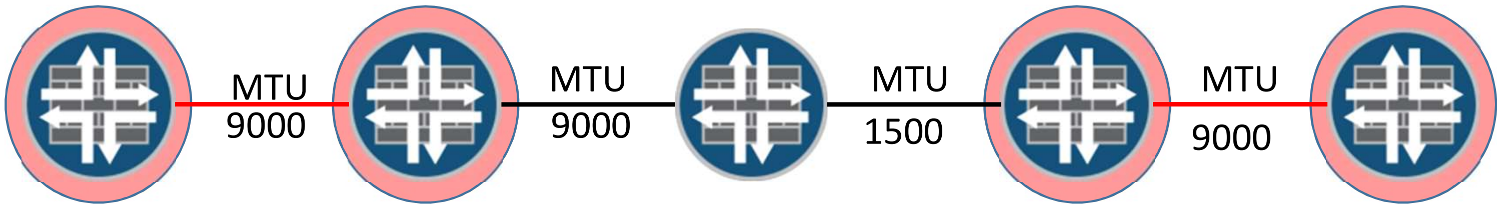
Packetization Layer Path Maximum Transmission Unit Discovery (PLPMTU) For IPsec Tunnels

draft-spiriyath-ipsecme-dynamic-ipsec-pmtu-01

Shibu Piriyath, Umesh Mangla, Nagavenkata Suresh Melam, Ron Bonica

IETF 101

This Is IPSec



MTU 9000

MTU 9000

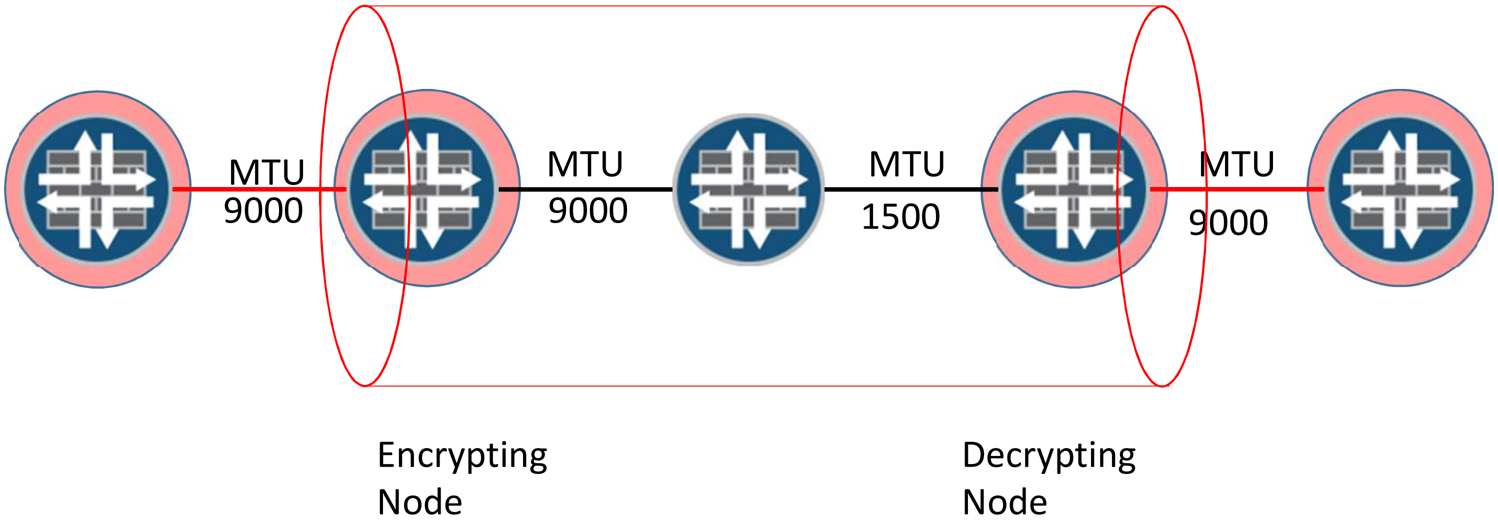
MTU 1500

MTU 9000

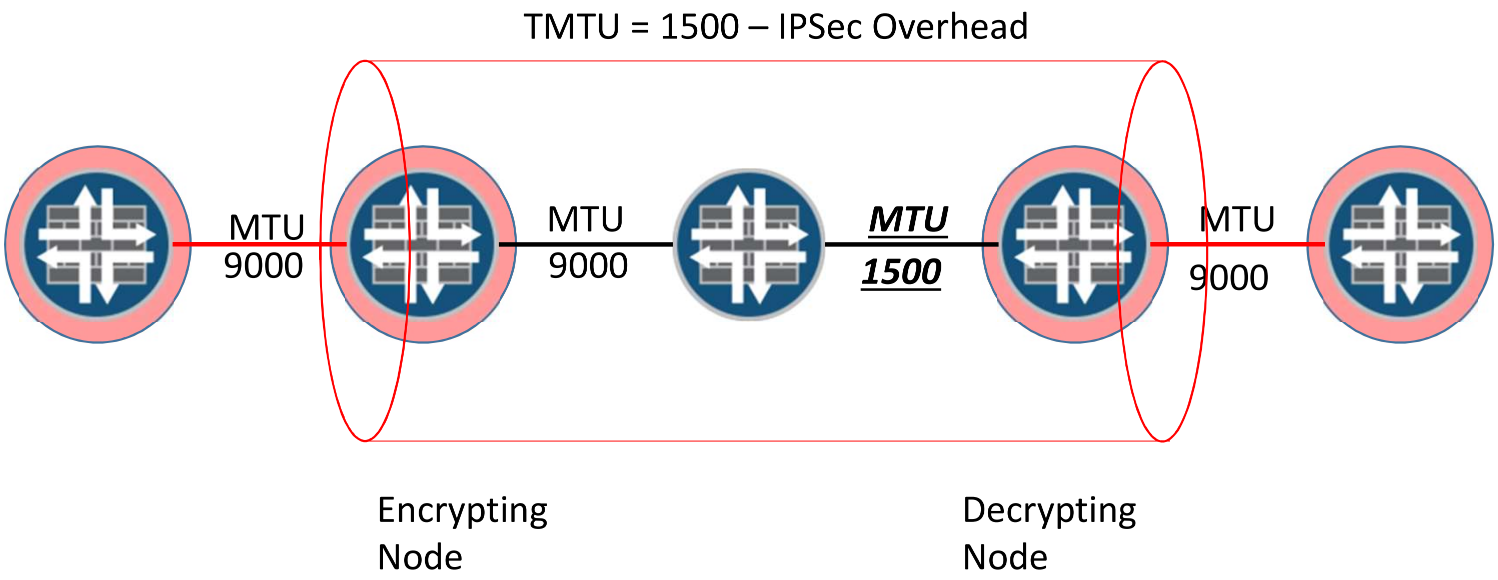
Encrypting
Node

Decrypting
Node

This Is IPSec Tunnel Mode



This Tunnel MTU (TMTU)



When The Encrypting Node Receives A Packet Larger than the TMTU

- Packet can be fragmented
  - That is, IPv4 and DF = 0
  - Options
    - Fragment, encapsulate and forward
    - Encapsulate, fragment and forward
- Packet cannot be fragmented
  - That is, IPv4 and DF = 1 or IPv6
  - Discard packet and send ICMP Packet Too Big to source

Encrypting Node Must Estimate TMTU

- Option1: Static, conservative estimate
  - IPv6: IPv6 minimum link MTU (1280) minus IPSec Overhead
  - IPv4: Value is debatable
- Option 2: Running, less conservative estimate
  - Option 1: Execute Path MTU (PMTUD) procedures
  - Option 2: Execute Packetization Layer Path MTU Discovery (PLMTUD) procedures
    - Described herein

PMTUD

- Initial PMTU estimate
    - Equals MTU of first link along the path to the decrypting mode
- Normal Operation
    - Send non-fragmentable packets through the tunnel
        - Originated by encrypting node
    - Some may be larger than the actual PMTU
- Refining PMTU estimate
    - When a downstream router cannot forward a packet because of its size, it discards the packet and sends an ICMP Packet Too Big (PTB) to the source
    - ICMP PTB indicates MTU of the link through which the packet could not be forwarded
- Tragic flaw
    - ICMP messages are easy to forge

PLPMTUD: Yesterday

- RFC 4821 defines PLPMTUD procedures for TCP
  - But not any other protocols
- Packetizing node (i.e., TCP endpoint)
  - Produces initial TMTU estimate
    - Equal to MTU of first hop along the path to the other endpoint
  - Refines TMTU estimate
    - Sends probe packets of varying sizes to TCP peer
    - Responds to in-band acknowledgments
    - Responds to ICMP Packet Too Big messages
      - If they can be authenticated

PLPMTUD: Today

- Draft-fairhurst-tsvwg-datagram-plpmtud defines
  - PLPMTUD procedures for other transport layer protocols
    - But not IPSec
  - A generic state machine so that PLPMTUD procedures can be applied to other technologies
  - Degrees of freedom granted to other technologies wanting to implement PLPMTUD
- Degrees of Freedom
  - Probe format
  - Acknowledgment format
  - ICMP authentication requirements

PLPMTUD for IPSec: IPv4 Probe Format

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |Version|  IHL  |Type of Service|          Total Length         |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |         Identification        |Flags|      Fragment Offset    |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |  Time to Live |    Protocol   |         Header Checksum       |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
IPv4 |                      Source Address                           |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |                     Destination Address                       |
   - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |           Source Port         |         Dest Port             |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |           UDP Length          |        UDP Checksum           |
 UDP +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |P|                     Reserved                                |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |                                                               |
  |  //                           Padding                           //
  |  |                                                               |
   - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

PLPMTUD for IPSec: IPv6 Probe Format

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |Version| Traffic Class |           Flow Label                  |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |         Payload Length        | Next Header   |   Hop Limit   |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |                                                               |
   |  +                                                               +
   |  |                                                               |
   |  +                     Source Address                            +
IPv6  |                                                               |
   |  +                                                               +
   |  |                                                               |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |                                                               |
   |  +                                                               +
   |  |                                                               |
   |  +                  Destination Address                          +
   |  |                                                               |
   |  +                                                               +
   |  |                                                               |
    - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |           Source Port         |         Dest Port             |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |           UDP Length          |        UDP Checksum           |
 UDP  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |P|                     Reserved                                |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |                                                               |
   |  //                          Padding                             //
   |  |                                                               |
    -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

PLPMTUD for IPSec: IPv4 Ack Format

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |Version|  IHL  |Type of Service|          Total Length         |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |         Identification        |Flags|      Fragment Offset    |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | |  Time to Live |    Protocol   |         Header Checksum       |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
IPv4 |                      Source Address                           |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |                     Destination Address                       |
   - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |           Source Port         |         Dest Port             |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 UDP |           UDP Length          |        UDP Checksum           |
  |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  |P|         Reserved            |       Probe Length            |
   - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

PLPMTUD for IPSec: IPv6 Ack Format

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |Version| Traffic Class |           Flow Label                  |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |         Payload Length        | Next Header   |   Hop Limit   |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |                                                               |
   |  +                                                               +
   |  |                                                               |
   |  +                     Source Address                            +
IPv6  |                                                               |
   |  +                                                               +
   |  |                                                               |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |                                                               |
   |  +                                                               +
   |  |                                                               |
   |  +                  Destination Address                          +
   |  |                                                               |
   |  +                                                               +
   |  |                                                               |
    - +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |           Source Port         |         Dest Port             |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 UDP  |           UDP Length          |        UDP Checksum           |
   |  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  |P|         Reserved            |       Probe Length            |
    -  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ICMP Authentication Requirements

- Ignore all ICMP PTB messages
- They can’t be authenticated to a sufficient degree

Next Steps

- Adopt as WG item