IPv6 Flow Label Specification

Tao ZHENG
Outline

- Introduction
- IPv6 Flow Label Specification
- Flow Labeling Requirements
- Flow state Establishment Requirements
- Security Considerations
- References
Introduction

- **A flow** is a sequence of related packets sent from a source to a unicast, anycast, or multicast destination
  - E.g. transport connections, media streams, but not necessarily 1:1

- **Flow labeling** with the **Flow Label field** enables classification of packets belonging to a specific flow
  - Without the flow label the classifier must use transport next header value and port numbers
    - Less efficient (need to parse the option headers)
    - May be impossible (due to fragmentation or IPsec ESP)
    - Layer violation may hinder introduction of new transport protocols
Introduction

- **Flow state** is established in a subset or all of the IP nodes on the path
  - Includes the *flow classifier*
  - Defines the *flow-specific treatment* the packets should receive
  - Can be signaled, or configured (administratively or manually)
  - Can also be determined algorithmically in some cases (e.g. load spreading)
IPv6 Flow Label Specification

- IPv6 header compared to IPv4 header

IPv6 header:
- Version
- Traffic Class
- Flow Label
- Payload Length
- Next Header
- Hop Limit
- Source Address
- Destination Address

IPv4 header:
- Version
- Header Length
- Type of Service
- Total Length
- Identification
- Flags
- Fragment Offset
- Time to Live
- Protocol
- Header Checksum
- Source Address
- Destination Address
- Options...

shaded fields have no equivalent in the other version

IPv6 header is twice as long (40 bytes) as IPv4 header without options (20 bytes)
IPv6 Flow Label Specification

- A packet is classified to a certain flow by the <Flow Label, Source Address, Destination Address> triplet
  - Allows the same Flow Label value to be used with different destinations
  - Flow state establishment methods may wildcard either of the addresses
  - The Flow Label value is meaningless out of the context of the addresses
  - Non-zero Flow Label value for labeled flows, no other requirements
- The Flow Label value MUST be delivered unchanged to the destination
The IPv6 node assigning a Flow Label value MUST keep track of all the <Flow Label, Source Address, Destination Address> triplets in use

- To prevent mixing separate flows together
- Programming interface needed, but out of scope
  - Three abstract functions defined in the draft

The use of the Flow Label field does not necessarily signal any requirement on packet reordering.

IPv6 nodes not providing flow-specific treatment MUST ignore the field when receiving or forwarding a packet.
Flow Labeling Requirements

- Source nodes SHOULD assign each unrelated transport connection and application data stream to a new flow.
- A source node MUST ensure that it does not unintentionally reuse Flow Label values it is currently using or has recently used when creating new flows.
- The source node MUST provide means for the applications and transport protocols to specify the Flow Label values to be used with their flows.
Flow Labeling Requirements

- the source node SHOULD select new Flow Label values in a well-defined sequence (e.g., sequential or pseudo-random) and use an initial value that avoids reuse of recently used Flow Label values each time the system restarts.
Flow state Establishment Requirements

- The methods are out of scope
  - But some rules needed to enable co-existence of different methods in IPv6 nodes
- MUST provide the means for flow state clean-up
  E.g. Soft state/hard state
- Flow state establishment methods MUST be able to recover from the case where the requested flow state cannot be supported.
Security Considerations

- Theft and Denial of Service
- IPsec and Tunneling Interactions
- Security Filtering Interactions
Theft and Denial of Service

- An adversary may be able to obtain better service by modifying the IPv6 header or by injecting packets with false addresses and/or labels.
- Treatment of IP headers by nodes is typically unverified.
Theft and Denial of Service

- There are two issues with different properties
  - Spoofing of the Flow Label
  - Spoofing of the whole 3-tuple
- Only applications with an appropriate privilege in a sending host will be entitled to set a non-zero Flow Label.
IPsec and Tunneling Interactions

- modification of the Flow Label by a network node has no effect on IPsec end-to-end security
- IPsec tunnel mode provides security for the encapsulated IP header's Flow Label.
The Flow Label does nothing to eliminate the need for packet filtering based on headers past the IP header, if such filtering is deemed necessary for security reasons on nodes such as firewalls or filtering routers.
Reference