Service Identification Considerations

BEREC Public Technical Workshop on Traffic Identification

Tomas Jakimavicius

Senior Director of Public Policy – Europe, GSMA

12 November 2020

Latest BEREC guidelines support:

- Different speeds/quality for IAS services – equivalent classes of traffic treated equally
- Quality differentiation for specific services where objectively necessary
- Lower quality may be supported to benefit certain services (e.g. low-power IOT)
- Zero-rating following data cap– possibly service-specific (education, .gov resources)

These require service identification

4G Network operation and quality assignment/assurance principles

The following elements allowing to implement quality assignment/assurance functionalities are standardized by 3GPP for 4G - There are different levels:

1 – For the access to the cell (also called “preemption” in case of congestion)

2 – For the access to the bandwidth (idem)

3 – For the flow through service classes that can be implemented to provide services other than IAS with a QOS level distinct from the IAS one.

Level 1: I access the cell
The terminal asks a signaling channel in order to ask for bandwidth (bearer). The parameter “access class” of the IMSI is used: the access classes are defined from 0 to 15. The network when receiving the request form the signalization canal, analyses the access class of the SIM card. In function the network provides the channel or postpone the demand.

Level 2: I ask for a bearer
The terminal will ask for a service. The parameter “ARP” (from 1 – high priority- to 15) is a prioritization at the source. To each service you can associate a different ARP.

Level 3: My flows are prioritized (debit, latency, error rate)
Once the signalization messages are exchanges between the network and the terminal, the service is set up with the associated QOS. The parameter “QCI” is used: service classes are defined by the norm for each usage.

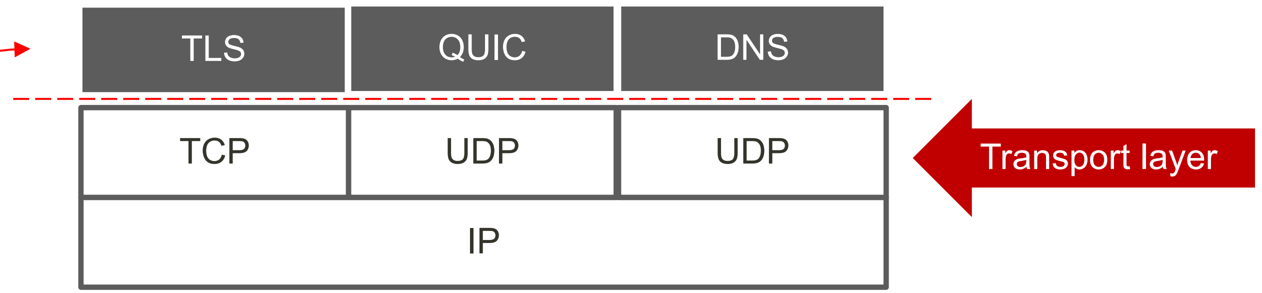
Communication metadata used by the network to identify services

Information	Visibility to network
URL	Low and reducing due to improved Internet security (HTTPS)
Domain	High but will reduce due to encrypted 3rd party DNS and TLS Client Hello
Destination IP address	Very high, but: - Services may change IP subnet due to CDN hosting or to reduce DDoS threat - Ipsec VPNs are likely to become more mainstream
Heuristics (packet size, pacing)	Always, but typically favours identification of large providers

Policy constraints on service identification

- Per latest guidelines, **Transport layer payload** is considered specific content (paras 69/70) and ISPs should not use this data in traffic management

This implies that none of this metadata can be used to identify services – including the domain name



Example of popular Internet protocol stacks

Questions and clarifications

- If the ISP is the DNS resolver, will ISPs be able to use domain names to identify services for (BEREC compliant) traffic management?

- Will ISPs be able to utilise domain names where visible in TLS handshakes to identify services for (BEREC compliant) traffic management?

- QUIC is a payload of the UDP transport protocol. Will ISPs be allowed to utilise the intentional network hint (‘spin bit’*) exposed in QUIC for network latency troubleshooting?

- If service provider adds a DSCP (DiffServ Codepoint) to their IP header requesting a certain traffic management, will ISPs be allowed to act on that with no further identification of the service?

* https://www.ietfjournal.org/enabling-internet-measurement-with-the-quic-spin-bit/

THANK YOU

Tomas Jakimavicius
Senior Director of Public Policy – Europe, GSMA
tjakimavicius@gsma.com
@TJakimavicius