

IKEv2 Link Maximum Atomic Packet and Packet Too Big Notification Extension

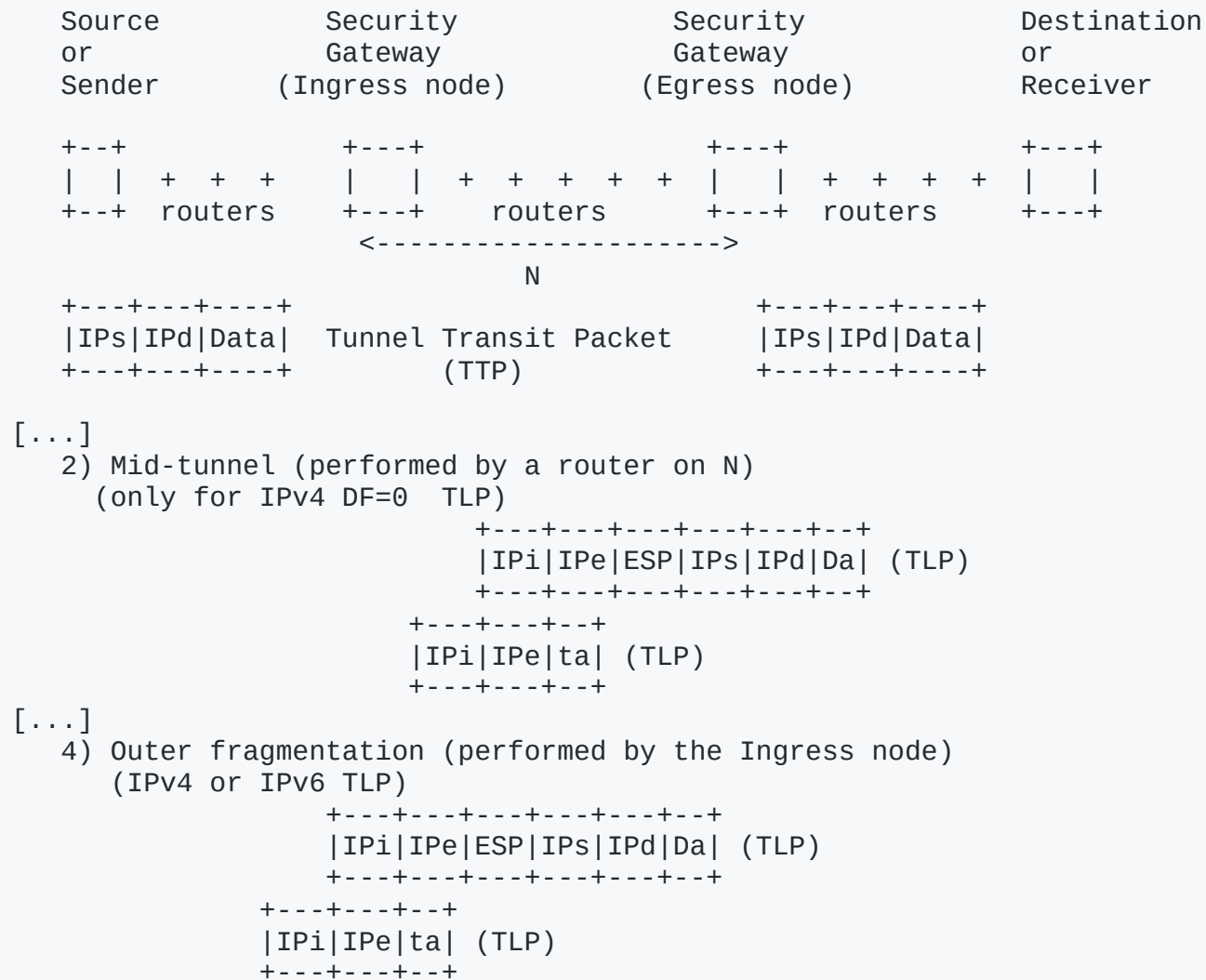
`draft-liu-ipsecme-ikev2-mtu-dect`

Liu, Zhang. Migault

Problem Statement

Fragments reassembling at the egress security gateway requires additional resources which under heavy load results in service degradations.

When Reassembly is observed ?



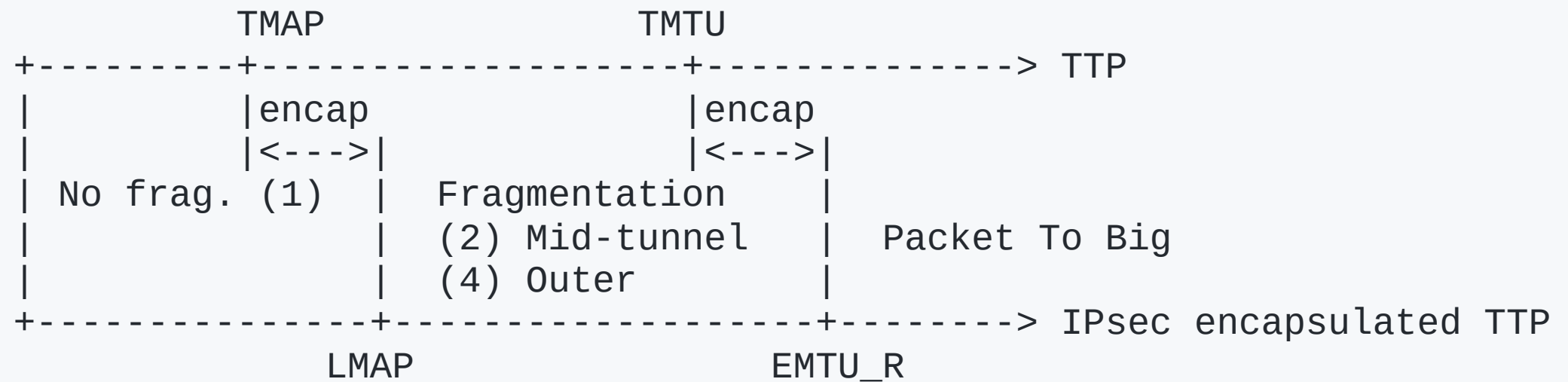
In both cases, the Egress nodes:

1. Reassembles fragments for an IPsec packet

- $\text{fragment} < \text{LMAP}$

2. Processes the reassembled IPsec packet

- $(\text{reassembled}) \text{ IPsec encapsulated TTP} < \text{EMTU_R}$



We define two notification payload:

1. Link Maximum Atomic Packet Notification (LMTA)
 - To inform the Ingress node of the observed LMAP
2. Packet Too Big Notification (PTB)
 - to inform the Ingress node of the EMTU, LMTU

Given LMTA, EMTU_R the Ingress node is able to:

1. Compute the TMAP and TMTU
2. Inform the Source of appropriate TTP size (or perform inner fragmentation)

Illustrative Example (LMAP)

Source or Sender	Security Gateway (Ingress node)	Security Gateway (Egress node)	Destination or Receiver
------------------------	---------------------------------------	--------------------------------------	-------------------------------

+---+	+---+	+---+	+---+
+ + +	+ + + + +	+ + + +	
+---+ routers	+---+ routers	+---+ routers	+---+

<----->

N

- 1) Mid-tunnel (performed by a router on N)
(only for IPv4 DF=0 TLP)

+---+---+---+---+---+
IPi IPE ESP IPs IPd Da (TLP)
+---+---+---+---+---+
+---+---+---+
IPi IPE ta (TLP)
+---+---+---+

- 2) Egress node detects fragmentation
 - a) it collects IPVersion the IP version of the first fragment as well as FragLen, the fragment length
 - b1) If all segment can be reassembled reassemble and the reassembled packet properly decrypted a Link Maximum Atomic Packet Notification (LMAP) is sent.
is sent on the IKEv2 channel
[IKEv2]
<--- N(LMAP [IPVersion, FragLen])

- 3) Upon receiving the LMAP or optionally the ingress node
 - a) Update the TMTU so that the Source performs source fragmentation with TTP packet that are not fragmented.

Source fragmentation
(IPv6 or IPv4)

+---+---+---+
IPs IPd Da (TTP)
+---+---+---+
+---+---+---+
IPs IPd ta
+---+---+---+

Where we are:

We considered ALL received comments with `ietf-intarea-tunnels` terminology,
Generalize the protocol to IPv4 and IPv6, add PTB,...

We implemented it and it solves our issue.

Remaining discussion:

- `ietf-intarea-tunnels` considers the router component - carrying the TTP - and the interface component - handling LTP - independent. Independence of the Tunnel MTU (for TTP) and link layer MTU for (LTP) is provided by performing outer fragmentation when needed.
- [RFC4301] takes another view considers the router component can adapt to the specific needs of the interface component. This is what we do here.

We are looking for adoption

Thanks.