

# Where is ECN stripped on the network?

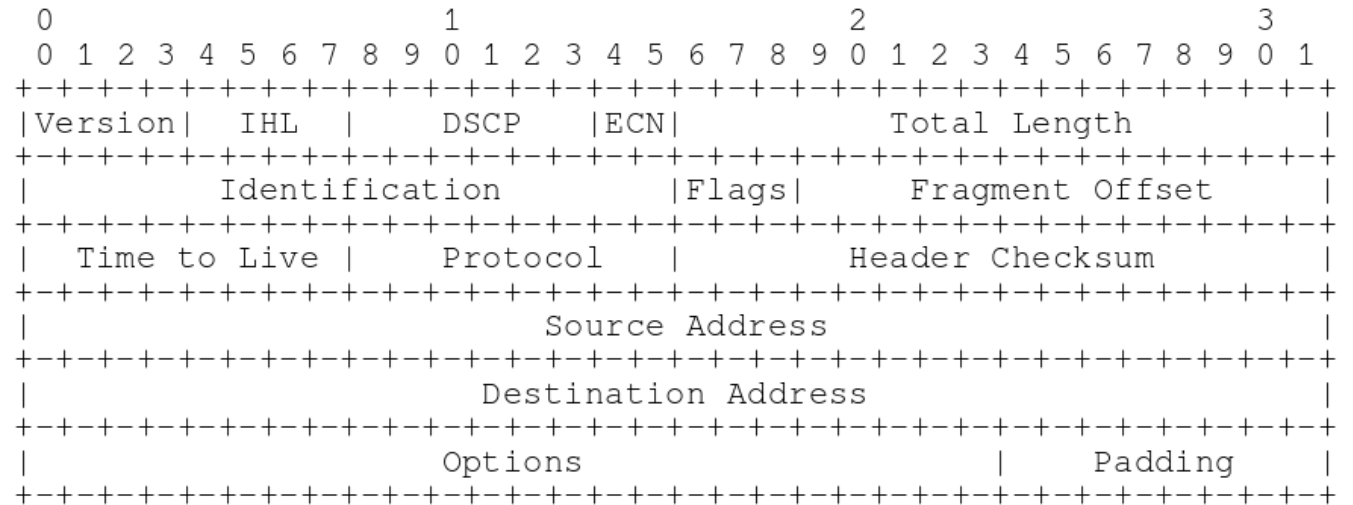
Myles Lamb (2325727L)

# Outline

- Background
- Aims
- Design
- Implementation
- Results

# Explicit Congestion Notification (ECN)

- Introduced by RFC 3168, in 2001
- Replaces two reserved bits of the Traffic Class byte
- Four possible bit values
  - 00 = Not ECN capable
  - 01 = ECT(1)
  - 10 = ECT(0)
  - 11 = CE (congestion experienced)
- Misconfigured devices have presented deployment issues



# Type of Service field

- Bits that constitute the ECN field have served previous purposes
- Devices implementing ToS may inadvertently destroy ECN signalling

```
 6 7 8 9 0 1 2 3
+---+---+---+---+
|   ToS   |0|0| (RFC 791, 1981)
+---+---+---+---+
```

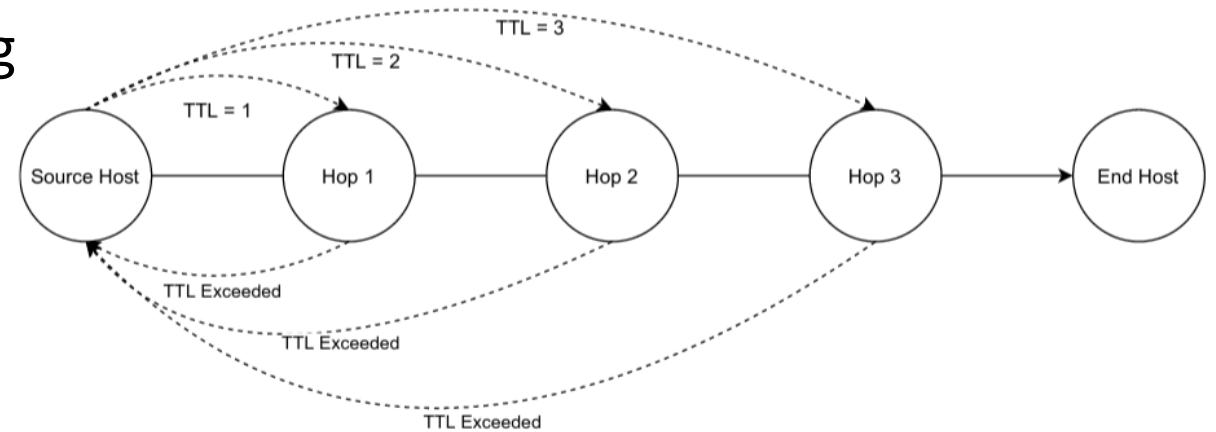
```
 6 7 8 9 0 1 2 3
+---+---+---+---+
|   ToS   |0| (RFC 1349, 1992)
+---+---+---+---+
```

```
 6 7 8 9 0 1 2 3
+---+---+---+---+
|   DSCP   |0|0| (RFC 2474, 1998)
+---+---+---+---+
```

```
 6 7 8 9 0 1 2 3
+---+---+---+---+
|   DSCP   |ECN| (RFC 3168, 2001)
+---+---+---+---+
```

# How do we measure ECN traversal?

- RFC 792 defines ICMP quotations for time exceeded responses
  - IP header + first 8 bytes of originating payload
- Traceroute style utility
  - Path level visibility to ECN field
- May additionally attribute to an Autonomous system



# Aims

- When devices remark packets, where does this happen?
- Are there deployment issues with ECN under Quic?
- Are ECT codepoints equivalent under remarking?
- Do IP versions exhibit different marking behaviours?
- Do Transport protocols influence modifications?

# Methodology

- 3 Host populations (3000 hosts in total)
  - DNS
  - NTP
  - Web servers
- Traceroute style probes under each ECT codepoint, and transport protocol
- Measured from 12 locations
  - AWS EC2 instances
  - Student Volunteers
- Several iterations over two weeks



NTP Servers



DNS resolvers



Web servers

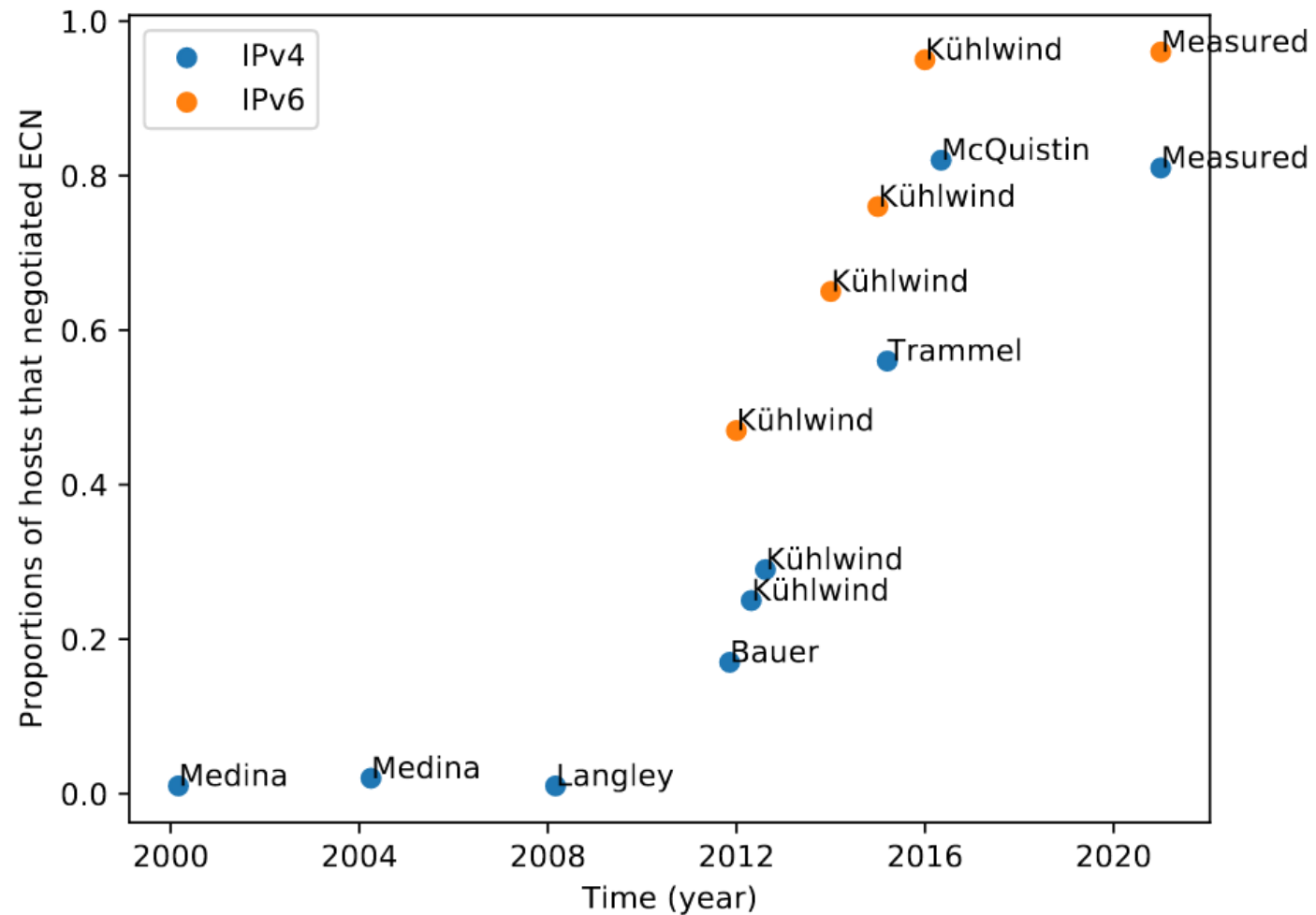
# Implementation

- Network analysis tool  
Implemented in C
- Utilises
  - Isquic by LiteSpeed
  - libpcap
  - libnetfilter\_queue
  - Various aspects of POSIX sockets
- Packer
  - Ubuntu Server 20.4 substrate
  - Distributed to VM locations
- Terraform
  - Deployment configuration as a parameterised terraform module
- Tool scheduled through cron



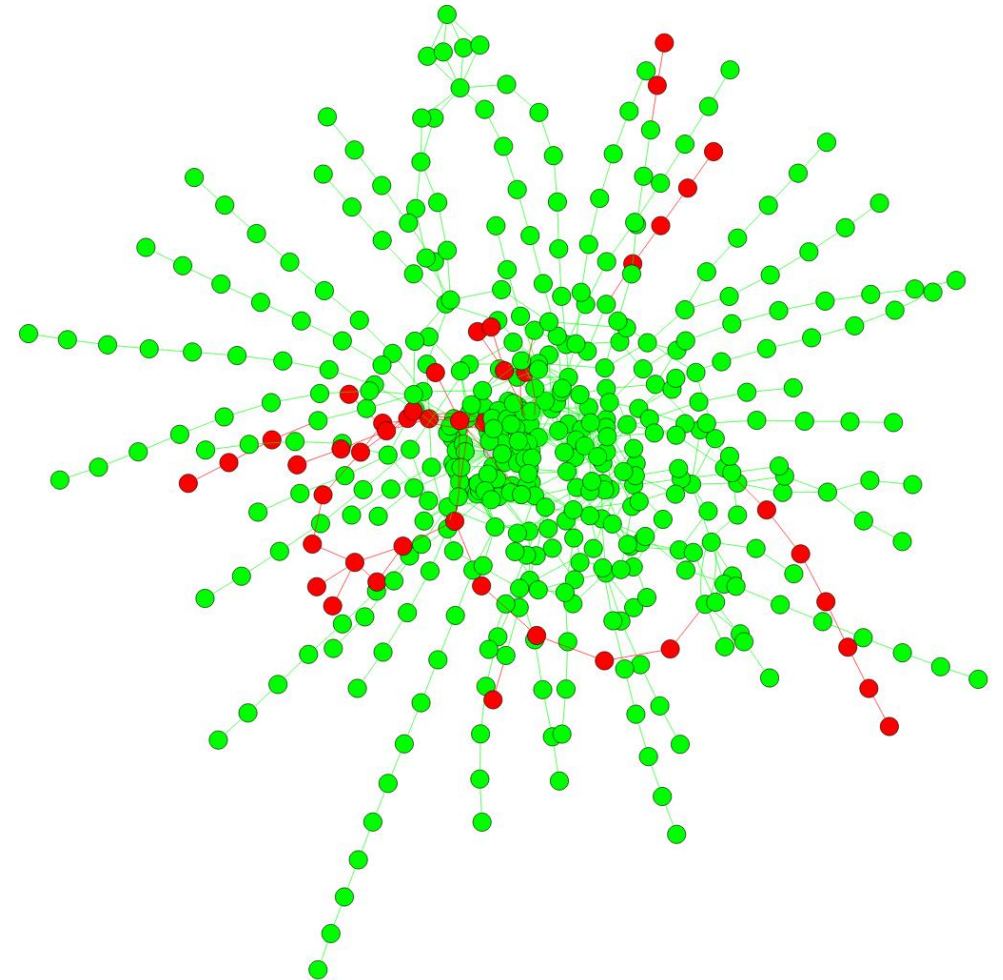
# Trends in ECN adoption

- 96% negotiated ECN under IPv6
- 80% negotiated ECN under IPV4
- Apparent plateau in growth of adoption under IPv4.



# Where is ECN stripped on the network?

- Web servers from Alexa Top Sites
- Traceroute using ECT(0) to hosts
- ICMP responses inspected
- Affects 8% of connections
  - 52% of modifications occurring on AS boundaries, lower than previous works
  - 98.2% of network interfaces pass ECT(0) unmodified
- One measurement location always clears on 1st hop



# ECT Removal Under Quic

- Subset of web servers identified supporting Quic (205 hosts)
- 8.5% connections experience ECT removal
  - Comparable to TCP
  - Generally occurring on AS boundaries
- No specific inhibitors to ECN deployment specific to Quic
  - Although, no hosts negotiated ECN under ietf-draft-29

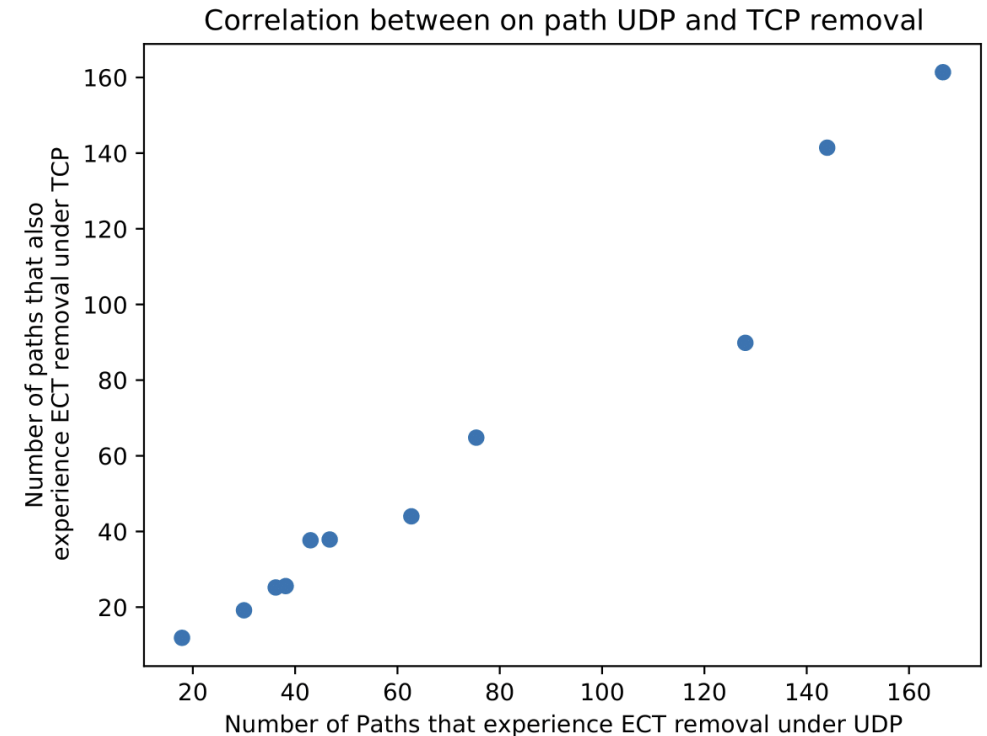
# IP Version Dependant Remarking

- Basic matching employed on web servers identifying dual stack hosts
- Counting paths that experience ECT removal within identified hosts
- IPv4 paths more exposed to destructive ECN remarking
- Under IPv6 DSCP+ECN always set to zero on destructive hop

Host	IPv4	IPv6	Difference
af-south-1	7.75	3.75	4.00
ap-northeast-1	7.14	4.90	2.24
eu-west-2	6.34	4.20	2.14
me-south-1	8.80	2.00	6.80
sa-east-1	7.16	3.33	3.83
us-east-1	18.25	11.5	6.75
us-west-1	14.00	8.85	5.15
Participant-3	7.37	4.25	3.12
Participant-4	8.70	3.25	5.45

# Transport Dependant Remarking

- UDP + TCP probes to DNS resolvers
- 63% of traces indicate removal within the same network hop.
  - 95% of traces within the same AS
- One outlier clearing ECT on all UDP traffic but not TCP.



# ECT Dependant remarking

## **Instances of remarking**

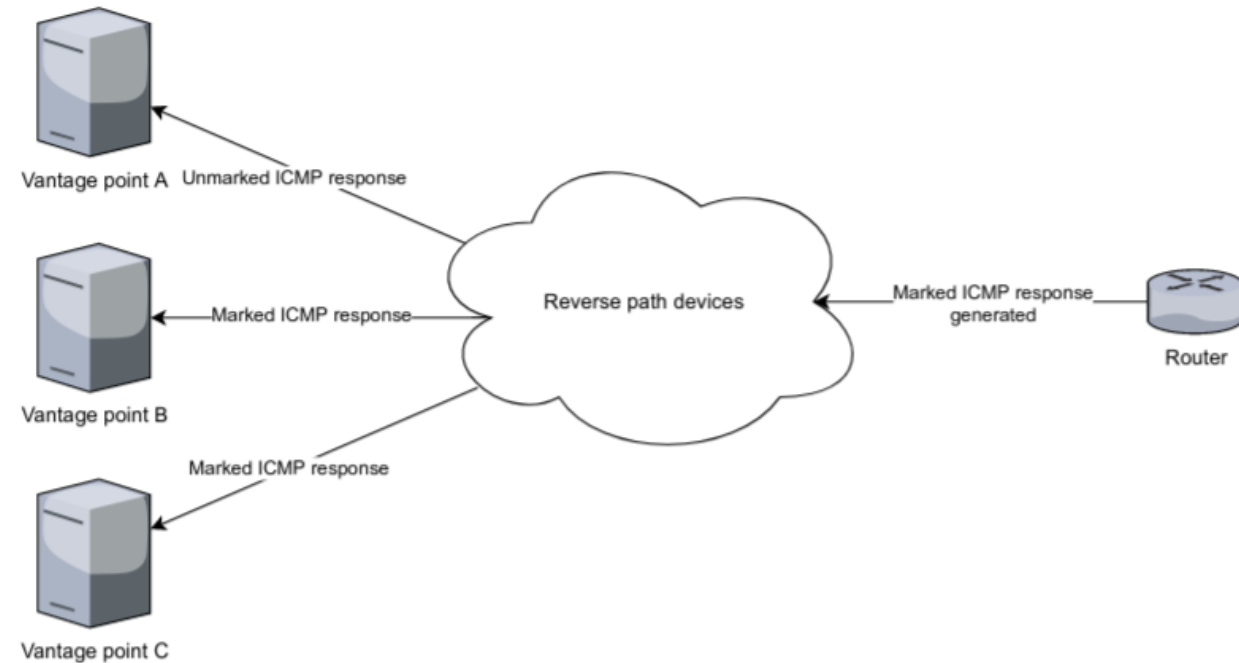
- Collecting ECT(0), ECT(1), CE traces to web servers.
- Around 8% of connections experience removal under each codepoint

## **Remarking behaviour**

- Simple Zeroing DSCP+ECN
- ECN zeroed + changed DSCP
- Partial change of ECT codepoint

# ECN on the reverse path

- Identified that some devices return ECT marked ICMP responses
  - 70% of connections
- RFC 1349 apparent root cause
  - Some ICMP responses should mimic ToS of source packet
- Implications?



# Conclusion

- ECN deployment appears to be plateauing
- ECN remarking more common within IPv4 paths
- Devices generally agnostic of transport substrate
- ECT codepoint does not affect remarking behaviours
- No immediate inhibitors of ECN deployment within Quic