**SA WG2 Meeting #143E S2-200xxxx**

**Feb 24 – Mar 9, 2021, Electronic**

**Source: Futurewei, Vivo ?, Tencent ?, Qualcomm ?, Ericsson**

**Title: Considerations on OS/user overriding operator DNS settings**

**Document for: Agreement**

**Agenda Item: 8.3**

**Work Item / Release: eEdge\_5GC /Rel-17**

***Abstract of the contribution:****This contribution introduces considerations on OS/user overriding operator DNS settings.*

# 1 Discussion

The case that OS/user overrides operator DNS setting is part of the considerations in TR clause 9.1.1. The new text proposed below captures the recommendations and limitations in Annex X.

# 2 Proposal

It is proposed to adopt the following changes into TS23.548.

 **\* \* \* \* 1st Change \* \* \* \***

# Annex X (informative): UE considerations for EAS (re)discovery

## X.1 General

DNS records maybe be cached in the UE by a system wide stub resolver and by application layer name resolution caches. The application (L7) cache is managed on a per application basis while the OS/system DNS cache is common to all applications of a UE network interface. When an application requests IP address resolution for a name, the application’s own name cache is checked first if one exists. If there is no match, the UE interface stub DNS resolver cache is queried. If there is still no cache hit, it results in a DNS query message that gets resolved by the mobile network operator’s DNS cache or further in the DNS hierarchy. These layers of caching have been designed to reduce both the latency of name resolution and load on DNS servers. The multiple layers of DNS cache in the UE and various policies in different implementations have an impact on name resolution when there is a network request to the UE to flush the DNS cache to facilitate EAS re-discovery. The behaviour of UE wide DNS stub resolver and application layer name caches are discussed here.

DNS records obtained from a network resolver contain a time-to-live (TTL) value. This is a hint provided by the network resolver and maybe used to determine the length of time that the record is cached. However, different OS implementations treat the hint differently. While some systems honour the TTL, many others enforce their own policies. For example, one system/OS may implement a policy to hold a DNS record for 2 seconds regardless of the TTL value, while another may hold the record as indicated in TTL value for the DNS record.

Name resolution caches in various applications also have different policies and behaviour. Some applications cache the name records for the length of the application session while others have a time limit. Some applications clear its name cache when the network interface is changed. The network change indication from the OS/ system to the application can be used to clear the application layer name cache for the distributed and multiple anchor modes. Coordination across the 5GC and application domain for name resolver caching behaviour is limited since there is no standard recommendation for application developers.

## X.2 Considerations on OS/UE overriding operator DNS settings

An application or VM in the UE may override operator-provided DNS settings with the aim of end-to-end privacy using 3rd party DoH for DNS and VPNs for securing the data plane. Other applications may perform operations like HTTP prefetch or preconnect operations to improve performance by anticipating what the user will do next. If the OS, user or applications override the operator-provided DNS settings, the DNS resolvers or servers in the third party may take the source IP address of the DNS request as the location information of UE, which may correspond to the local/remote PSA UPF or other entities (e.g., a NAT server) on the N6 interface.

When the DNS server configuration in the OS overrides the operator provided DNS, the DNS queries may still be sent over the correct PDU session for the application if URSP policies and interpretation is implemented by the UE and Network. Such a setup would work if the DNS resolver is using the IP address of the UE or the DNS server as location information. In principle, this does not work with session breakout, since session breakout requires L3/L4 traffic steering policies for the traffic to the selected DNS, and that may only be possible if it is configured in the ULCL in advance by the MNO.

Another potential for DNS override happens when tethering or loosely coupled modems are used. Then the UE/modem must act as a DNS server/proxy to support the dynamics of the edge use-cases. The issues with session breakout regarding flush of DNS-entries applies for session breakout (see X.3 below) and with multiple sessions unless the TTL by the server/proxy in the UE is set to zero. The issues with application internal DNS can’t be handled at all.

## X.3 UE considerations for session breakout

When there is a change of network interface, UE operating systems can provide an indication to notify the application that subscribes to it. In the case of multiple sessions or distributed anchor point connectivity models, the indication of network interface change may be used to flush the application name cache. However, in the session breakout connectivity model, the selection of a new session breakout path does not result in a new network interface at the UE. But, session break out results in a NAS rediscovery message sent by SMF to the UE modem. Thus, unless the operating system can receive this information from the modem and use it to inform the application, there is no indication from the operating system when a new session breakout path is selected and since the application name cache is not cleared, solutions described in 6.x.x, 6.x.y cannot be used as such.

If the NAS rediscovery is not supported in the UE, the anycast addresses can be used, where changes to the session breakout path will result in selection of the “closest” EAS server instance. Also, r application layer redirect to a specific EAS instance may be used when reaching a specific EAS instance if desired by the application.

**\* \* \* \* End of Changes \* \* \* \***