Better don’t be too QUIC(K)

Yuri Gbur

whoami

Yuri Gbur

- MSc in Computer Science at Technische Universität (TU) Berlin
- Security Consultant at SEC Consult
- Deputy Lead for Cloud Security

y.gbur@sec-consult.com

@yukonsec

yukonsec@infosec.exchange

QUIC(K) Background

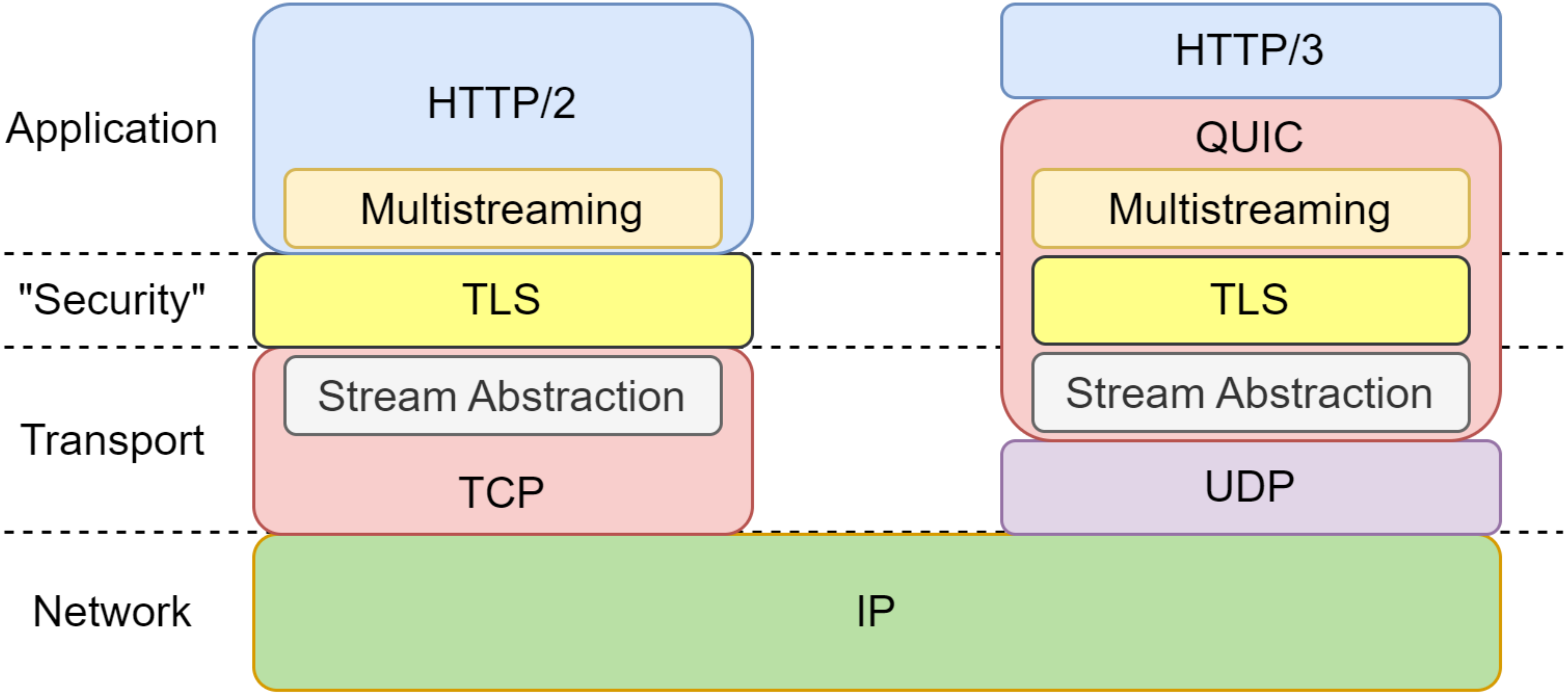
Why QUIC?

- RFC 8999
- RFC 9000
- RFC 9001
- RFC 9002

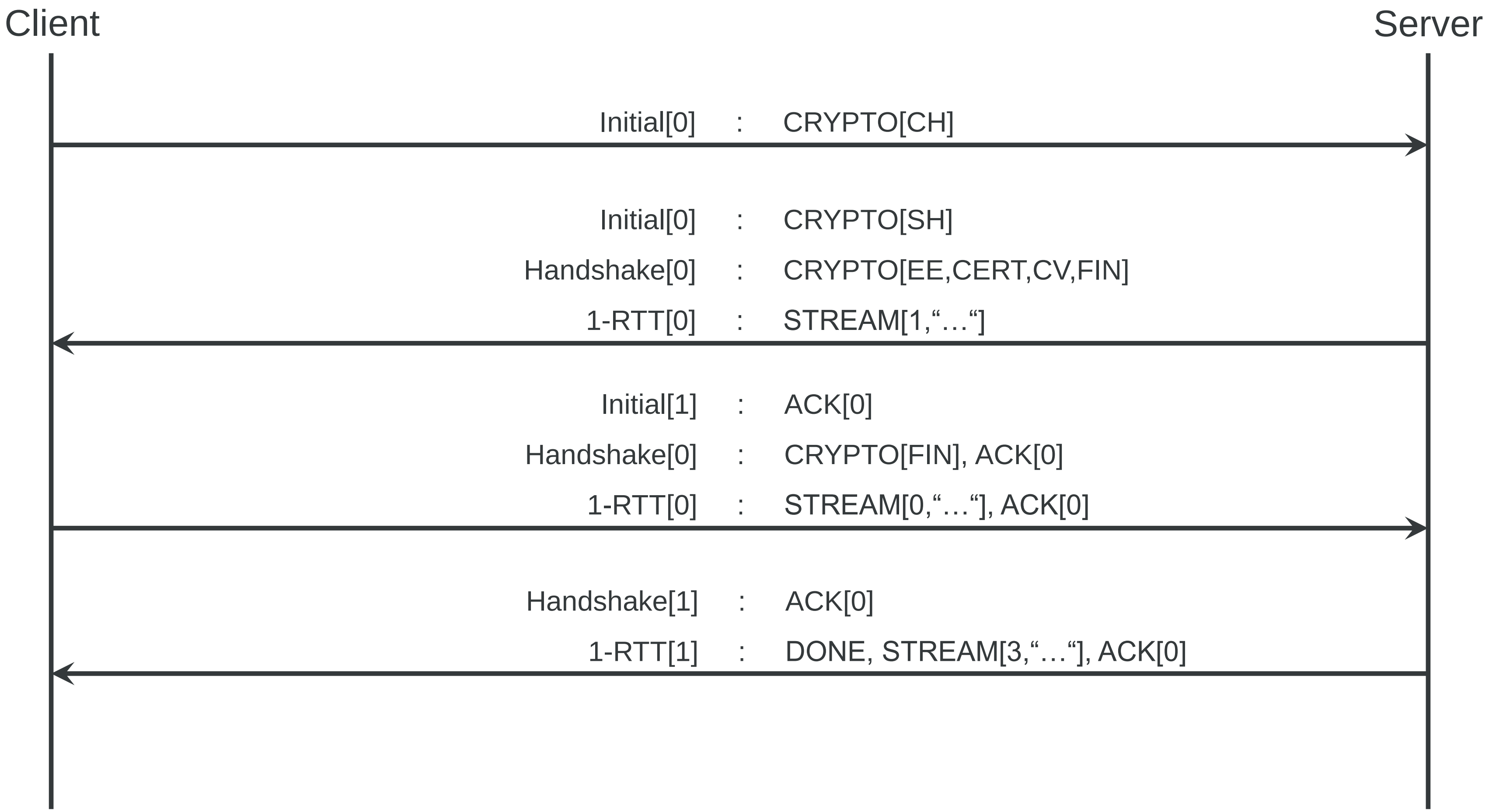
- RFC 9115 (HTTP/3)

THE APACHE SOFTWARE FOUNDATION
Google
CLOUDFLARE
moz://a
Akamai
Microsoft
LITESPEED
NGINX

HTTP/2 VS HTTP/3



QUIC Handshake



Client

Server

Initial[0] : CRYPTO[CH]

Initial[0] : CRYPTO[SH]

Handshake[0] : CRYPTO[EE,CERT,CV,FIN]

1-RTT[0] : STREAM[1,“…“]

Initial[1] : ACK[0]

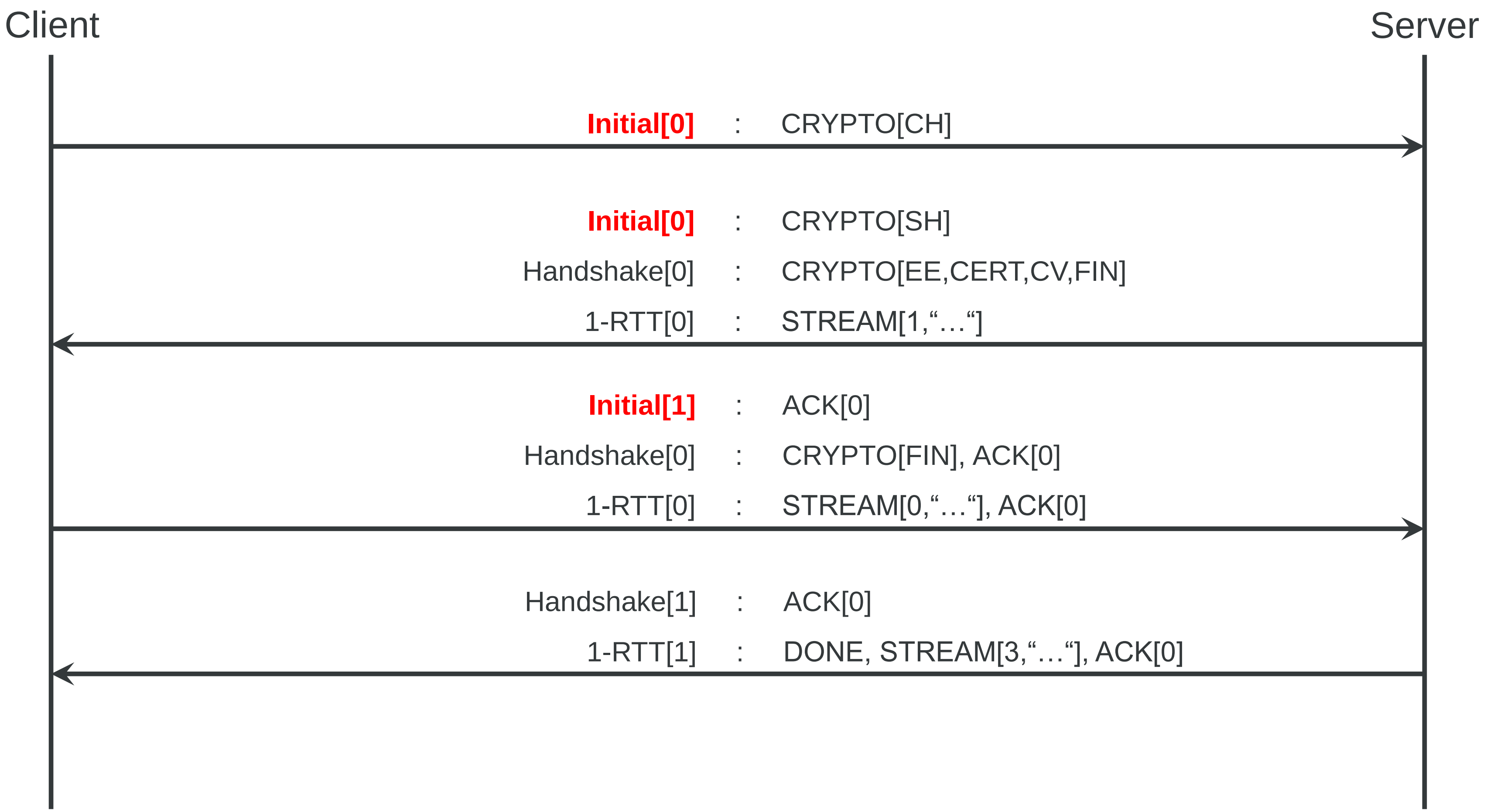
Handshake[0] : CRYPTO[FIN], ACK[0]

1-RTT[0] : STREAM[0,“…“], ACK[0]

Handshake[1] : ACK[0]

1-RTT[1] : DONE, STREAM[3,“…“], ACK[0]

QUIC Handshake



Client

Server

Initial[0] : CRYPTO[CH]

Initial[0] : CRYPTO[SH]

Handshake[0] : CRYPTO[EE,CERT,CV,FIN]

1-RTT[0] : STREAM[1,“…“]

Initial[1] : ACK[0]

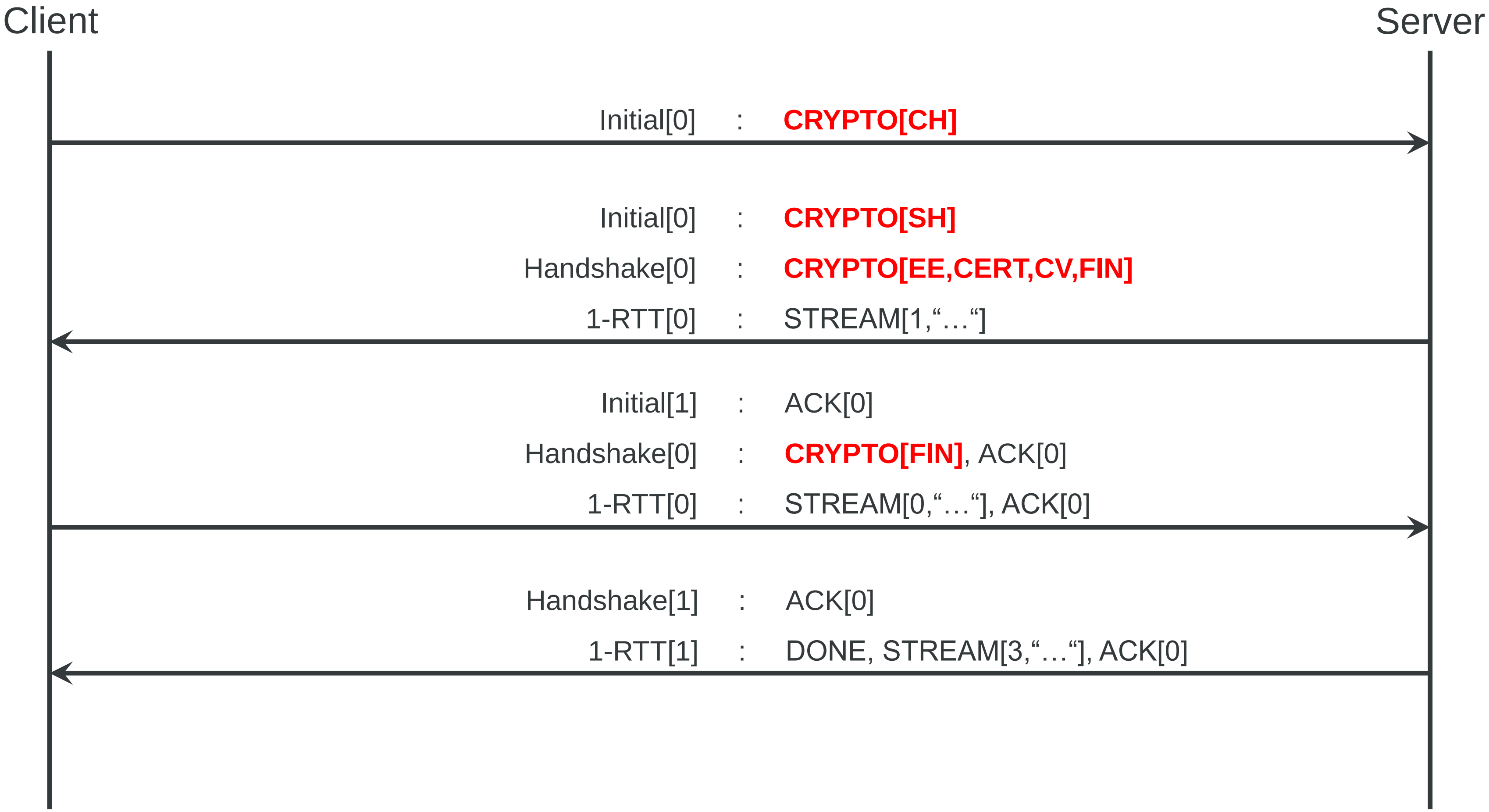
Handshake[0] : CRYPTO[FIN], ACK[0]

1-RTT[0] : STREAM[0,“…“], ACK[0]

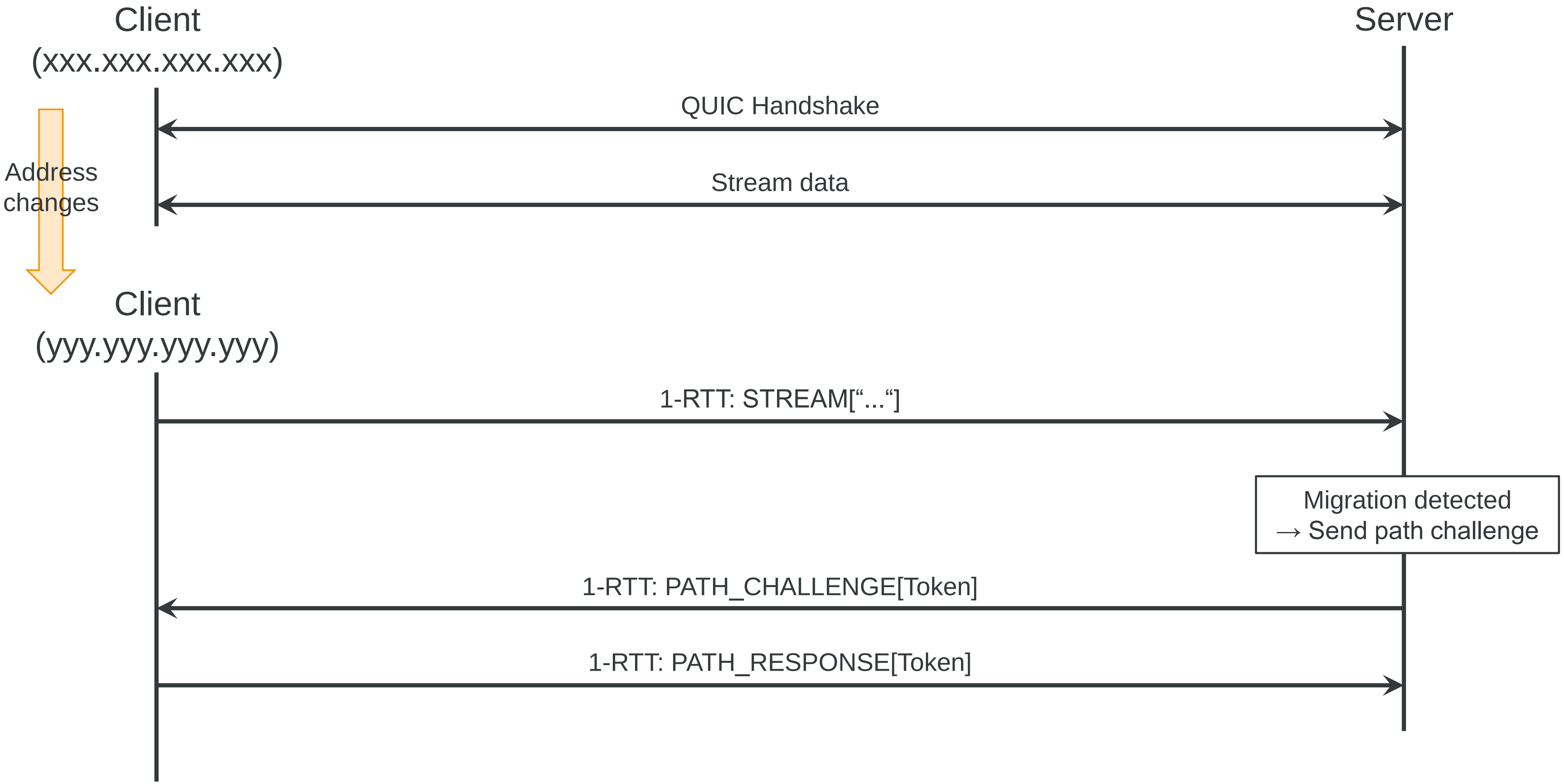
Handshake[1] : ACK[0]

1-RTT[1] : DONE, STREAM[3,“…“], ACK[0]

QUIC Handshake


Client
Server
Initial[0] : **CRYPTO[CH]**
Initial[0] : **CRYPTO[SH]**
Handshake[0] : **CRYPTO[EE,CERT,CV,FIN]**
1-RTT[0] : STREAM[1,“…“]
Initial[1] : ACK[0]
Handshake[0] : **CRYPTO[FIN]**, ACK[0]
1-RTT[0] : STREAM[0,“…“], ACK[0]
Handshake[1] : ACK[0]
1-RTT[1] : DONE, STREAM[3,“…“], ACK[0]

Connection Migration



Client
(xxx.xxx.xxx.xxx)

Server

QUIC Handshake

Stream data

Address changes

Client
(yyy.yyy.yyy.yyy)

1-RTT: STREAM[“...“]

Migration detected
→ Send path challenge

1-RTT: PATH_CHALLENGE[Token]

1-RTT: PATH_RESPONSE[Token]

Challenges with Securing QUIC

Living in the User Land

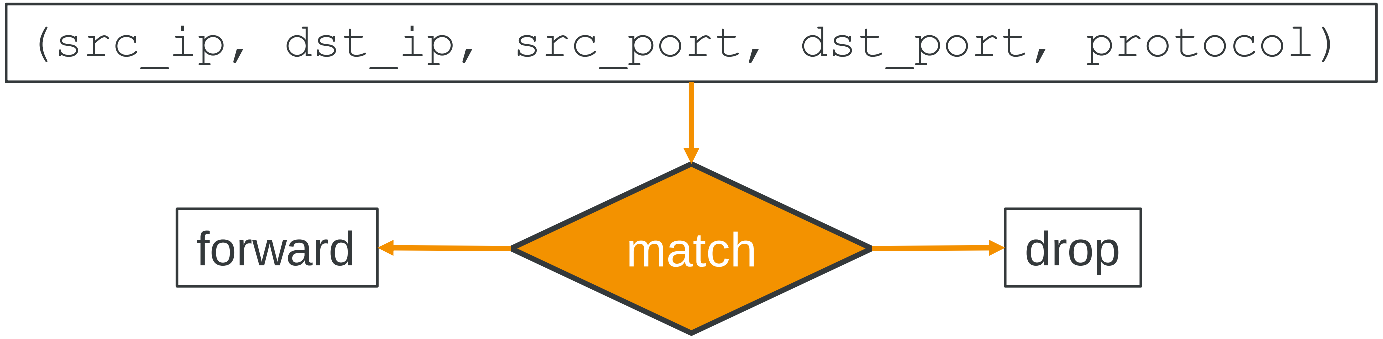
Pro

- Easier / faster updates of the “transport” layer.

Con

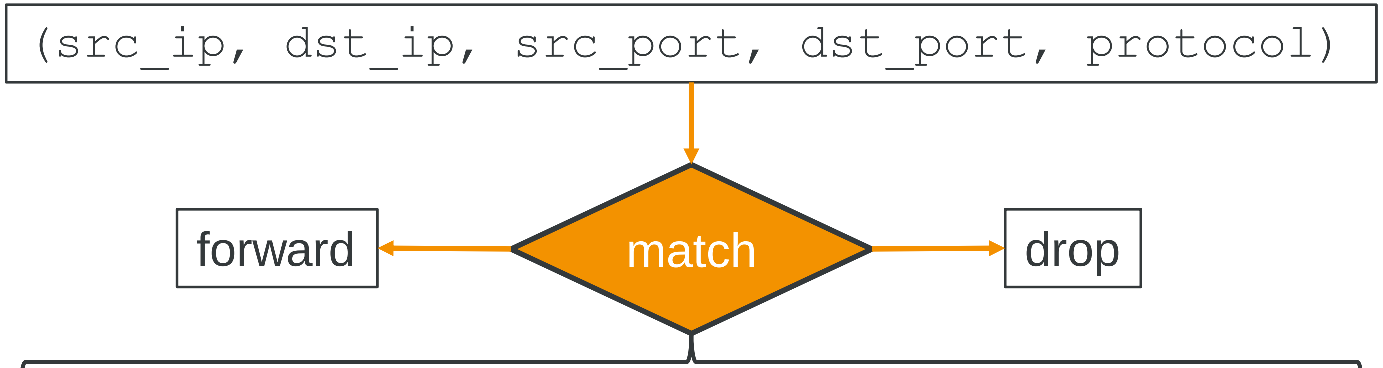
- No common TCP syscalls (e.g. listen, connect).
- Larger attack surface and weaker security boundaries.
- Lots of different / custom implementations of the same network functionality.

Transport Layer Firewalls



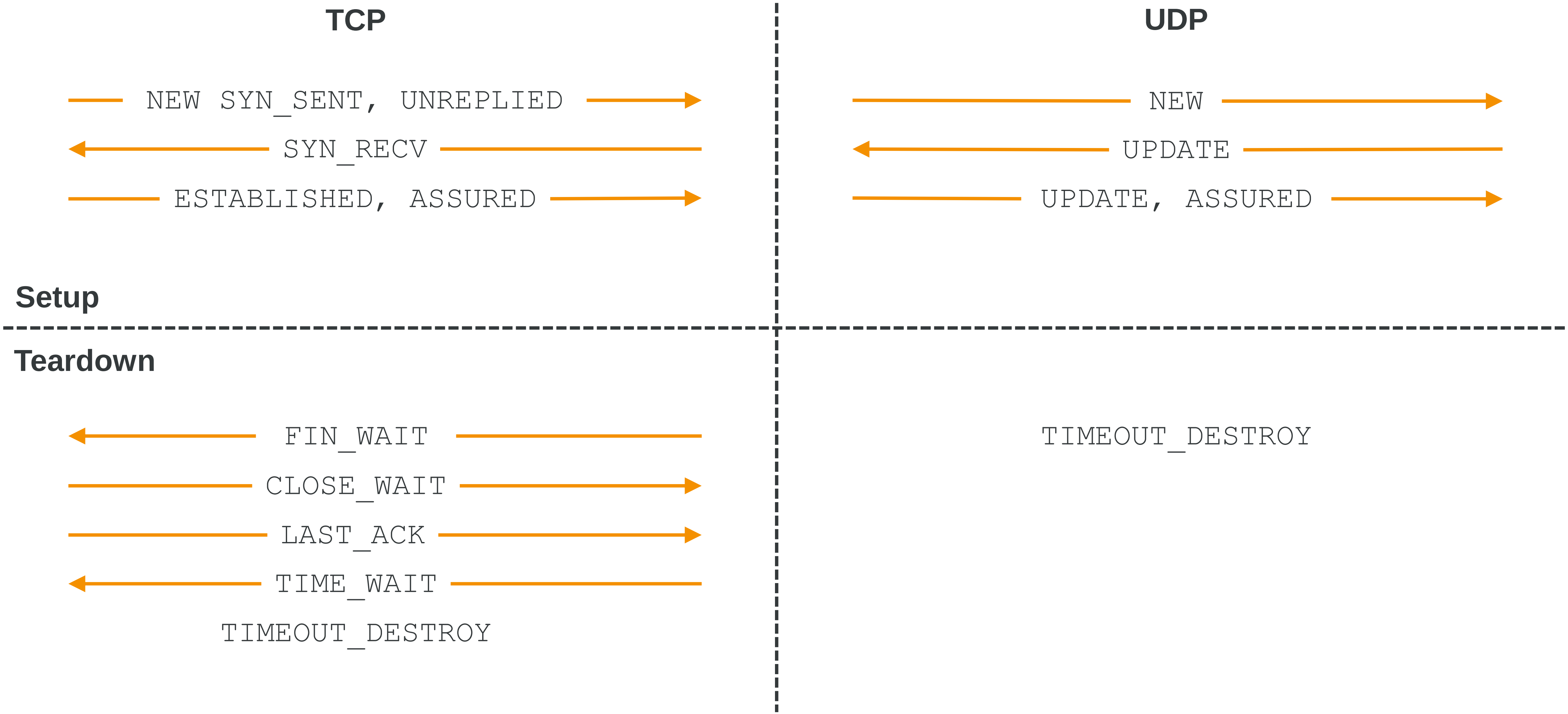
Stateless

Stateful



(.111, .234, 1234, 443, TCP)	SYN_SENT, UNREPLIED
(.112, .234, 2345, 443, TCP)	SYN_RECV
(.113, .234, 3456, 443, TCP)	ESTABLISHED, ASSURED
(.114, .234, 4567, 443, TCP)	FIN_WAIT

Stateful Tracking



TCP

NEW SYN_SENT, UNREPLIED

SYN_RECV

ESTABLISHED, ASSURED

Setup

Teardown

FIN_WAIT

CLOSE_WAIT

LAST_ACK

TIME_WAIT

TIMEOUT_DESTROY

UDP

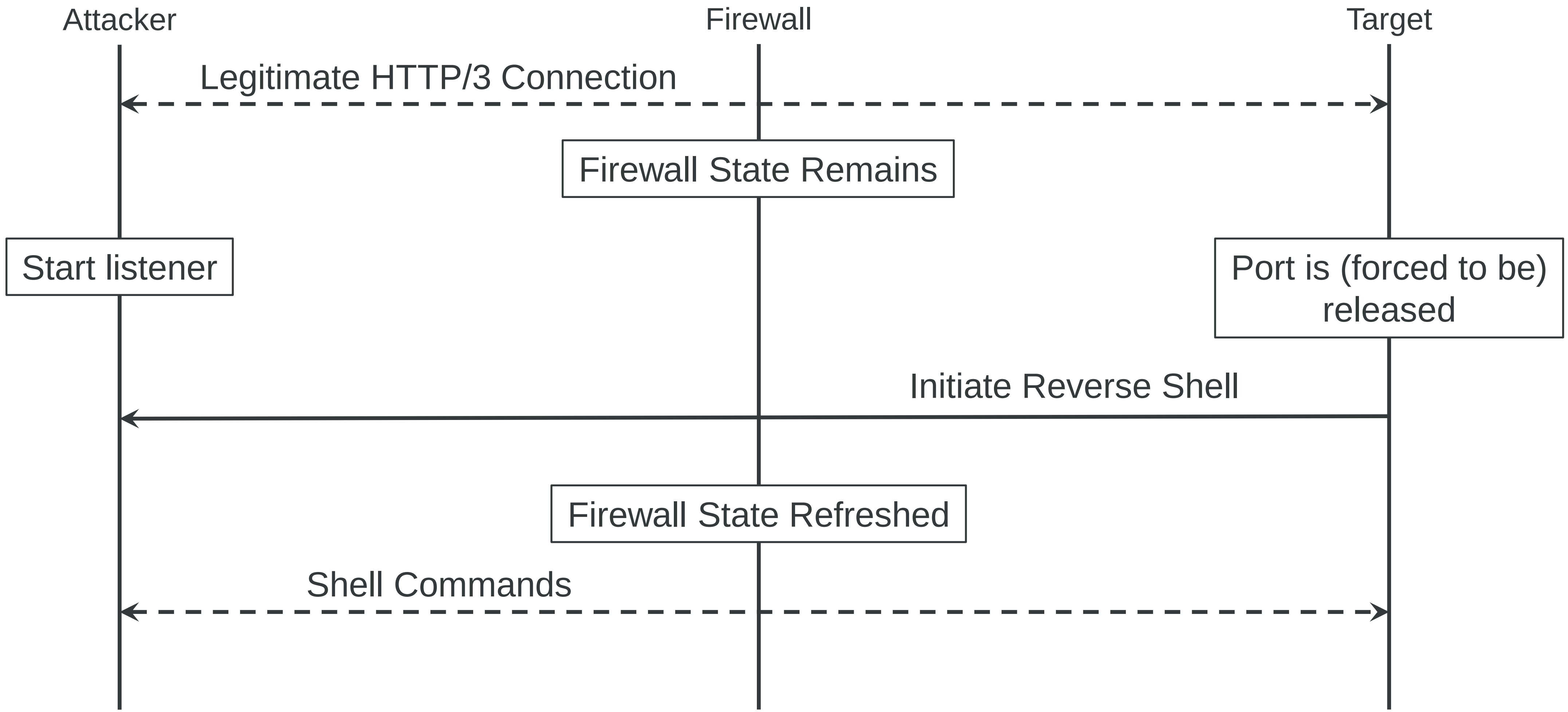
NEW

UPDATE

UPDATE, ASSURED

TIMEOUT_DESTROY

UDP Hole Punching



Attacker

Firewall

Target

Legitimate HTTP/3 Connection

Firewall State Remains

Start listener

Port is (forced to be) released

Initiate Reverse Shell

Firewall State Refreshed

Shell Commands

Deep Packet Inspection with QUIC

Routing / Optimization

- Important metadata headers are encrypted → Impact on routing strategies.
- Limited support by load balancers → Bypasses possible.

Application Layer Security

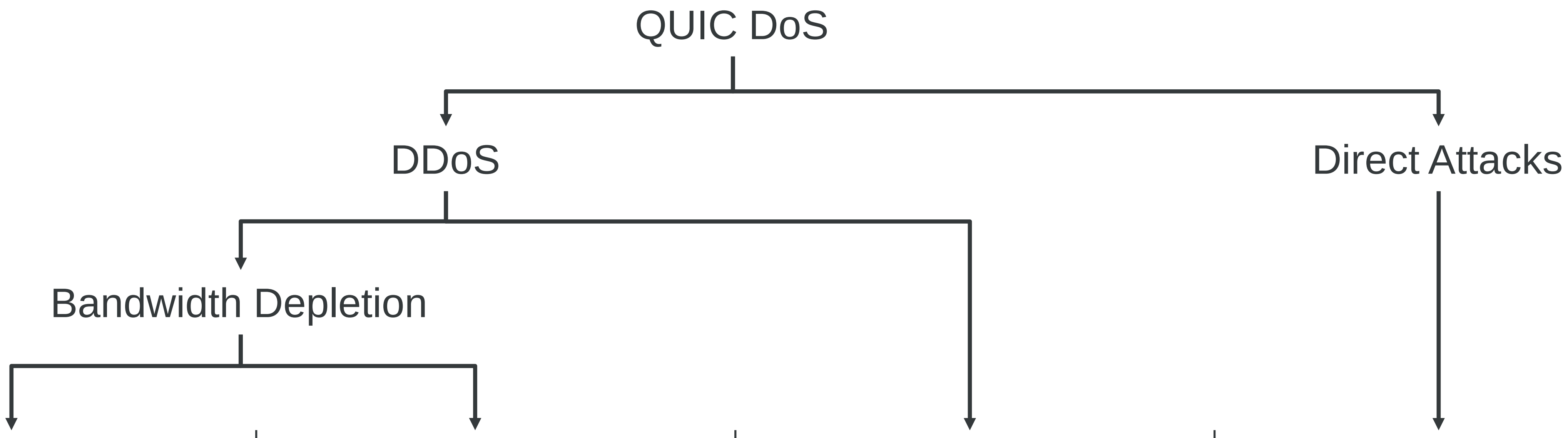
- Very limited support by existing WAFs.
- No support for the integrated multistreaming.

General Tooling Support

Tool	QUIC / HTTP/3	Alternatives
Wireshark	✓	
Chrome / Firefox	✓	
BurpSuite	✘	-
OWASP ZAP	✘	-
Nessus	✘	-
testssl, sslscan, …	✘	-
Postman	✘	Pororoca
curl (Experimental)	(✓)	
mitmproxy (Experimental, Forks)	(✓)	mitmproxy by meitinger
netcat	✘	quiccat by rossia (limited features)
socat	✘	quicat by pas2k

Disclaimer: No guarantees for any of those tools. Use carefully!

(D)DoS – Same Same but Different



QUIC DoS

DDoS

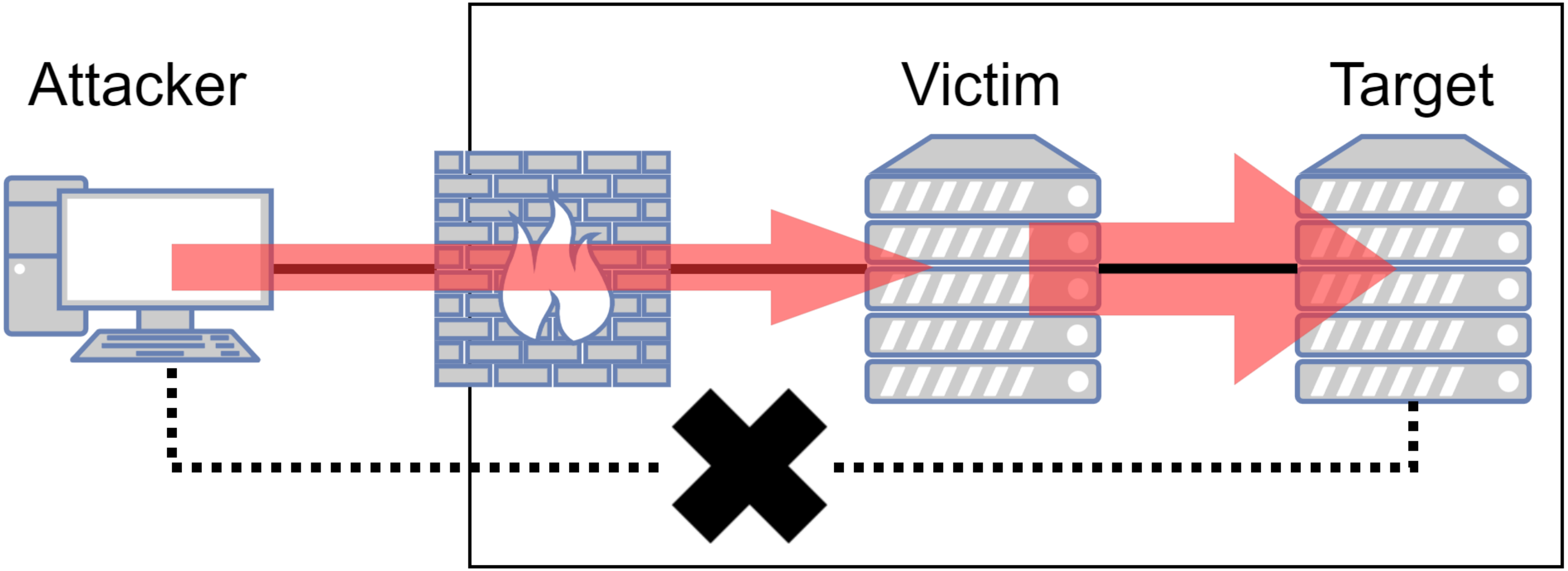
Direct Attacks

Bandwidth Depletion

Flood Attack	Amplification Attack	Resource Depletion	Packet Injection
• UDP Flooding	• **Connection Migration**	• Client Initial Flooding	• Handshake Termination
• Optimistic ACK	• **Server Initial**	• Stream Commitment	• Stateless Reset Oracle
	• 0-RTT Token	• Slow-Loris	
		• Stream Fragmentation	
		• Out-of-Context Frames	

Request Forgery

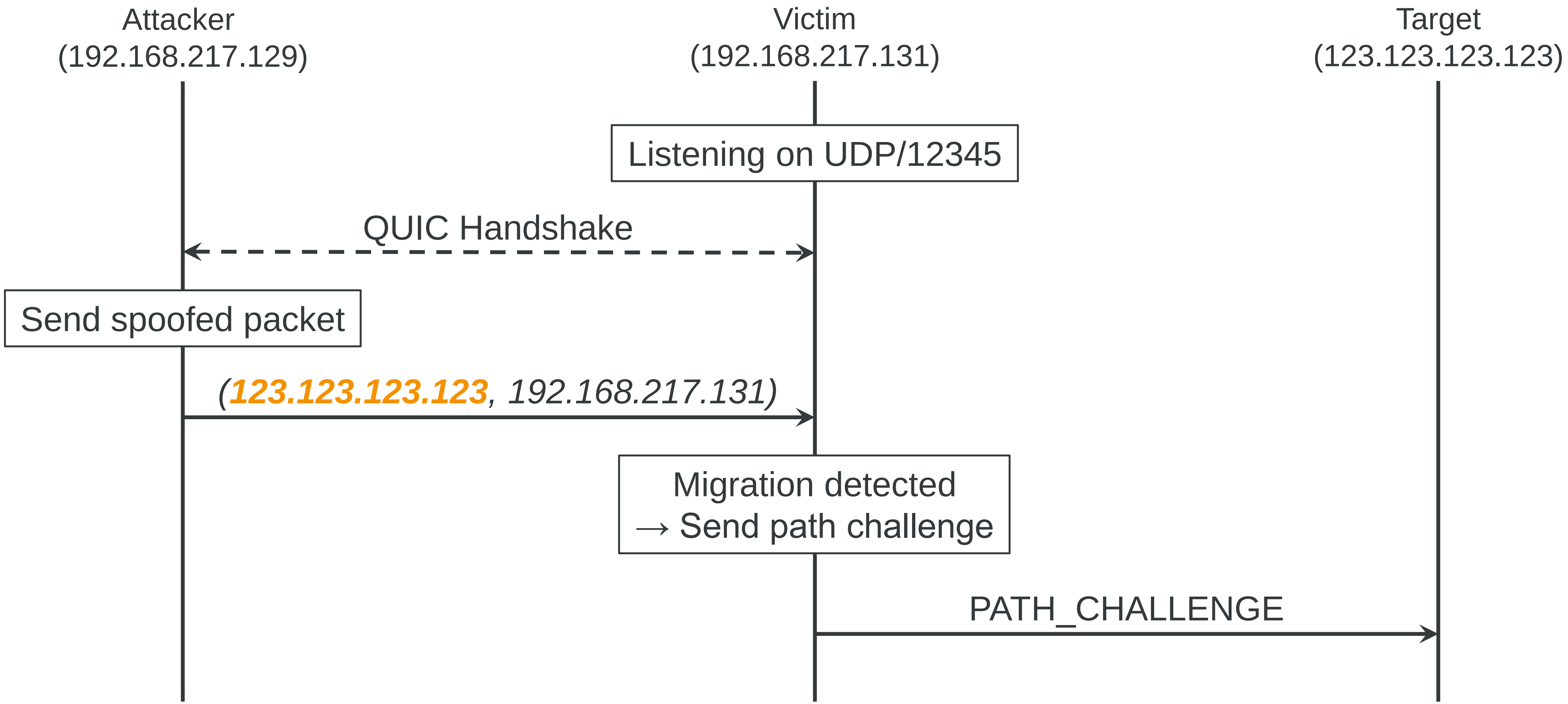
Client-side Request Forgery



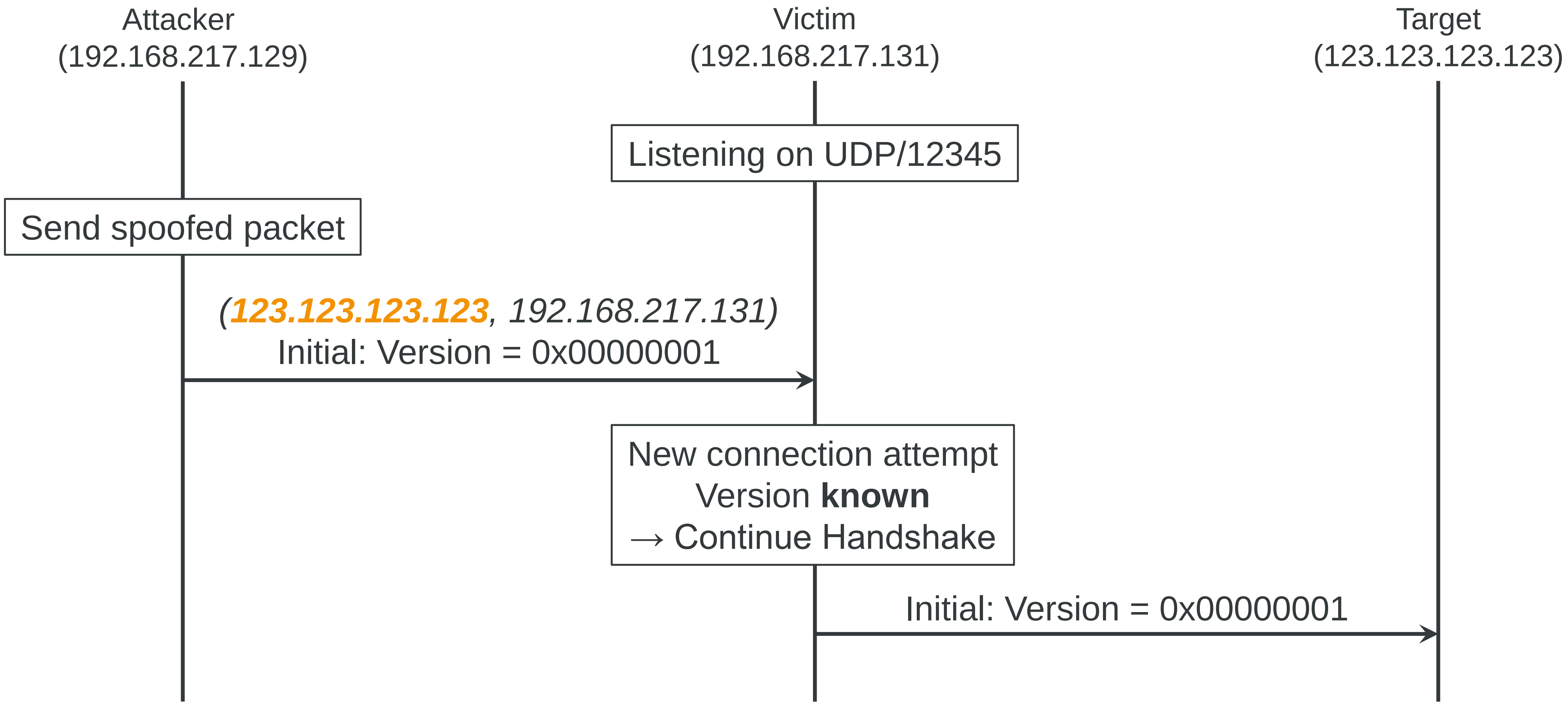
— Bypassing Network Restrictions

➡ Utilizing Victim Resources

Connection Migration Request Forgery (CMRF)



Server Initial Request Forgery (SIRF)



Attacker
(192.168.217.129)

Victim
(192.168.217.131)

Target
(123.123.123.123)

Listening on UDP/12345

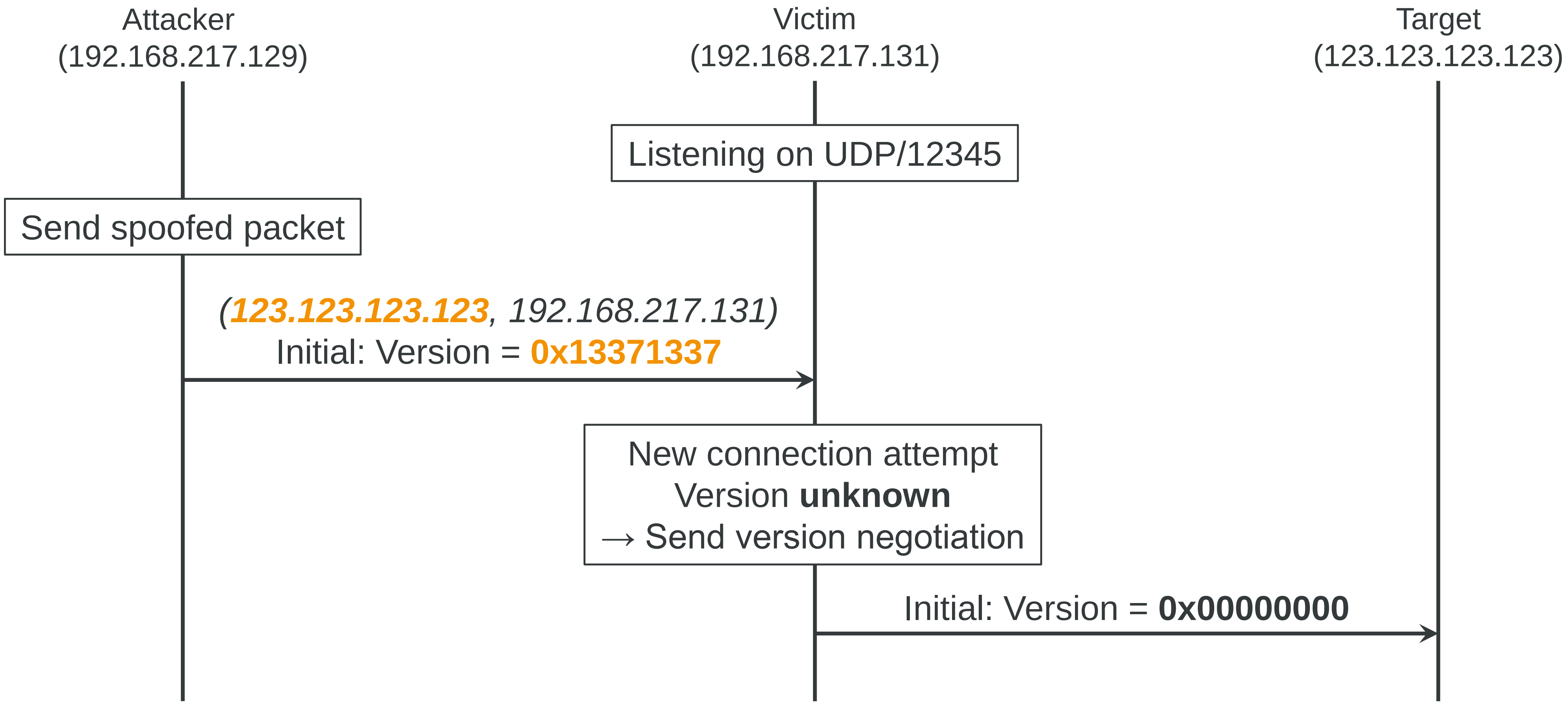
Send spoofed packet

*(**123.123.123.123**, 192.168.217.131)*
Initial: Version = 0x00000001

New connection attempt
Version **known**
→ Continue Handshake

Initial: Version = 0x00000001

Version Negotiation Request Forgery (VNRF)



Attacker
(192.168.217.129)

Victim
(192.168.217.131)

Target
(123.123.123.123)

Listening on UDP/12345

Send spoofed packet

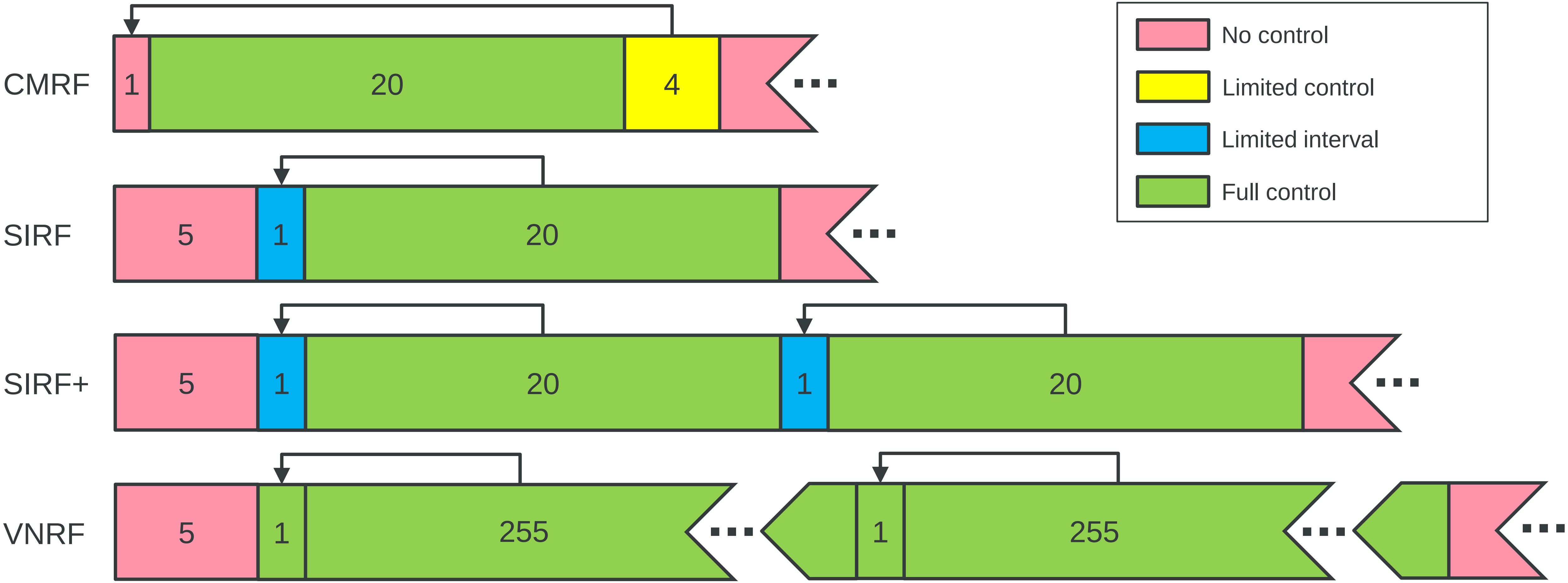
*(**123.123.123.123**, 192.168.217.131)*
Initial: Version = **0x13371337**

New connection attempt
Version **unknown**
→ Send version negotiation

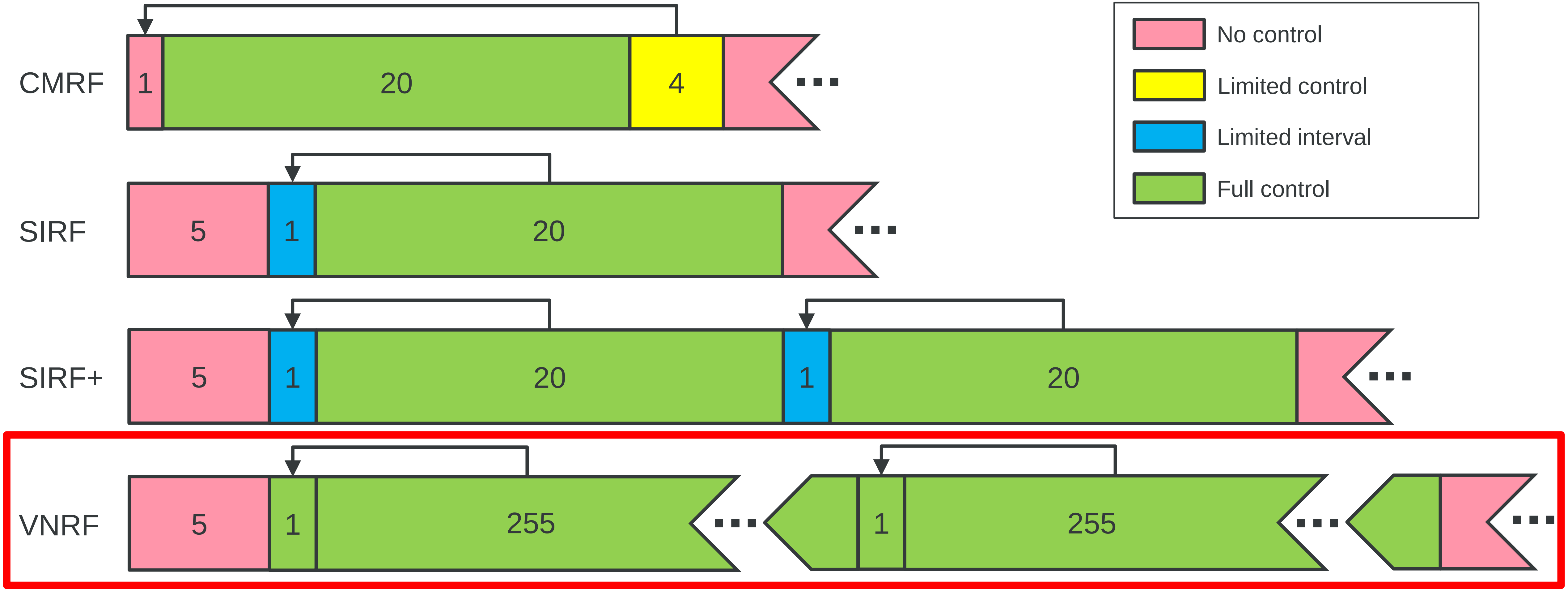
Initial: Version = **0x00000000**

Protocol Impersonation

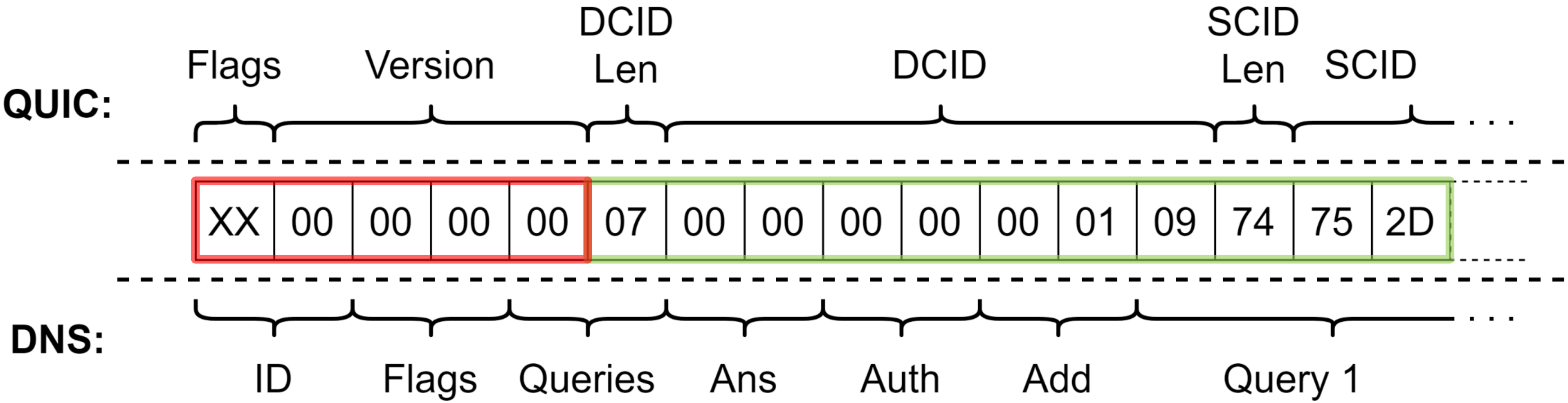
Controllable Bytes for Protocol Impersonation



Controllable Bytes for Protocol Impersonation

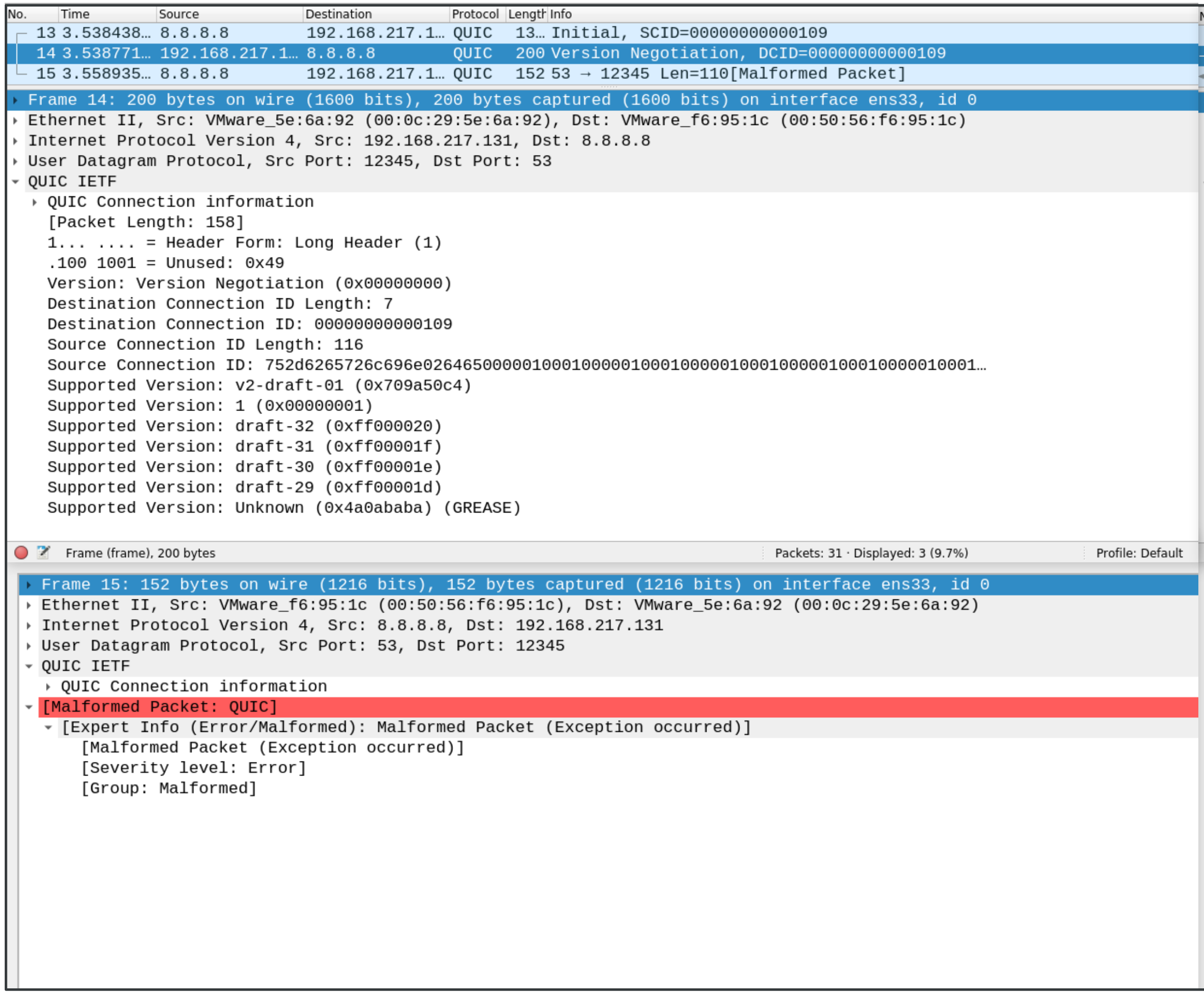


Impersonating DNS Requests with VNRF



XX	00	00	00	00	07	00	00	00	00	00	01	09	74	75	2D

Impersonating DNS Requests with VNRF (cont‘d)

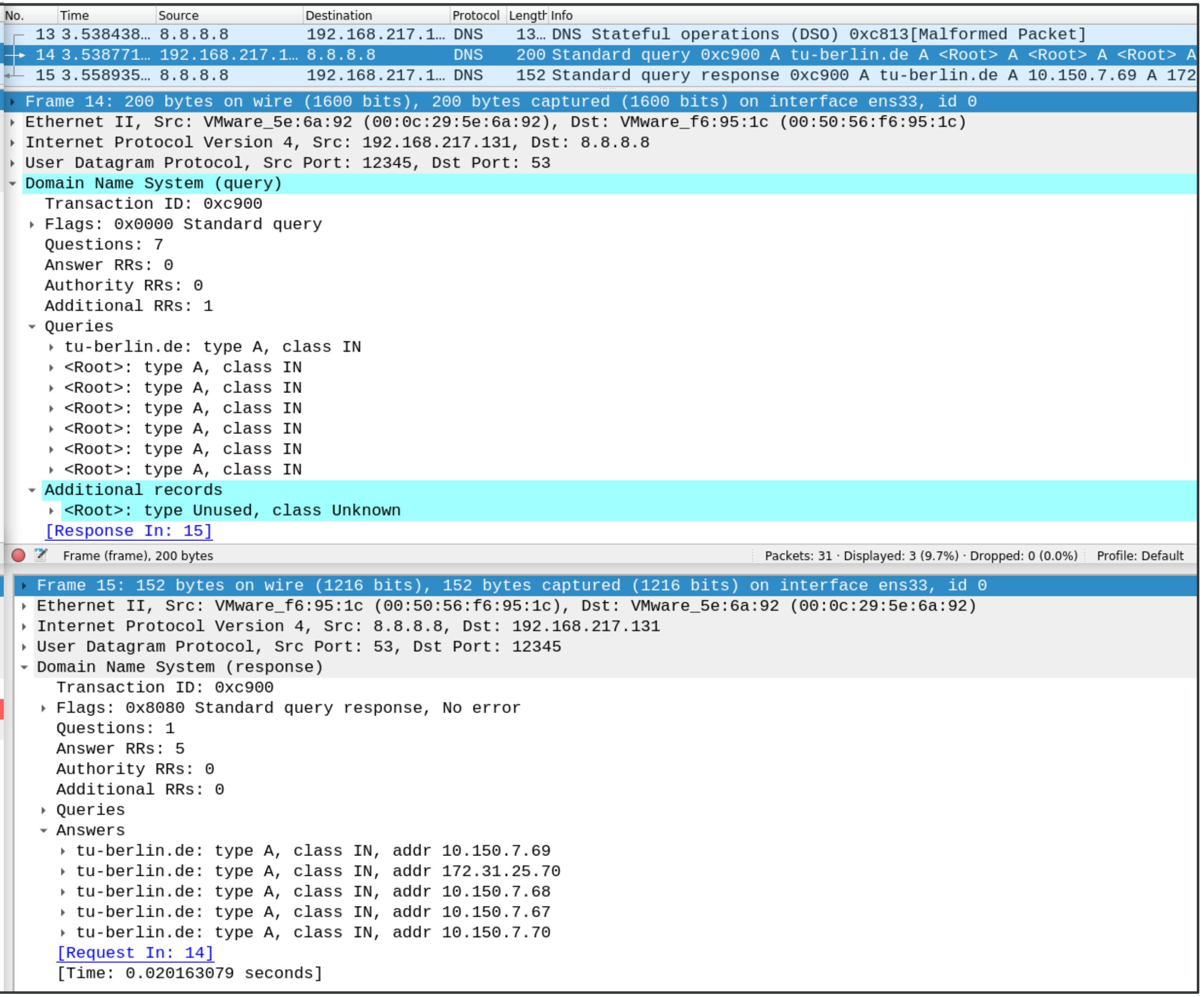


```
No.  Time          Source           Destination      Protocol Length Info
  13 3.538438…    8.8.8.8          192.168.217.1…   QUIC     13…    Initial, SCID=00000000000109
  14 3.538771…    192.168.217.1…   8.8.8.8          QUIC     200    Version Negotiation, DCID=00000000000109
  15 3.558935…    8.8.8.8          192.168.217.1…   QUIC     152    53 → 12345 Len=110[Malformed Packet]

▸ Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
▸ Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 12345, Dst Port: 53
▾ QUIC IETF
  ▸ QUIC Connection information
    [Packet Length: 158]
    1... .... = Header Form: Long Header (1)
    .100 1001 = Unused: 0x49
    Version: Version Negotiation (0x00000000)
    Destination Connection ID Length: 7
    Destination Connection ID: 00000000000109
    Source Connection ID Length: 116
    Source Connection ID: 752d6265726c696e02646500000100010000010001000001000100000100010000010001…
    Supported Version: v2-draft-01 (0x709a50c4)
    Supported Version: 1 (0x00000001)
    Supported Version: draft-32 (0xff000020)
    Supported Version: draft-31 (0xff00001f)
    Supported Version: draft-30 (0xff00001e)
    Supported Version: draft-29 (0xff00001d)
    Supported Version: Unknown (0x4a0ababa) (GREASE)

Frame (frame), 200 bytes                    Packets: 31 · Displayed: 3 (9.7%)          Profile: Default

▸ Frame 15: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_f6:95:1c (00:50:56:f6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.217.131
▸ User Datagram Protocol, Src Port: 53, Dst Port: 12345
▾ QUIC IETF
  ▸ QUIC Connection information
▾ [Malformed Packet: QUIC]
  ▾ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
      [Malformed Packet (Exception occurred)]
      [Severity level: Error]
      [Group: Malformed]
```



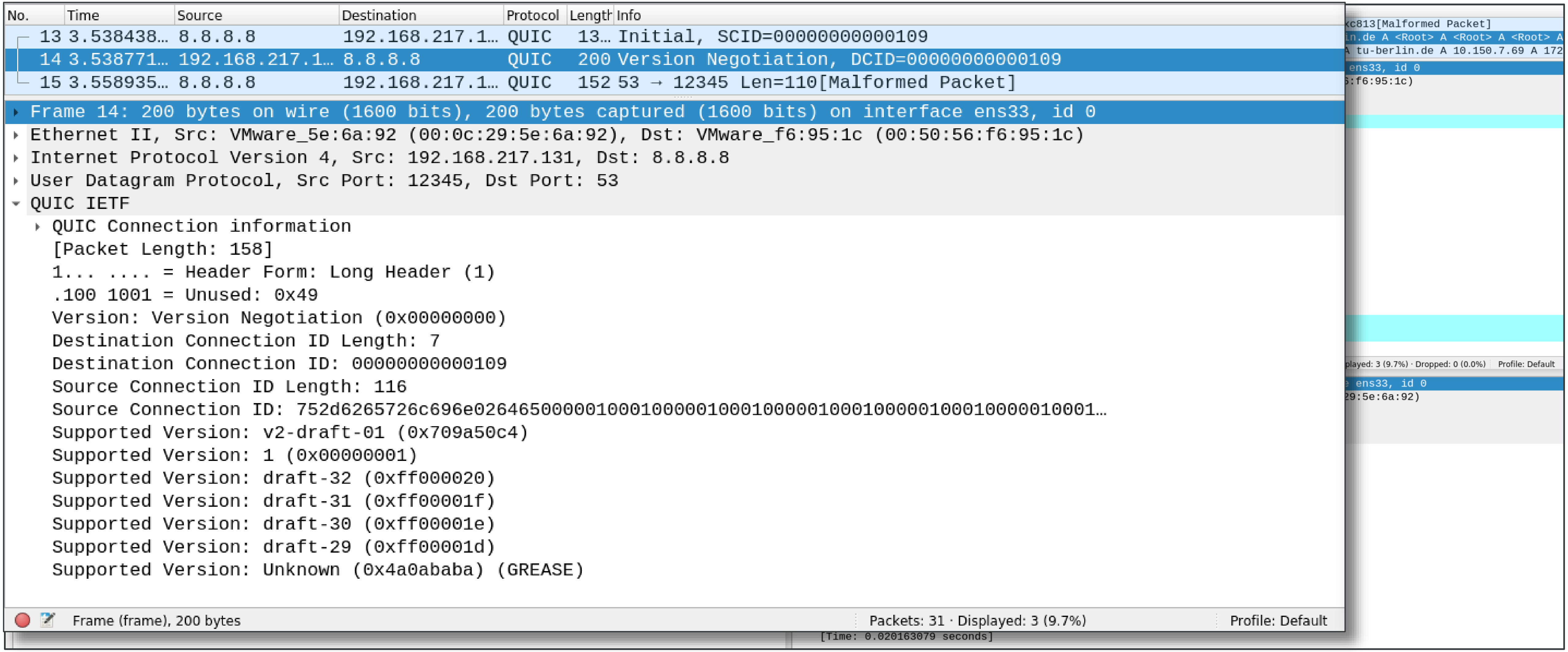
```
No.  Time          Source           Destination      Protocol Length Info
  13 3.538438…    8.8.8.8          192.168.217.1…   DNS      13…    DNS Stateful operations (DSO) 0xc813[Malformed Packet]
  14 3.538771…    192.168.217.1…   8.8.8.8          DNS      200    Standard query 0xc900 A tu-berlin.de A <Root> A <Root> A <Root> A
  15 3.558935…    8.8.8.8          192.168.217.1…   DNS      152    Standard query response 0xc900 A tu-berlin.de A 10.150.7.69 A 172

▸ Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
▸ Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 12345, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xc900
  ▸ Flags: 0x0000 Standard query
    Questions: 7
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ tu-berlin.de: type A, class IN
    ▸ <Root>: type A, class IN
    ▸ <Root>: type A, class IN
    ▸ <Root>: type A, class IN
    ▸ <Root>: type A, class IN
    ▸ <Root>: type A, class IN
    ▸ <Root>: type A, class IN
  ▾ Additional records
    ▸ <Root>: type Unused, class Unknown
    [Response In: 15]

Frame (frame), 200 bytes          Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%)     Profile: Default

▸ Frame 15: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_f6:95:1c (00:50:56:f6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.217.131
▸ User Datagram Protocol, Src Port: 53, Dst Port: 12345
▾ Domain Name System (response)
    Transaction ID: 0xc900
  ▸ Flags: 0x8080 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▸ tu-berlin.de: type A, class IN, addr 10.150.7.69
    ▸ tu-berlin.de: type A, class IN, addr 172.31.25.70
    ▸ tu-berlin.de: type A, class IN, addr 10.150.7.68
    ▸ tu-berlin.de: type A, class IN, addr 10.150.7.67
    ▸ tu-berlin.de: type A, class IN, addr 10.150.7.70
    [Request In: 14]
    [Time: 0.020163079 seconds]
```

Impersonating DNS Requests with VNRF (cont‘d)



```
No.  Time         Source           Destination      Protocol Length Info
  13 3.538438…    8.8.8.8          192.168.217.1…   QUIC     13…    Initial, SCID=000000000000109
  14 3.538771…    192.168.217.1…   8.8.8.8          QUIC     200    Version Negotiation, DCID=000000000000109
  15 3.558935…    8.8.8.8          192.168.217.1…   QUIC     152    53 → 12345 Len=110[Malformed Packet]
```

```
▸ Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
▸ Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 12345, Dst Port: 53
▾ QUIC IETF
  ▸ QUIC Connection information
    [Packet Length: 158]
    1... .... = Header Form: Long Header (1)
    .100 1001 = Unused: 0x49
    Version: Version Negotiation (0x00000000)
    Destination Connection ID Length: 7
    Destination Connection ID: 000000000000109
    Source Connection ID Length: 116
    Source Connection ID: 752d6265726c696e02646500000100010000010001000001000100000100010000010001…
    Supported Version: v2-draft-01 (0x709a50c4)
    Supported Version: 1 (0x00000001)
    Supported Version: draft-32 (0xff000020)
    Supported Version: draft-31 (0xff00001f)
    Supported Version: draft-30 (0xff00001e)
    Supported Version: draft-29 (0xff00001d)
    Supported Version: Unknown (0x4a0ababa) (GREASE)
```

Frame (frame), 200 bytes | Packets: 31 · Displayed: 3 (9.7%) | Profile: Default

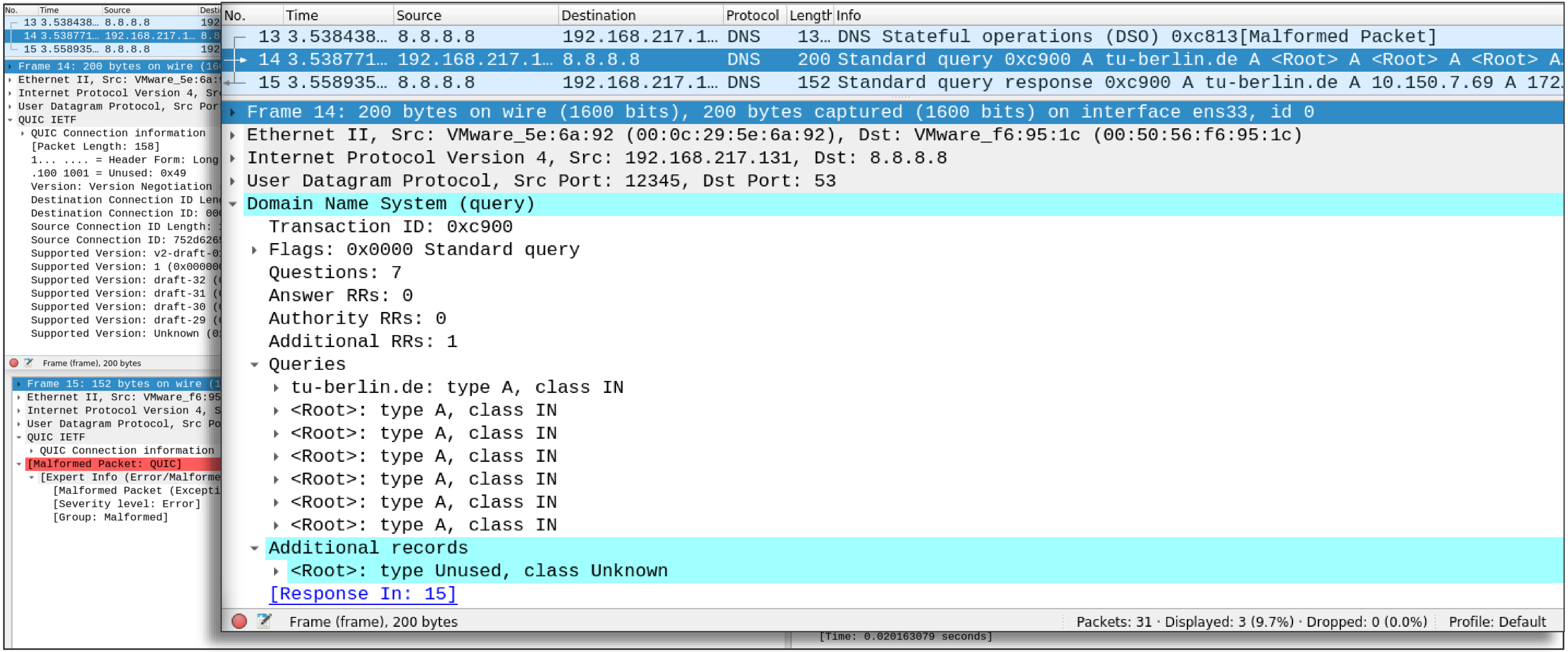
```
xc813[Malformed Packet]
in.de A <Root> A <Root> A <Root> A
A tu-berlin.de A 10.150.7.69 A 172
 ens33, id 0
6:f6:95:1c)
```

played: 3 (9.7%) · Dropped: 0 (0.0%) | Profile: Default

```
e ens33, id 0
29:5e:6a:92)
```

```
[Time: 0.020163079 seconds]
```

Impersonating DNS Requests with VNRF (cont‘d)



```
No.  Time        Source          Desti
  13 3.538438…   8.8.8.8         192
  14 3.538771…   192.168.217.1…  8.8
  15 3.558935…   8.8.8.8         192

Frame 14: 200 bytes on wire (16
Ethernet II, Src: VMware_5e:6a:
Internet Protocol Version 4, Sr
User Datagram Protocol, Src Por
QUIC IETF
  QUIC Connection information
  [Packet Length: 158]
  1... .... = Header Form: Long
  .100 1001 = Unused: 0x49
  Version: Version Negotiation
  Destination Connection ID Len
  Destination Connection ID: 00
  Source Connection ID Length:
  Source Connection ID: 752d626
  Supported Version: v2-draft-0
  Supported Version: 1 (0x00000
  Supported Version: draft-32 (
  Supported Version: draft-31 (
  Supported Version: draft-30 (
  Supported Version: draft-29 (
  Supported Version: Unknown (0
```

Frame (frame), 200 bytes

```
Frame 15: 152 bytes on wire (1
Ethernet II, Src: VMware_f6:95
Internet Protocol Version 4, S
User Datagram Protocol, Src Po
QUIC IETF
  QUIC Connection information
[Malformed Packet: QUIC]
  [Expert Info (Error/Malforme
    [Malformed Packet (Excepti
    [Severity level: Error]
    [Group: Malformed]
```

```
No.  Time        Source          Destination     Protocol Length Info
  13 3.538438…   8.8.8.8         192.168.217.1…  DNS      13…    DNS Stateful operations (DSO) 0xc813[Malformed Packet]
  14 3.538771…   192.168.217.1…  8.8.8.8         DNS      200    Standard query 0xc900 A tu-berlin.de A <Root> A <Root> A <Root> A…
  15 3.558935…   8.8.8.8         192.168.217.1…  DNS      152    Standard query response 0xc900 A tu-berlin.de A 10.150.7.69 A 172…

Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0
Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 12345, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0xc900
  Flags: 0x0000 Standard query
  Questions: 7
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    tu-berlin.de: type A, class IN
    <Root>: type A, class IN
    <Root>: type A, class IN
    <Root>: type A, class IN
    <Root>: type A, class IN
    <Root>: type A, class IN
    <Root>: type A, class IN
  Additional records
    <Root>: type Unused, class Unknown
  [Response In: 15]
```

Frame (frame), 200 bytes | Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) | Profile: Default

[Time: 0.020163079 seconds]

Mitigation

CID Reflection

- A server always choses a fresh SCID, also for version negotiation

Hashing

- A „seed“ for a CID still chosen by the client
- The server uses a hash of the seed as DCID
- An attacker would need to calculate the inverse to create a meaningful payload

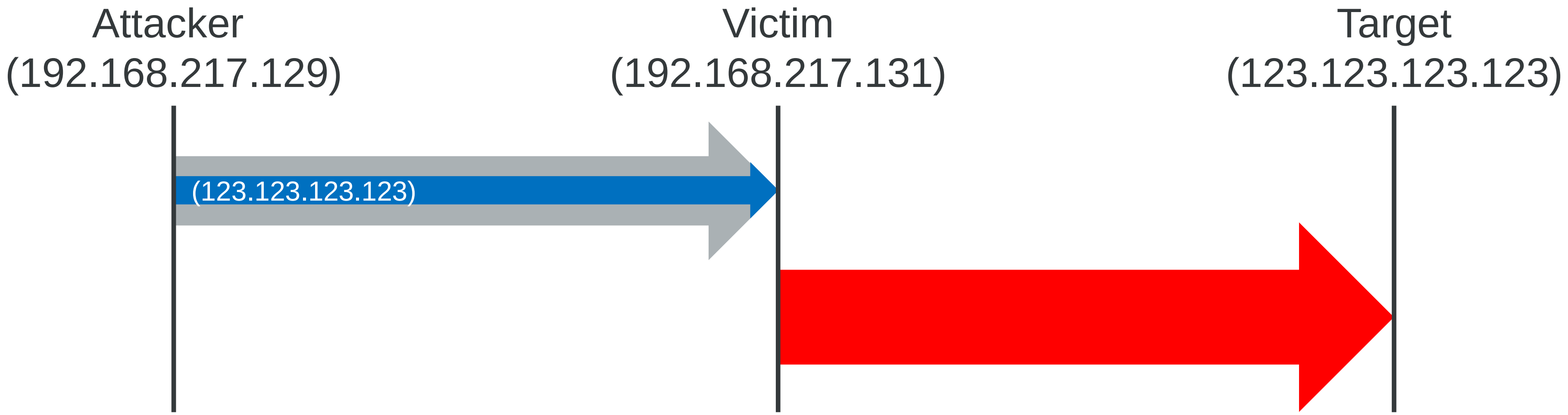
Masking

- QUIC headers get an additional field containing a masking value
- The masking value is randomly generated by the server
- The entire remaining header is XORed
- Client maintains control over DCID but payloads will appear „random“

Traffic Amplification

Path amplification VS Bandwidth Amplification

$$PAF = \frac{\#\, Bytes\ from\ victim\ to\ target}{\#\, Bytes\ from\ attacker\ to\ victim\ with\ spoofed\ address}$$



$$BAF = \frac{\#\, Bytes\ from\ victim\ to\ target}{\#\, Bytes\ from\ attacker\ to\ victim}$$

Amplification Pitfalls

“[…] not send more than three times the amount of data received on any unvalidated path.”

Minimum path requirements

- „QUIC must not be used if the network path cannot support 1200 bytes datagrams“
- Ensured through padding of initial packets and path challenges
- Small packets on new paths are an issue
- ***Server should send two separate path validations***

Unbalanced handshake sizes

- Server initial packets are larger than client intial packets
- ***Server initial packets should never be larger than 3*1200 bytes***

Amplification Pitfalls

Reliability

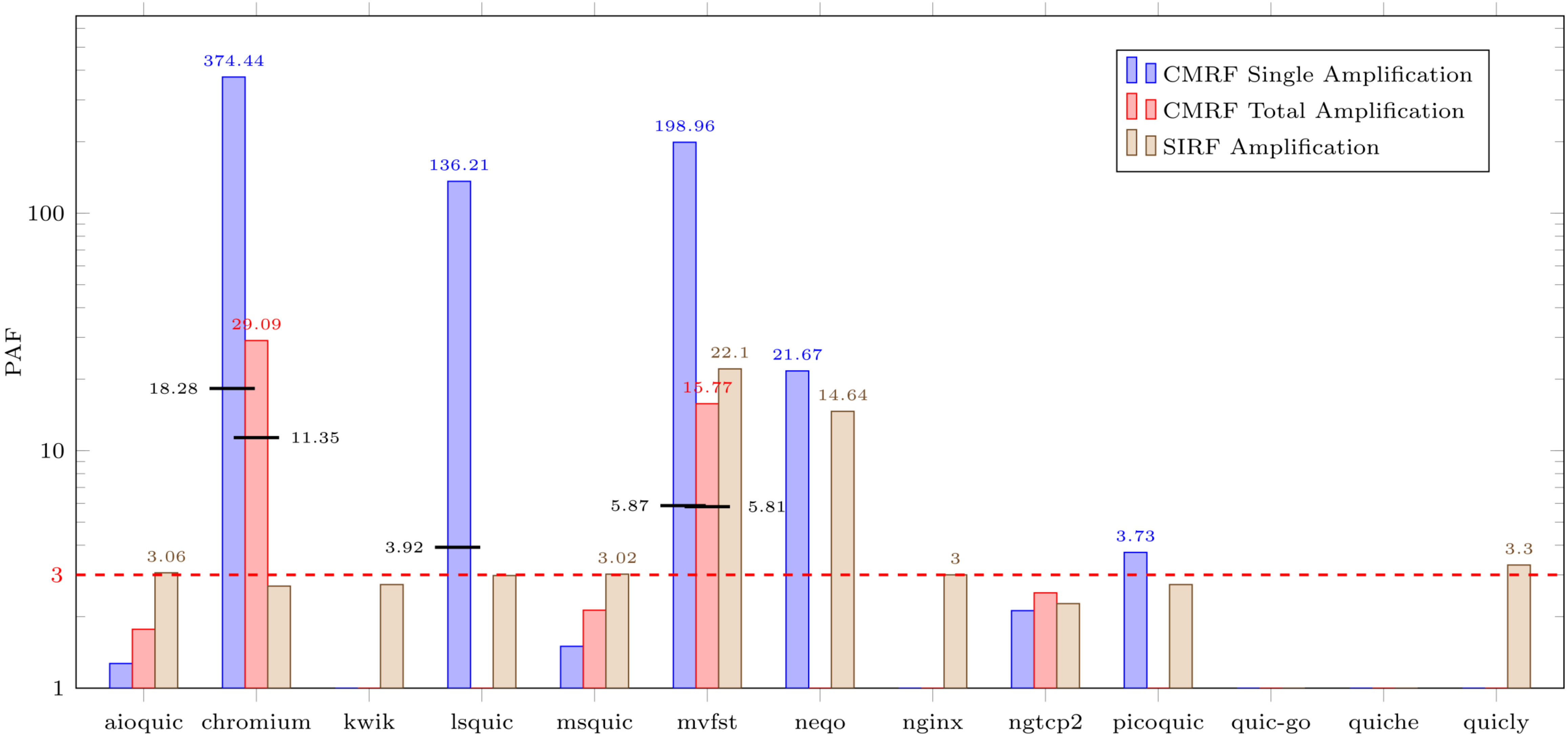
- No „typical“ reliability in path challenges, server can send multiple challenges
  - Initial bursts
  - Re-send with timeout
- ***Multiple challenges definitely surpass amplification limits***

- Normal packets are re-sent if the acknowledgment is not received
- ***Server should not re-send server initial packets***
  - Retries for the initial messages have to be handled by the client.

Mitigation

RTFM

Amplification



Conclusion

Conclusion

- ***Greater attack surface and room for errors.***
- ***“Old” vulnerabilities become more relevant again.***
- ***Poor tooling support.***
  - Offensive and Defensive.
- ***We see a significant discrepancy between specification and implementations.***
- ***Novel attack vectors like protocol impersonation.***
  - Currently no built-in protection mechanism.

Thanks!

Blogpost with additional technical details:

https://r.sec-consult.com/quic

NDSS Paper about request forgery in QUIC:

https://www.ndss-symposium.org/ndss-paper/quicforge-client-side-request-forgery-in-quic/

Paper about firewall issues in QUIC:

https://arxiv.org/abs/2107.05939

Thanks for listening!