Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Offloading Encryption to QUIC Enabled NICs

Andy Gospodarek – Software Architect, Broadcom
Eric Davis – System Architect, Broadcom
Eric Spada – Distinguished Engineer, Broadcom

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Overview of QUIC

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

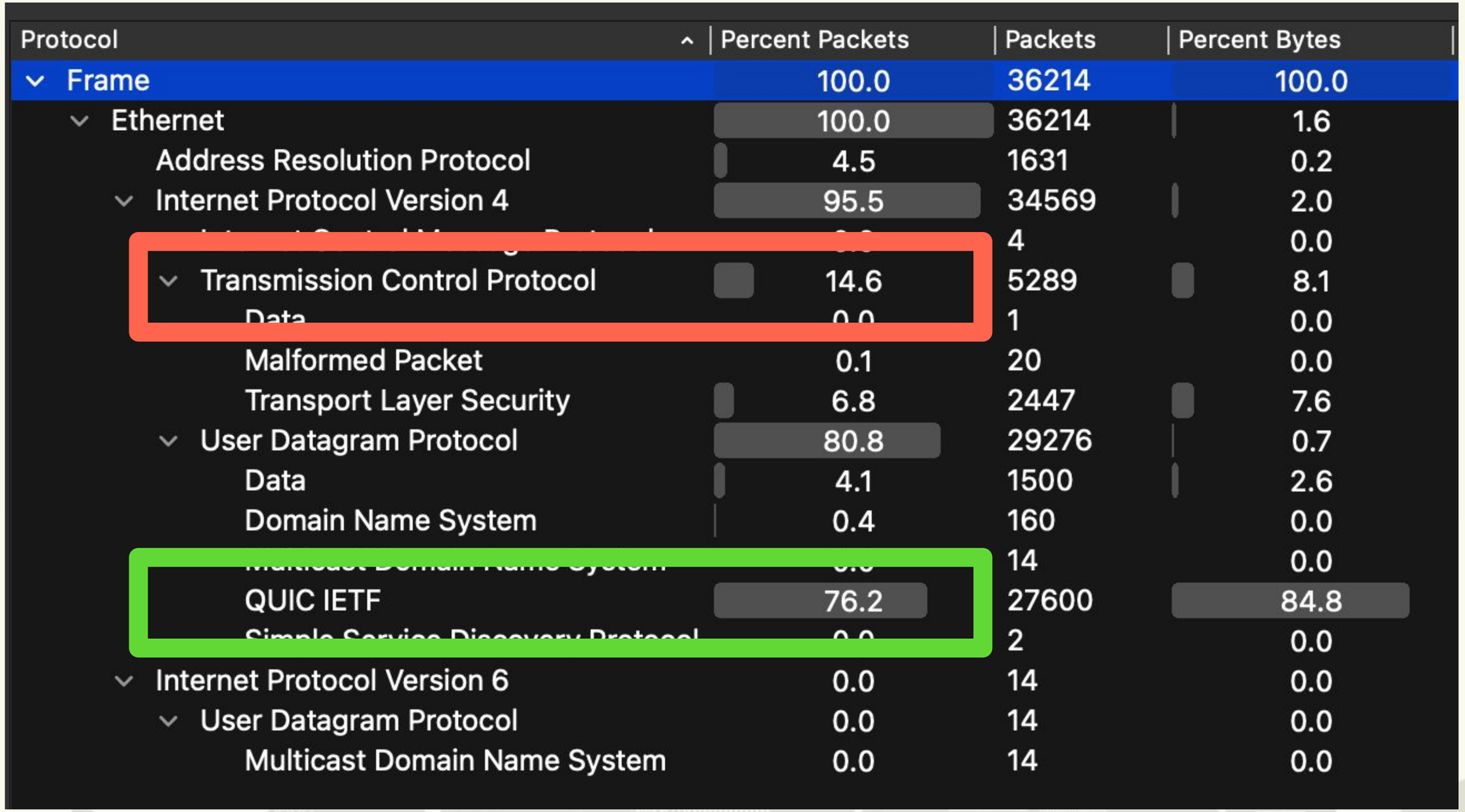
Transport protocol that runs over UDP

Utilizes TLS1.3 for handshake/key exchange

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Transmit and Receive Connection IDs are used to identify unique connections

Encryption is self-contained within each packet



Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	36214	100.0
Ethernet	100.0	36214	1.6
Address Resolution Protocol	4.5	1631	0.2
Internet Protocol Version 4	95.5	34569	2.0
[illegible]	[illegible]	4	0.0
Transmission Control Protocol	14.6	5289	8.1
Data	0.0	1	0.0
Malformed Packet	0.1	20	0.0
Transport Layer Security	6.8	2447	7.6
User Datagram Protocol	80.8	29276	0.7
Data	4.1	1500	2.6
Domain Name System	0.4	160	0.0
[illegible]	[illegible]	14	0.0
QUIC IETF	76.2	27600	84.8
[illegible]	[illegible]	2	0.0
Internet Protocol Version 6	0.0	14	0.0
User Datagram Protocol	0.0	14	0.0
Multicast Domain Name System	0.0	14	0.0

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Hardware offload good; software only bad

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Checksum Offload, LRO/GRO, GSO, Tunnel Offload, nTuple filtering, HW Timestamping, kTLS, TC, ...

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

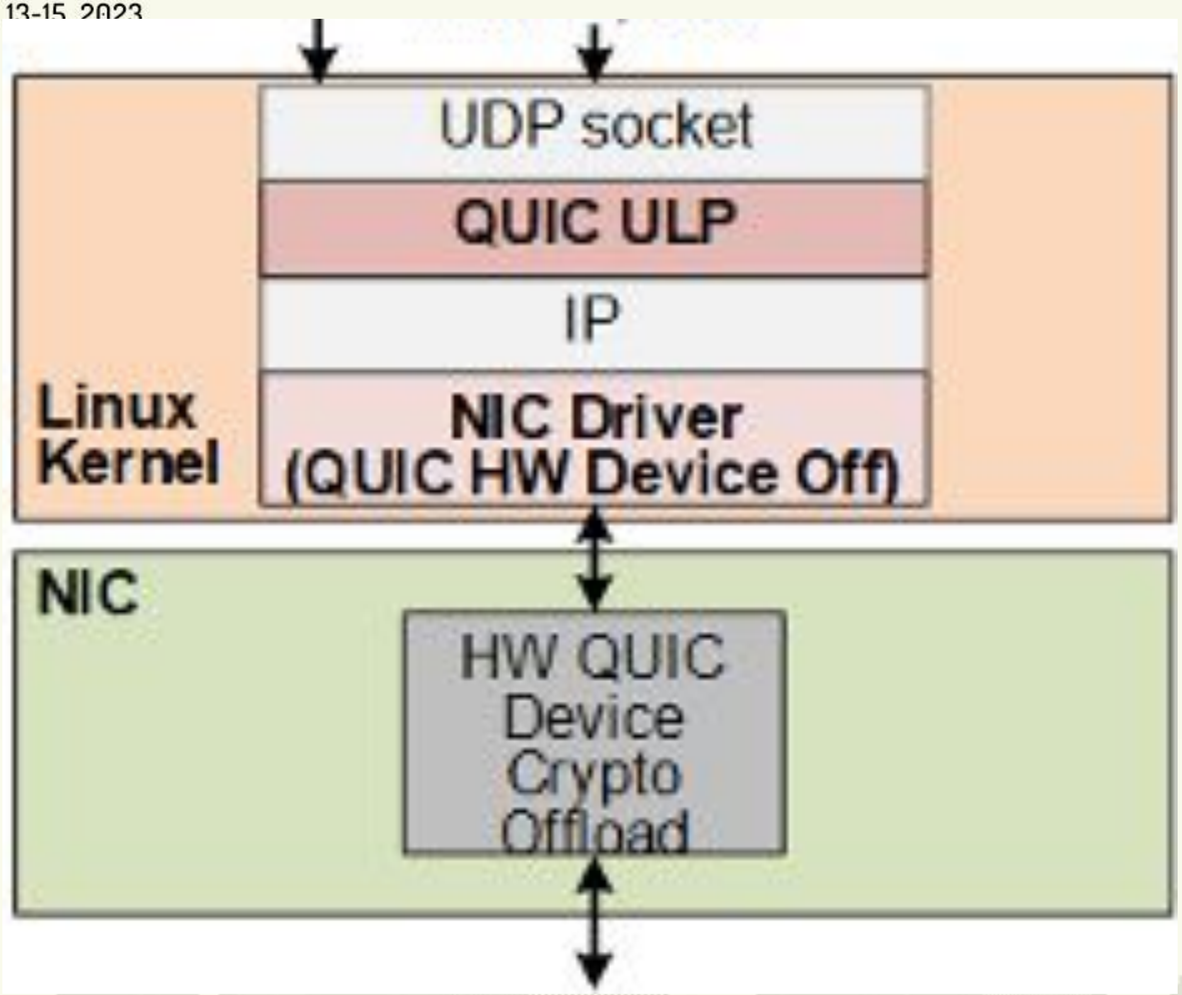
What could QUIC hardware offload look like?

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Leverage experience from kTLS Offload to support QUIC Offload

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

`quic` kernel module with userspace/netlink and driver interface


UDP socket
QUIC ULP
IP
Linux
Kernel
NIC Driver
(QUIC HW Device Off)
NIC
HW QUIC
Device
Crypto
Offload

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Tracks flow, connection ID, direction and QUIC session/crypto information for offload


```
#define QUIC_MAX_CONN_ID_LEN 20
#define QUIC_MAX_PKT_NUM_LEN 8

struct quic_flow_ctx {
    u8 conn_id_len;
    u8 conn_id[QUIC_MAX_CONN_ID_LEN];
    u8 pkt_num[QUIC_MAX_PKT_NUM_LEN];
    u8 key_phase;
    u8 cipher;
    u16 xid;

    union {
        struct cipher_aes_gcm_128 aes_gcm_128;
        struct cipher_aes_ccm_128 aes_ccm_128;
        struct cipher_chacha20_poly1305 chacha20_poly1305;
    } cipher_info;
};
```

Receives offload requests via netlink


```
# ip crypto show mode quic
4ed45802: rx 10.0.0.1:53227 10.0.0.100:443 cid e45ea092c337f4eb cipher
aes_gcm_128 dev ens7f0np0
```

Adds offloaded connection info to drivers and hardware

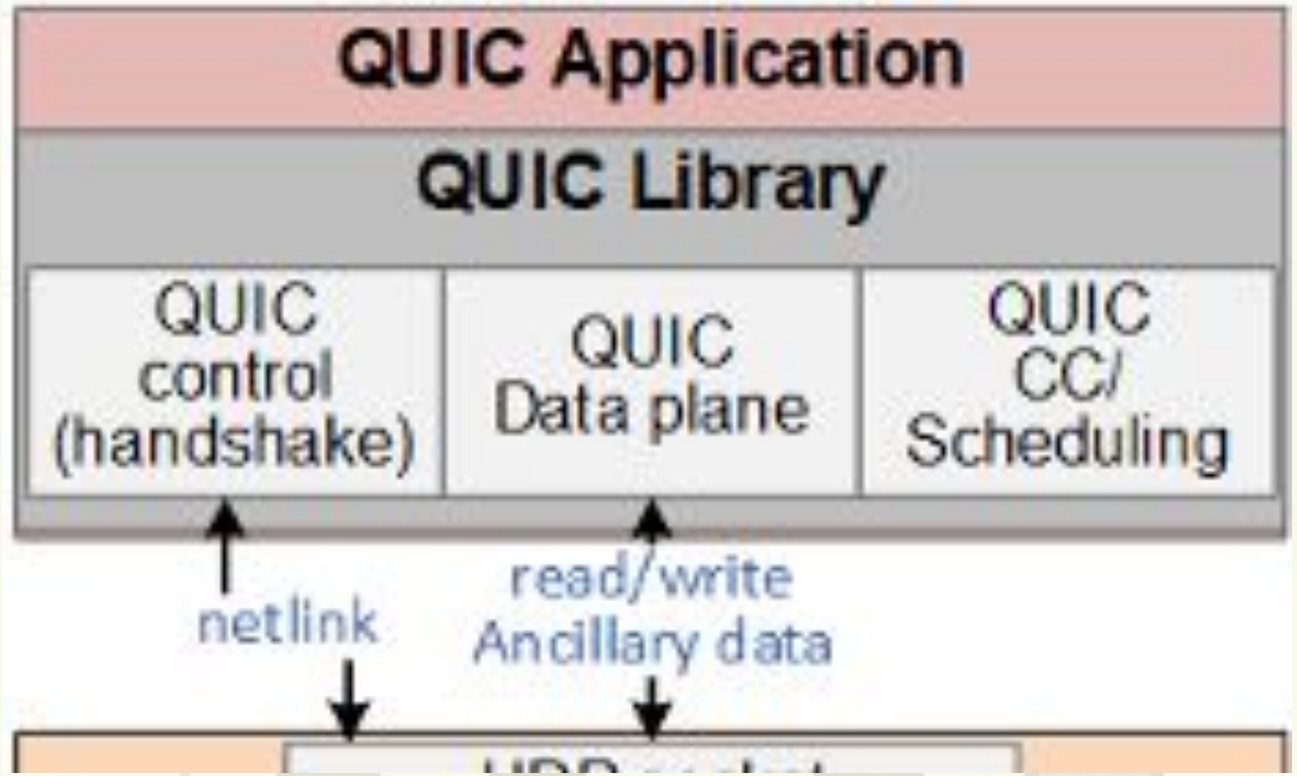

```
enum quic_offload_dir {
     QUIC_OFFLOAD_DIR_RX,
     QUIC_OFFLOAD_DIR_TX
};

int (*quic_dev_add)(struct net_device *netdev,
                    struct sock *sk,
                    struct quic_flow_ctx *flow_ctx
                    enum quic_offload_dir direction);
```

Returns XID to caller if flow can be offloaded

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

QUIC userspace components


QUIC Application
QUIC Library
QUIC control (handshake)
QUIC Data plane
QUIC CC/ Scheduling
netlink
read/write Ancillary data

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Application/Library does initial connection setup/handshake

If application wants to offload; send request to offload via `netlink`

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Application stores XID returned in netlink ext_ack cookie

Transmit datapath

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

XID passed into `cmsghdr` if data is to be encrypted by hardware

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

XID added to sk_buff extension in socket layer

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Network driver formats TX buffer descriptor as needed based on sk_buff extension data

Hardware sends encrypted packet to peer

Receive datapath

Frames will be decrypted by hardware and validation reported in buffer descriptor

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

Driver will populate sk_buff extension with decrypt and authentication status from buffer descriptor

Socket will set `cmsghdr` and pass back to application, indicating XID, encryption, validation status

Sounds simple, right?

Conclusions and Next Steps

QUIC is well suited for device offload

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

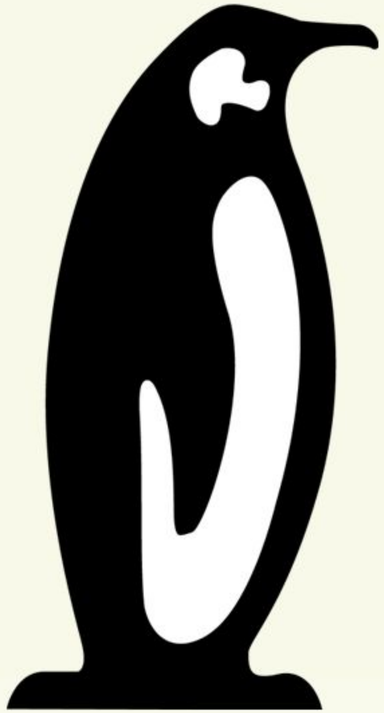
Modifications to kernel and network drivers are clear

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

QUIC device offload will be part of bnxt_en driver updates

QUIC Libraries may take more work to increase adoption and usage

FIN



Linux Plumbers Conference

Richmond, Virginia | November 13-15, 2023