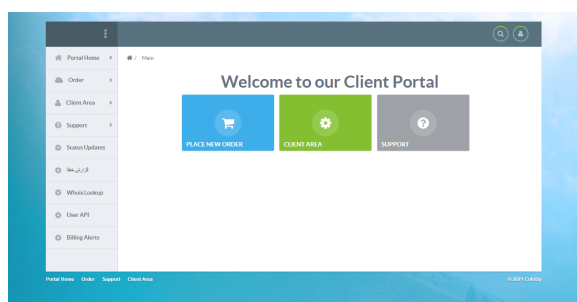
۳. پیش از بررسی نتایج باید بررسی کنیم که آی پی آدرس DNS-Server های شکن متعلق به کجاست. در سایت دو آی پی آدرس قرار گرفته است. اولین مورد `178.22.122.100` است که متعلق به شرکت آسیانک (`Asiatech Data Transmission company`) بوده و دومین آی پی `185.51.200.2` است که متعلق به شرکت مهندسی صفرویک پرداز (`Sefroyek Pardaz Engi-`) است. (`neering Co. LTD`)

با انجام تنظیمات مربوطه و وارد کردن آدرس Oracle داریم:

489 5.152691	192.168.1.100	178.22.122.100	DNS	74 Standard query 0xa2f2 A www.oracle.com
492 5.221112	192.168.1.100	185.51.200.2	DNS	74 Standard query 0xa2f2 A www.oracle.com
495 5.273204	178.22.122.100	192.168.1.100	DNS	117 Standard query response 0xa2f2 A www.oracle.com CNAME us1.shcan.ir A 162.223.88.52
500 5.276747	185.51.200.2	192.168.1.100	DNS	117 Standard query response 0xa2f2 A www.oracle.com CNAME us1.shcan.ir A 162.223.88.52
635 6.329435	192.168.1.100	178.22.122.100	DNS	79 Standard query 0x2de7 A c.oracleinfinity.io
639 6.395383	192.168.1.100	185.51.200.2	DNS	79 Standard query 0x2de7 A c.oracleinfinity.io
650 6.568923	178.22.122.100	192.168.1.100	DNS	174 Standard query response 0x2de7 A c.oracleinfinity.io CNAME c.oracleinfinity.io.edgekey.net CNAME e11123.g.akamaiedge.net A 95.101.18.83
672 6.787557	185.51.200.2	192.168.1.100	DNS	174 Standard query response 0x2de7 A c.oracleinfinity.io CNAME c.oracleinfinity.io.edgekey.net CNAME e11123.g.akamaiedge.net A 92.123.210.100
755 7.048241	192.168.1.100	178.22.122.100	DNS	73 Standard query 0x7ff6 A go.oracle.com
763 7.087485	178.22.122.100	192.168.1.100	DNS	116 Standard query response 0x7ff6 A go.oracle.com CNAME us1.shcan.ir A 162.223.88.52



همان طور که در تصویر مشخص است در نتیجه درخواست آدرس [www.oracle.com](http://www.oracle.com) خروجی به این صورت بوده که این آدرس Alias ای برای آدرس [us1.shecan.ir](http://us1.shecan.ir) است و آدرس آی پی 162.223.88.52 گزارش شده است. این آدرس آی پی در آمریکا قرار داشته و متعلق به شرکتی به اسم ColoUp است. با مراجعه به سایت این شرکت می توان مشاهده کرد که این شرکت مرتبط به خدمات شبکه است و البته بخش گزارش خطا به زبان فارسی هم دارد در نتیجه می توان به این نتیجه رسید که با شکن در ارتباط است.



خروجی برگردانده شده به صورت زیر است:

#### Answers

[www.oracle.com](http://www.oracle.com): type CNAME, class IN, cname [us1.shecan.ir](http://us1.shecan.ir)

Name: [www.oracle.com](http://www.oracle.com)

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 118 (1 minute, 58 seconds)

Data length: 15

CNAME: [us1.shecan.ir](http://us1.shecan.ir)

[us1.shecan.ir](http://us1.shecan.ir): type A, class IN, addr 162.223.88.52

Name: [us1.shecan.ir](http://us1.shecan.ir)

Type: A (Host Address) (1)

Class: IN (0x0001)

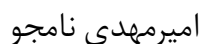
Time to live: 214 (3 minutes, 34 seconds)

Data length: 4

Address: 162.223.88.52

سایر موارد مربوط به Oracle که مشاهده می شود، مربوط به CDN ها و موارد متفرقه دیگری هستند که تحریم نبوده و همان IP اصلی آن ها برگردانده شده است. البته [go.oracle.com](http://go.oracle.com) هم تحریم است و برای آن هم آدرس مربوط به [us1.shecan.ir](http://us1.shecan.ir) برگردانده شده است.

بدین ترتیب به نظر می رسد که درخواست هایی که ما برای سایت Oracle می فرستیم به جای این که مستقیماً به سایت Oracle برود، به سایت واسطه ای که آدرس آن [us1.shecan.ir](http://us1.shecan.ir) است می رود و سپس از طریق این سایت به Oracle منتقل شده و جواب ها هم از طریق همین سایت با آی پی 162.223.88.52 برای ما بر می گردد:



## تمرین دوم

[illegible]

در مورد مواردی که تحریم نیستند، آدرس ای پی تغییری نمی کند و در این زمینه شکن تغییری در روند کار ایجاد نکرده و مانند یک DNS-Server معمولی عمل می کند.

نتایج، که برای فیسبوک بر می گردد به صورت زیر است:

IP	Host	Time	Size	Source
55.2.20.2015	192.168.1.100	176.122.122.100	0x5	74 Standard query Redis 5 www.google.com
56.2.20.2015	176.122.122.100	192.168.1.100	0x5	89 Standard query request Redis 5 www.google.com 142.250.103.18
57.2.20.2015	176.122.122.100	176.122.122.100	0x5	76 Standard query Redis 6 Facebook.com
57.2.20.2030	192.168.1.100	176.122.122.100	0x5	75 Standard query Redis 3 www.facebook.com
58.2.20.2015	176.122.122.100	176.122.122.100	0x5	76 Standard query Redis 4 www.facebook.com
58.2.20.2030	176.122.122.100	192.168.1.100	0x5	88 Standard query request Redis 4 Facebook.com 157.140.240.10
60.2.20.2015	176.122.122.100	192.168.1.100	0x5	126 Standard query request Redis 7 www.facebook.com 176.146.141.128 Facebook.com 8 16 375.268.28

آی‌پی‌هایی که با آدرس‌های 69.171.250.35 و 157.240.194.35 برگردانده می‌شوند، هر دو واقعا متعلق به فیسبوک هستند. اما با این حال اگر پکت‌های TCP جا به جا شده به این IP را مشاهده کنیم وضعیت زیر را می‌بینیم:

[illegible]

مشاهده می‌شود که اکثر موارد به رنگ سیاه یا قرمز هستند. سیاه با حروف قرمز به معنی BAD TCP و قرمز با حروف زرد به معنی TCP RST است. تقریباً هیچ کدام از پکت‌های ارسالی ما به درستی به فیسبوک منتقل نشده‌اند. این بدین معنی است که فیلترینگ اعمال شده برای فیسبوک تنها در لایه DNS نیست. بلکه فیلترینگ‌های دیگری هم اعمال شده است که پکت‌ها را بعد از رسیدن به ISP‌های داخلی، با توجه به آدرس آن که مربوط به فیسبوک است و جزو سایت‌های فیلتر شده است، Drop می‌کند تا به فیسبوک نرسند.

در این مورد Shecan هم نقش خاصی ایفا نکرده و صرفاً آدرس واقعی سایت [www.facebook.com/us1.shecan.ir](http://www.facebook.com/us1.shecan.ir) را به ما برگردانده است و از آن جایی که جزو سایت‌های تحریمی هم نیست، آدرس سرورهای

۴. خیر همان طور که در بالا توضیح داده شد، روش کار شکن بدین صورت است که لیستی از سایت‌های تحریم شده دارد و برای آن سایت‌ها، آی‌پی مربوط به سرورهای خود شکن را که در کشور دیگری مستقر هستند به ما بر می‌گرداند. بدین ترتیب، ریکوئست‌های ما به آن سایت از طریق سرورهای شکن که به نوعی نقش Man in the Middle را ایفا کرده است به آن سایت منتقل شده و جواب‌ها از طریق این سرور شکن به ما می‌رسد.

در مورد سایت‌های فیلتر شده، شکن یا عملکردی مانند DNS های ISP ها داشته و IP نامعتبری بر می‌گرداند و یا این که نهایتاً IP واقعی آن سایت را به ما می‌دهد. حتی با وجود این IP واقعی هم امکان دسترسی به سایت ممکن نیست چون درخواست ما در راه به سرورهای ISP ها



می‌رسد و در آن جا با توجه به این که مقصد آن جزو Blacklist سایت‌های فیلتر شده است، اجازه انتقال به آن داده نمی‌شود و Drop می‌شود. فیلترینگ سایتی نظیر فیسبوک صرفاً در لایه DNS اعمال نشده، بلکه در لایه‌های دیگر هم اعمال شده است که اجازه انتقال بسته‌های درخواستی ما داده نشود تا حتی با داشتن آی‌پی سایت هم نتوان به آن دسترسی پیدا کرد.

۵. در قسمت قبلی هم یکی از IP های facebook نوشته شد. آی‌پی دیگری که با متصل بودن VPN فرانسه بدست آمد، 179.60.195.36 بود که واقعا IP ثبت شده شرکت Facebook بوده و موقعیت جغرافیایی آن هم در بلژیک است که همسایه فرانسه است. در صورت وصل بودن VPN، اطلاعات از طریق پروتکل ESP به سرورهای VPN ارسال شده و از طریق آن اطلاعات مربوط به فیسبوک دریافت می‌شود و سایت بدون مشکل باز می‌شود. با این حال در صورت قطع VPN و تلاش برای دسترسی به این آی‌پی وضعیت بسته‌ها مشابه زیر خواهد بود:

1180	181.993004	192.168.1.100	179.60.195.36	TCP	55 [TCP keep-alive] 61474 → 80 [ACK] Seq=61474 Win=11280 Len=0
1184	181.993061	192.168.1.100	179.60.195.36	TCP	55 [TCP keep-alive] 61475 → 80 [ACK] Seq=61475 Win=11280 Len=0
1188	181.993062	179.60.195.36	192.168.1.100	TCP	80 [TCP keep-alive ACK] 80 → 61474 [ACK] Seq=61474 Win=0 Len=0
1182	181.993062	179.60.195.36	192.168.1.100	TCP	80 [TCP keep-alive ACK] 80 → 61475 [ACK] Seq=61475 Win=0 Len=0
1211	181.780562	179.60.195.36	192.168.1.100	TCP	80 80 → 61474 [FIN, ACK] Seq=61474 Win=0 Len=0
1212	181.780568	192.168.1.100	179.60.195.36	TCP	54 61474 → 80 [ACK] Seq=61474 Win=11280 Len=0
1213	181.712373	179.60.195.36	192.168.1.100	TCP	80 80 → 61475 [FIN, ACK] Seq=61475 Win=0 Len=0
1214	181.712374	192.168.1.100	179.60.195.36	TCP	54 61475 → 80 [ACK] Seq=61475 Win=11280 Len=0
1215	225.134135	192.168.1.100	179.60.195.36	TCP	54 61475 → 80 [FIN, ACK] Seq=61475 Win=11280 Len=0
1216	225.134134	192.168.1.100	179.60.195.36	TCP	54 61474 → 80 [FIN, ACK] Seq=61474 Win=11280 Len=0
1219	225.061119	179.60.195.36	192.168.1.100	TCP	80 80 → 61475 [RST] Seq=61475 Win=0 Len=0
1218	225.061120	179.60.195.36	192.168.1.100	TCP	80 80 → 61474 [RST] Seq=61474 Win=0 Len=0

در ابتدا تعدادی بسته اولیه رد و بدل شده اما نتیجه نهایی به TCP RST ختم شده است و همچنین با بررسی محتویات پیام‌های TCP آمده متوجه می‌شویم که همگی آن‌ها بسیار کوتاه هستند و اطلاعات کافی سایت را در بر ندارند.

```

0000  40 8d 5c 17 fe f2 98 48 27 22 a5 b8 08 00 45 00  @.....H'....E.
0010  00 28 00 00 40 00 4d 06 f5 62 b3 3c c 24 c0 a8  -(.@M- b-<$-
0020  01 64 00 50 f0 22 4b bd aa 44 00 00 00 50 04  -dP"K- D...P-
0030  00 00 90 fe 00 00 95 04 69 3e 47 5f          .....i>G_

```

دلیل این موضوع هم این است که عملاً فیلترینگ برای این سایت‌ها صرفاً از لایه DNS نیست. بلکه به نوشته ویکی‌پدیا تکنولوژی Deep Packet Inspecting در بخش فیلترینگ به کار رفته که جزئیات بسته‌های رد و بدل شده را بررسی می‌کند. بدین ترتیب مواردی نظیر آدرس مبدا یا مقصد و همچنین محتویات و کلمات استفاده شده در متن پیام در صورت رمزنگاری نشدن آن می‌تواند باعث بشود که Packet مورد نظر به عنوان محتوای فیلتر شده شناسایی شده و بعد از رسیدن به ISP ها Drop شود و در مواردی نظیر بالا تنها شامل رسیدن بسته‌هایی با محتوای بسیار کم هستیم.

علاوه بر این نکته مهم دیگری هم وجود دارد و آن هم بررسی بسته http ارسال شده است. با بررسی این بسته‌ها به مورد زیر می‌رسیم:

```

18 1.742480 192.168.1.100 179.60.195.36 HTTP 400 GET / HTTP/1.1
20 1.912977 179.60.195.36 192.168.1.100 HTTP 402 HTTP/1.1 301 Moved Permanently

```

پاسخ دریافت شده برای درخواست GET از این آدرس، کد 301 Moved Permanently است.

Hypertext Transfer Protocol  
 HTTP/1.1 301 Moved Permanently\r\n  
 Location: http://www.facebook.com/\r\n



```
Content-Type: text/html; charset="utf-8"\r\n
Date: Fri, 30 Apr 2021 15:11:44 GMT\r\n
Alt-Svc: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600\r\n
Connection: keep-alive\r\n
Content-Length: 0\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.170568000 seconds]
[Request in frame: 19]
[Request URI: http://179.60.195.36/]
```

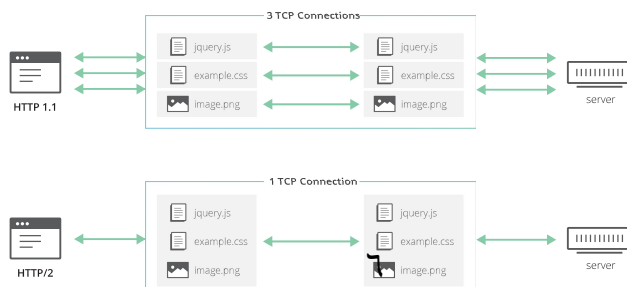
آدرس جدید این سایت facebook.com اعلام شده است. در نتیجه دوباره سیستم سعی می‌کند از طریق DNS آدرس جدید را پیدا کند ولی در این زمینه هم با فیلترینگ مربوط به DNS رو به رو می‌شود و با آدرس 10.10.34.36 روبه‌رو می‌شود که آدرس معتبری نیست.

## ۲ سوال دوم

۱. پروتکل QUIC یک پروتکل برای لایه انتقال است که توسط گوگل طراحی شده و اکنون بعد از چندین سال طی مراحل آزمایشی، توسط IETF به عنوان استاندارد جدید پذیرفته شده است. این پروتکل در مراحل اولیه توسط مروگر Chrome و برای ارتباط با بعضی از سرویس‌ها و سایت‌های گوگل استفاده می‌شد اما اکنون شاهد گسترش استفاده آن و اضافه شدن پشتیبانی از آن به مرورگرهای دیگر هم اضافه شده است.

هدف اصلی از طراحی QUIC، ایجاد پروتکلی بوده است که هم به انتقال ترافیک HTTP و HTTPS سرعت بخشیده و هم امن‌تر باشد. این پروتکل بر پایه UDP بنا شده است تا برای پیاده‌سازی آن نیاز به تغییر Middle-Box های میانی ساختار شبکه نباشد. این پروتکل سعی دارد با یکی کردن مراحل مربوط به Handshake پروتکل‌های TCP و همچنین پروتکل TLS که برای HTTPS استفاده می‌شود را در یک پروتکل یکپارچه کند و همچنین امکانات مربوط به Multiplexing در HTTP/2 را هم به شکلی بهتر برای جلوگیری از HOL Blocking پیاده‌سازی کند.

۲. در پروتکل HTTP/2 امکان Multiplexing درخواست‌ها فراهم شد. به این شکل که به جای این که چندین Connection از نوع TCP برقرار شود که هر کدام اطلاعات بخشی از صفحه را دریافت کنند، یک اتصال TCP ایجاد شده و بسته به این که هر قسمت متعلق به کدام بخش صفحه است، Multiplexing صورت گرفته و به یکی از آن‌ها تعلق می‌گیرد.





تنها ایرادی که در این زمینه وجود دارد مشکل Head of Line Blocking است. در این حالت اگر یکی از پکت‌های TCP از دست برود، باید منتظر ارسال مجدد آن بمانیم و عملاً مزایای Multiplexing از بین می‌رود و با وجود تقسیم شدن به سگمنت‌های مختلف، همگی آن‌ها معطل رسیدن بسته از دست رفته خواهند بود.

با این حال QUIC از پایه به این شکل طراحی شده است که Multiplexing را به طور کامل پشتیبانی کند. این پروتکل قسمت‌های مختلف صفحه را به Stream‌های مجزا تقسیم می‌کند. از دست رفتن داده در یک پکت خاص مربوط به یک Stream مشخص، تنها منجر به معطل شدن همان Stream شده و بقیه Stream Frame‌ها می‌توانند با موفقیت بعد از دریافت به بخش مربوطه متصل شده و معطل رسیدن بسته Stream از دست رفته نخواهند بود. در این اتصال استریم‌های مختلف HTTP می‌توانند به استریم‌های مختلف QUIC مرتبط بشوند. ضمن این که همه این استریم‌ها از یک کانکشن QUIC استفاده کرده و در نتیجه نیازی به انجام handshake‌های مجدد ندارند.

نتیجه نهایی همه این موارد این است که در اکثر اوقات، از دست رفتن یک پکت در یک استریم منجر به ایرادی یا بلاک شدن بقیه نمی‌شود و بقیه می‌توانند با موفقیت مراحل انتقال خود را انجام بدهند.

۳. اتصال QUIC را کلاینت که یکی از Endpoint‌های اتصال است برقرار می‌کند. در QUIC اطلاعات مربوط به ورژن، رمزنگاری و Handshake‌های اولیه همگی با هم صورت می‌گیرند تا تاخیری که در اثر مراحل شروع کار صورت می‌گیرد کاهش یابد.

هر کدام از پکت‌های اولیه که توسط کلاینت ارسال می‌شوند باید فلگ مربوط به ورژن را به حالت On در آورده و جزئیات ورژن مورد استفاده را در میان بگذارند. تمامی پکت‌های ارسالی کلاینت در ابتدا این فلگ را در حالت On می‌گذارند تا زمانی که یک جواب از سمت سرور با فلگ ورژن Off دریافت شود. سرور هم پس از این که اولین پکتی از کلاینت را دریافت کرد که فلگ ورژن آن Off □□□، باید پکت‌های دیگری که با فلگ On ممکن است به دلیل تاخیر دریافت شوند را نادیده بگیرد.

هنگامی که سرور یک پکت با Connection ID جدیدی را دریافت می‌کند، ورژن آن را با ورژن‌هایی که پشتیبانی می‌کند مقایسه می‌کند و اگر از آن پشتیبانی می‌کند، تا انتهای عمر این اتصال از آن استفاده می‌کند.

در صورتی که این ورژن قابل قبول نباشد، با تاخیر یک Round-Trip Time از سمت سرور یک پکت برای مذاکره در مورد ورژن به کلاینت ارسال می‌شود که در آن فلگ ورژن On بوده و لیست ورژن‌های قابل قبول در آن آمده است. کلاینت هم پس از دریافت این موضوع، یکی از آن پروتکل‌ها را انتخاب کرده و براساس آن اطلاعات را از ابتدا باز ارسال می‌کند.

برای جلوگیری از حملات Downgrading، جزئیات مربوط به ورژن که کلاینت در ابتدا مشخص کرده و ورژن‌های پشتیبانی شده توسط سرور در اطلاعات مربوط به Handshake رمزنگاری هم قرار می‌گیرند تا کلاینت با چک کردن آن‌ها بتواند از صحت این اطلاعات اطمینان حاصل کند.

در همین مراحل اطلاعات مربوط به رمزنگاری و Handshake اولیه لایه انتقال هم انجام می‌گیرد. یعنی همزمان مراحل انتقال جزئیات رمزنگاری و Handshake لازم با هم انجام می‌شود. QUIC در ورژن‌های فعلی خود از پروتکل TLS برای رمزنگاری استفاده می‌کند اما این امکان وجود دارد که در آینده امکان استفاده از پروتکل‌های دیگری هم مهیا بشود. در حین انجام عملیات





Handshake، اطلاعات سطح Application هم امکان انتقال دارند. به شکل ساده، ارتباط اولیه رمزنگاری به چنین شکلی قابل انجام است:



در همین مرحله، می‌توان اطلاعات مربوط به Explicit Congestion Notification را هم منتقل کرد که مشخص کند آیا یکی از طرفین درگیر Congestion شده است یا نه که طرف دیگر بداند باید با نرخ ارسال پایین اطلاعات را ارسال کند یا نه.

در مورد اتمام اتصال، روش به این صورت است که اتصالات بعد از این که در وضعیت Idle یا بلااستفاده قرار بگیرند، برای مدتی باز می‌ماند و پس از گذشت آن زمان، سرور اتصال را قطع می‌کند. این قطع شدن اتصال لزوماً با خبر کردن کلاینت همراه نخواهد بود چون اگر این اتصال در دستگاه‌های همراه (موبایل‌ها) برقرار شود، این کار نیازمندی فعال‌سازی دوباره اینترنت در این دستگاه‌ها بوده و منجر به مصرف برق می‌شود. در اصل به طور کلی دو نوع بسته شدن اتصال وجود دارد:

- خاموشی صریح: در این حالت یکی از Endpoint ها یک فریم CONNECTION\_CLOSE برای Endpoint دیگر ارسال می‌کند که آغازگر اتمام ارتباط است. Endpoint دیگر می‌تواند یک فریم GOAWAY ارسال کند که به معنی این است که به زودی ارتباط بسته خواهد شد. ارسال این سیگنال مشخص می‌کند که استریم‌های فعلی همچنان به کار خود ادامه می‌دهند تا به اتمام برسند ولی دیگر Stream جدیدی ایجاد نخواهد شد تا بعد از اتمام کار قبلی‌ها، کار به اتمام برسد. بعد از اتمام کار دوباره CONNECTION\_CLOSE ارسال می‌شود و اتصال به اتمام می‌رسد. اگر در حالی که هنوز استریم‌های ناتمام داریم این فریم ارسال شود، سمت دیگر باید این طور فرض کند که استریم‌ها به پایان نرسیده بودند ولی به شکل غیر منتظره بسته شدند.

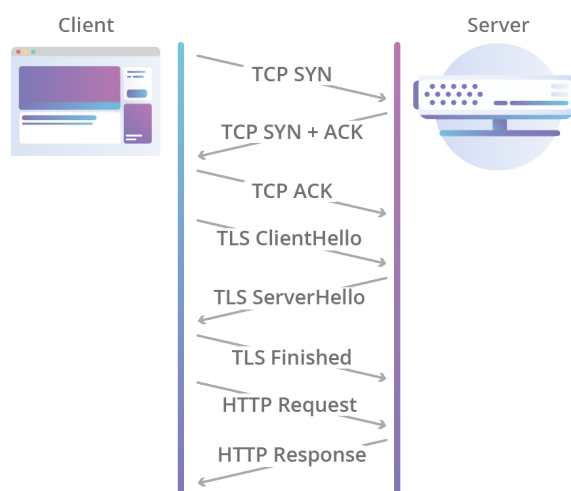
- خاموشی ضمنی: تایم‌اوت پیش‌فرض برای قرار گرفتن یک اتصال در وضعیت بلااستفاده 30 ثانیه است و در همان ابتدای ایجاد به عنوان یک پارامتر ضروری که ICSL نام دارد باید مشخص بشود. حداکثر زمانی هم که می‌توان برای این کار تعیین کرد 10 دقیقه است. اگر هیچ فعالیتی روی این اتصال به اندازه زمان مشخص شده وجود نداشته باشد، اتصال بسته می‌شود. در هنگام بسته شدن، به طور پیش‌فرض یک فریم CONNECTION\_CLOSE ارسال می‌شود ولی می‌توان ارسال آن را غیرفعال کرد تا در شبکه‌هایی که هزینه ارسال



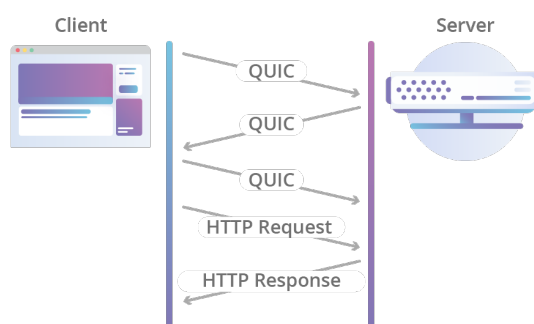
بالاست (نظیر شبکه‌های موبایل)، بدون دریافت پیام جدید در سمت دیگر، اتصال بسته بشود.

در زیر دو مقایسه بین اتصال TCP رایج به همراه رمزنگاری TLS که برای شروع نیاز به دو RTT دارد با پروتکل QUIC که با یک RTT این کار را انجام می‌دهد قرار گرفته است:

### HTTP Request Over TCP + TLS



### HTTP Request Over QUIC



۴. این قسمت براساس درفت هشتم QUIC نوشته شده است (لینک داده شده در صورت سوال درفت دوم QUIC است):

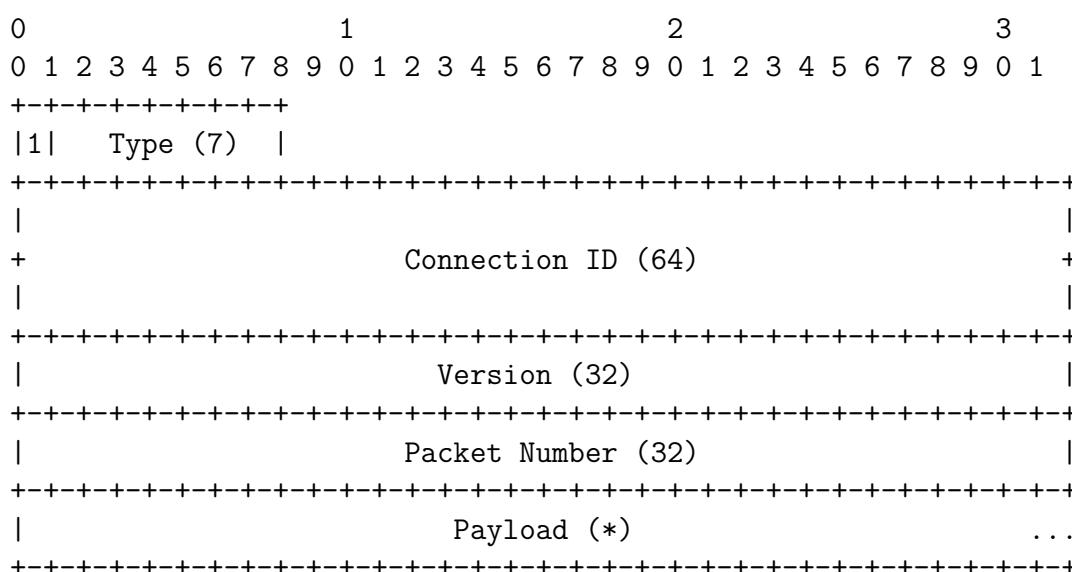
<https://tools.ietf.org/html/draft-ietf-quic-transport-08>



ابتدا باید توجه کنیم که همه داده‌های عددی به صورت Big-Endian انکود شده و ارسال می‌شوند. در نتیجه با ارزش‌ترین بیت، بیت صفرم است.

هر بسته کوئیک می‌تواند هدر بلند یا هدر کوتاه داشته باشد. هدرهای بلند معمولاً برای مشخص کردن ورژن اولیه و شروع اتصال استفاده می‌شوند. پس از آن از هدرهای کوتاه استفاده می‌شود.

هدر بلند ساختاری مانند زیر دارد:



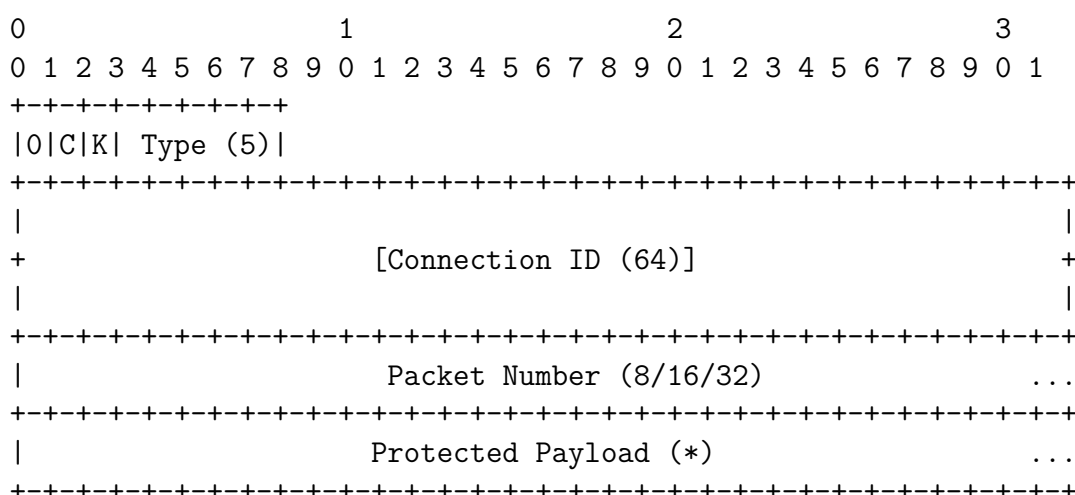
این هدرها قبل از کامل شدن فرآیند ارتباط اولیه و مشخص شدن ورژن استفاده می‌شوند. بیت اول بسته 1 است. هفت بیت بعدی بیانگر نوع بسته هستند و 128 نوع بسته مختلف می‌تواند برای این فیلد در نظر گرفته بشود اما فعلاً از همه آن‌ها استفاده نمی‌شود. بعد از آن 64 بیت برای مشخص کردن Connection ID می‌آیند که عملاً عامل تمایز اصلی بین اتصالات است. پس از آن 32 بیت برای مشخص کردن ورژن QUIC استفاده شده و مشخص می‌کند که سایر هدرها و فیلدهای پیام به چه شکل تفسیر می‌شوند. پس از آن هم Packet Number می‌آید که 32 بیتی است اما می‌تواند بیانگر عددی بین 0 تا  $2^{62} - 1$  باشد اما به شیوه خاصی تنها 32 کم ارزش آن ارسال می‌شوند. بعد از این‌ها بخش اصلی و Payload پیام قرار می‌گیرد. انواع پکت‌هایی که با حالت Long ارسال می‌شوند شامل چهار پکت هستند.

- 0x7F: Initial
- 0x7E: Retry
- 0x7D: Handshake
- 0x7C: 0-RTT Protected



نحوه تفسیر Payload و فیلدهای خاص درون آن بسته به ورژن‌های مختلف QUIC می‌تواند متفاوت باشد.

هدر کوتاه ساختاری مانند زیر دارد:



اولین بیت در این نوع هدر برابر 0 است. بیت دوم اصطلاحاً بیت Omit Connection ID Flag است و در صورتی که 0 باشد Connection ID را در ادامه هدر خواهیم داشت و در غیر این صورت، Connection ID را نخواهیم داشت. بیت بعدی Key Phase Bit است که به شناسایی کلیدهای حفاظتی که در پکت قرار دارند در سمت گیرنده کمک می‌کند. جزییات دقیق این موضوع به نحوه پیاده‌سازی سیستم رمزنگاری QUIC-TLS ربط دارد و خارج از مقوله این سوال است.

پس از این 5 بیت برای تعیین نوع بسته وجود دارد. بسته‌های کوتاه می‌توانند 32 نوع مختلف داشته باشند اما فعلاً از همه این 32 نوع استفاده نشده است.

پس از آن 64 بیت Connection ID می‌تواند وجود داشته باشد. در صورتی که فیلد Omit Connection ID Flag برابر 1 باشد این قسمت را نخواهیم داشت.

پس از آن شماره بسته ( IrPacket Number) می‌آید. بسته به نوع بسته این شماره می‌تواند 8، 16 یا 32 بیتی باشد. پس از آن هم قسمت Protected Payload قرار دارد.

براساس پیاده‌سازی‌ها، انواع پکت‌های کوتاه فعلاً شامل سه نوع (از 32 نوع ممکن) است که طول Packet Number را مشخص می‌کند.

- 0x1F: 8-bit Packet Number
- 0x1E: 16-bit Packet Number
- 0x1D: 32-bit Packet Number

با تمام این‌ها به نظر تغییراتی در این فرمتینگ در نسخه‌های جدیدتر QUIC داده شده است و خصوصاً در حالت Short شاهد اضافه شدن یکسری فلگ‌های تک‌بیتی دیگر هم هستیم.



۵. برای این مورد ابتدا باید به نحوه ارسال پکت‌ها در QUIC توجه کنیم. در ارسال بسته‌ها، هر بسته شامل Packet Number است. این شماره بسته در طول عمر یک اتصال هیچ‌وقت تکرار نشده و مقدار آن هم به شکل اکیدا صعودی افزایش می‌یابد. در نتیجه شناسایی مواردی که دو بار ارسال شده اند به راحتی امکان پذیر است.

هر بسته می‌تواند شامل چندین فریم باشد. دو فریم اصلی که برای ما اهمیت دارند، یکی فریم STREAM است که دیتای اصلی را در خود دارد و البته اطلاعات مربوط به Handshake رمزنگاری هم در آن قرار می‌گیرند. بخش دیگر فریم‌های ACK هستند. QUIC از سیستم NACK یا Negative Acknowledgment استفاده می‌کند. بدین شکل که بیش‌ترین شماره پکتی که دیده شده ارسال شده و در کنار آن، شماره پکت‌هایی که کمتر از آن هستند و دریافت نشده‌اند به عنوان بازه‌های ارسال NACK می‌شوند تا آن موارد باز ارسال بشوند. همچنین در فریم مربوط به ACK یک timestamp برای مشخص کردن زمان ارسال این پیام هم قرار دارد. همچنین QUIC امکان استفاده از 255 بازه NACK را دارد که در محیط‌هایی که امکان Loss بالاست، باعث سرعت بخشیدن به بازیابی می‌شود. همچنین مشخص کردن زمان ACK باعث می‌شود که گیرنده ACK متوجه اختلاف زمانی بین ارسال ACK و دریافت بسته اصلی بشود و ارسال بسته‌های بعدی را متناسب با آن تنظیم کند. (مثلا بررسی کند که یکسری از بسته‌ها که ACK آن‌ها دریافت نشده، احتمالا در زمان فعلی به دست گیرنده رسیده و صرفا هنوز ACK آن‌ها نرسیده است، در نتیجه فرایند را از بسته‌های بعدی ادامه بدهد)

با توجه به این مقدمه مکانیزم Loss Recovery در QUIC به این شکل است:

#### • در هنگام ارسال بسته:

- اگر Handshake به درستی صورت نگرفته باشد، یک تایمر استارت زده شده و مقدار اولیه آن 1.5 برابر SRTT بوده و کاهش نرخ ارسال آن به صورت نمایی است.
- اگر تعداد زیادی بسته NACK شده اند، احتمالا باید timer مربوط به از دست رفتن را استارت زد. مقدار پیش‌فرض آن  $0.25RTT$  است.
- اگر کمتر از 2 پکت لایه انتقال ارسال شده است، تایمر مربوط به ریستار می‌شود. اگر چندین پکت در راه ارسال باشند، مقدار آن برابر ماکسیمم  $10ms$  و  $2 \times SRTT$  خواهد بود و اگر تنها تنها یک بسته در راه باشد مقدار آن برابر  $\max(1.5 \times SRTT, 2 \times SRTT + \text{timer ack delayed})$  خواهد بود.
- اگر حداقل دو بسته لایه انتقال ارسال شده است، تایمر Retransmission Timeout را استارت می‌زنیم و مقدار آن برابر  $\max(200ms, SRTT + 4 \times RTTVAR)$  خواهد بود و بعد از اولین تایم‌اوت مجدد، مقدار آن به صورت نمایی کم خواهد شد.

#### • در هنگام دریافت ACK:

در هنگام دریافت ACK مراحل زیر طی می‌شود:

- این ACK صحت سنجی و اعتبارسنجی شده و ACK‌هایی که بدون ترتیب آمده اند و یا قبلا ACK آن‌ها دریافت شده نادیده گرفته می‌شوند.
- مقادیر مربوط به RTT دوباره محاسبه شده و آپدیت می‌شوند.
- ارسال کننده که ACK را دریافت کرده، بسته‌هایی که مقدارشان از Packent Number این ACK کمتر بوده و جزو بخش NACK نیستند را به عنوان موارد ACKED شده علامت گذاری می‌کند.



- بسته‌هایی که مقدار Packet Number آن‌ها کمتر از بیش‌تری ACK مشاهده شده بوده و در دسته NACK ها باشند، به عنوان بسته‌های گمشده علامت گذاری می‌شوند.
  - حد آستانه برای بسته‌های گمشده به طور پیش‌فرض برابر 3 است.
  - بسته‌هایی که بیش‌تر حد آستانه گفته شده گزارش گمشدن داشته باشند، برای ارسال مجدد آماده می‌شوند.
  - اگر تعداد بسته‌های NACK شده زیاد باشند و مقدار بیش‌ترین بسته دیده‌شده برابر بزرگترین بسته ارسال شده باشد، تایمر ارسال مجدد برابر  $0.25RTT$  می‌شود.
  - در صورتی که بسته‌های NACK شده خیلی قابل توجه نیستند، تایمر بخش قبل متوقف می‌شود.
- هنگام به پایان رسیدن تایمر:
- پروتکل QUIC از یک تایمر Loss Recovery استفاده می‌کند که هنگام ست شدن، می‌تواند در حالت‌های مختلفی باشد. این وضعیت عملی که باید انجام شود را مشخص می‌کند.
- در حالت Handshake
    - \* بسته‌های Handshake دوباره ارسال می‌شوند.
  - در حالت Loss
    - \* بسته‌های قابل توجهی که NACK شده‌اند به عنوان از دست رفته شده در نظر گرفته می‌شوند.
    - \* این از دست رفتن به کنترلر بخش Congestion گزارش می‌شود.
    - \* بسته به میزانی که کنترلر Congestion اجازه بدهد، بسته‌ها باز ارسال می‌شوند.
  - در حالت TLP (بسته لایه انتقال)
    - \* کوچک‌ترین بسته‌ای که به میزان قابل توجهی LOSS شده است و قابل ارسال مجدد است را ارسال می‌کنیم.
    - \* هیچ بسته‌ای را به عنوان گمشده علامت گذاری نمی‌کنیم تا ACK بعدی برسد.
    - \* تایمر را برای حالت TLP یا RTO ریستارت می‌کنیم.
  - حالت RTO: کلمه RTO به معنی Retransmission Timeout است.
    - \* دو بسته‌ای که به میزان قابل توجهی Loss برای آنان گزارش شده و سائز کمتری داشته و قابل ارسال مجدد هستند، دوباره ارسال می‌شود.
    - \* مقدار Congestion Window برابر 1 بسته شده و منتظر می‌مانیم تا Ack بعدی برسد تا مطمئن شویم که RTO ما اضافی نبوده است.
    - \* تایمر برای RTO بعدی ریست می‌شود. (با نرخ Backoff نمایی)