



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.

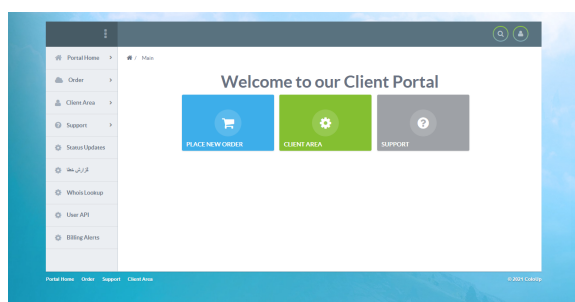
۳. پیش از بررسی نتایج باید بررسی کنیم که آی پی آدرس DNS-Server های شکن متعلق به کجاست. در سایت دو آی پی آدرس قرار گرفته است. اولین مورد `178.22.122.100` است که متعلق به شرکت آسیانک (Asiatech Data Transmission company) بوده و دومین آی پی `185.51.200.2` است که متعلق به شرکت مهندسی صفرویک پرداز (Sefroyek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

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 خروجی به این صورت بوده که این آدرس Alias ای برای آدرس 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: type CNAME, class IN, cname us1.shecan.ir

Name: 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

us1.shecan.ir: type A, class IN, addr 162.223.88.52

Name: 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 هم تحریم است و برای آن هم آدرس مربوط به 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 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:



600 0.118096	192.168.1.100	192.168.1.100	TCP	54 53088 → 443 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
610 0.118073	192.168.1.100	192.168.1.100	TCP	5378 443 → 53088 [RST] Seq=10780434940 Win=0 Len=0 [RST segment of a reassembled PDU]
612 0.118179	192.168.1.100	192.168.1.100	TCP	54 53088 → 443 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
612 0.118175	192.168.1.100	192.168.1.100	TCP	1444 Application Data [TCP segment of a reassembled PDU]
613 0.118201	192.168.1.100	192.168.1.100	TCP	54 53088 → 443 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
614 0.118248	192.168.1.100	192.168.1.100	TCP	1444 443 → 53088 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
615 0.118257	192.168.1.100	192.168.1.100	TCP	54 53088 → 443 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
616 0.118264	192.168.1.100	192.168.1.100	TCP	54 53088 → 443 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
617 0.118262	192.168.1.100	192.168.1.100	TCP	54 53088 → 443 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
618 0.118259	192.168.1.100	192.168.1.100	TCP	1444 Application Data [TCP segment of a reassembled PDU]
619 0.118242	192.168.1.100	192.168.1.100	TCP	54 53088 → 443 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
620 0.118222	192.168.1.100	192.168.1.100	TCP	1444 443 → 53088 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]
621 0.118242	192.168.1.100	192.168.1.100	TCP	54 53088 → 443 [ACK] Seq=10780434940 Win=10280 Len=0 [TCP segment of a reassembled PDU]

از آن جایی که این آی پی در آمریکا قرار دارد و درخواست‌های ما از طریق آن به Oracle منتقل می‌شود، Oracle تحریم را اعمال نکرده و اطلاعات را به سرورهای شکن فرستاده و از آن طریق پاسخ مربوطه به ما بر می‌گردد.

در مورد مواردی که تحریم نیستند، آدرس‌های آی پی تغییری نمی‌کند و در این زمینه شکن تغییری در روند کار ایجاد نکرده و مانند یک DNS-Server معمولی عمل می‌کند.

نتایجی که برای فیسبوک بر می‌گردد به صورت زیر است:

16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
16 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14

آی پی‌هایی 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:

160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14
160 0.140551	192.168.1.100	192.168.1.100	600	600 Standard query request 0 www.google.com 0 142.250.139.14

مشاهده می‌شود که اکثر موارد به رنگ سیاه یا قرمز هستند. سیاه با حروف قرمز به معنی BAD و قرمز با حروف زرد به معنی TCP RST است. تقریبا 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 صرفا آدرس واقعی سایت www.facebook.com را به ما برگردانده است و از آن جایی که جزو سایت‌های تحریمی هم نیست، آدرس سرورهای us1.shecan.ir را به ما نداده است.

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، آی پی 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 نهایتا 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/]
```

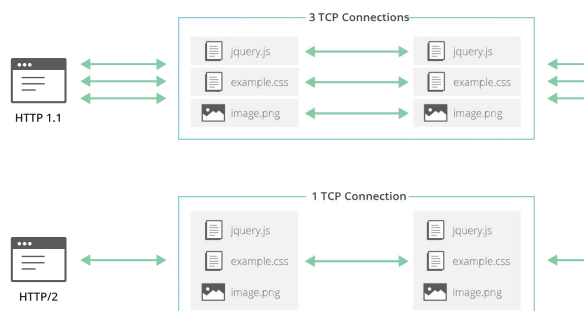
آدرس جدید این سایت facebook.com اعلام شده است. در نتیجه دوباره سیستم سعی می‌کند از طریق DNS آدرس جدید را پیدا کند ولی در این زمینه هم با فیلترینگ مربوط به DNS رو به رو می‌شود و با آدرس 10.10.34.36 روبه‌رو می‌شود که آدرس معتبری نیست.

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.