

Traceback using IPv6 flowlabel

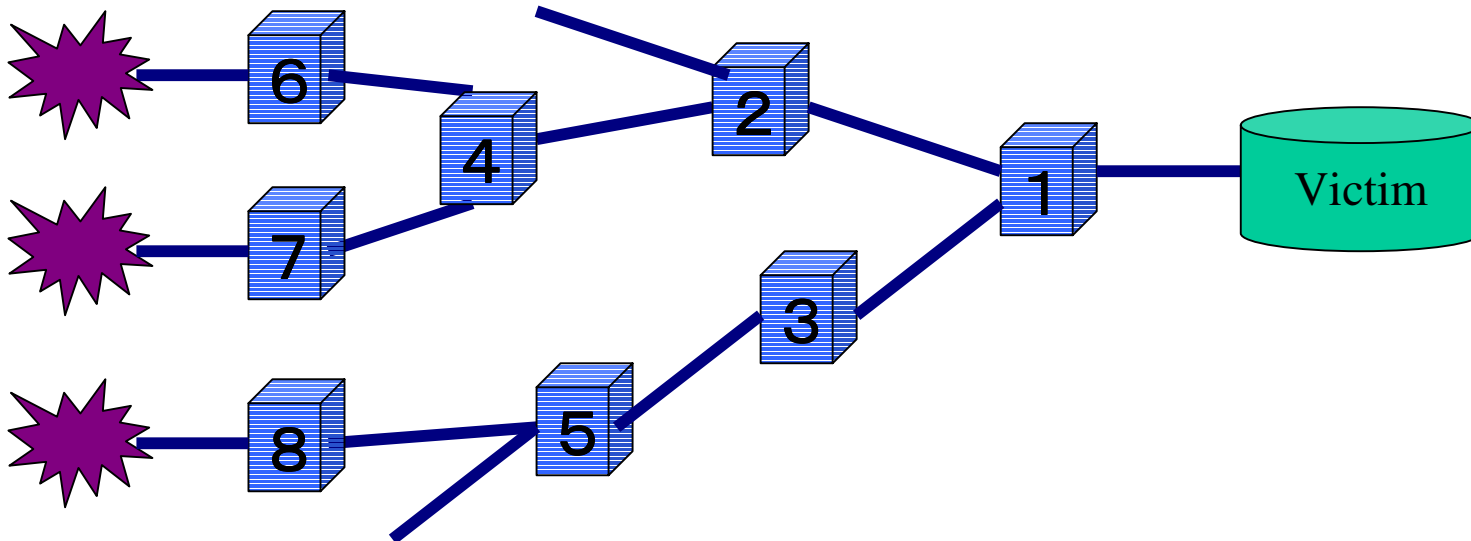
NARA Institute Science and Technology
Masafumi OE <masa@fumi.org>

What is this?

- Traceback using IPv6 flowlabel and ICMP.
 - For making attack paths(traceback), use Flowlabel
 - For constructing more actual attack paths, use ICMP
- Flowlabel(20bit) has
 - IPv6 address on the previous hop and the current hop
 - Distance from marking router.
- Proposal paper
<http://iplab.aist-nara.ac.jp/research/itrace/>

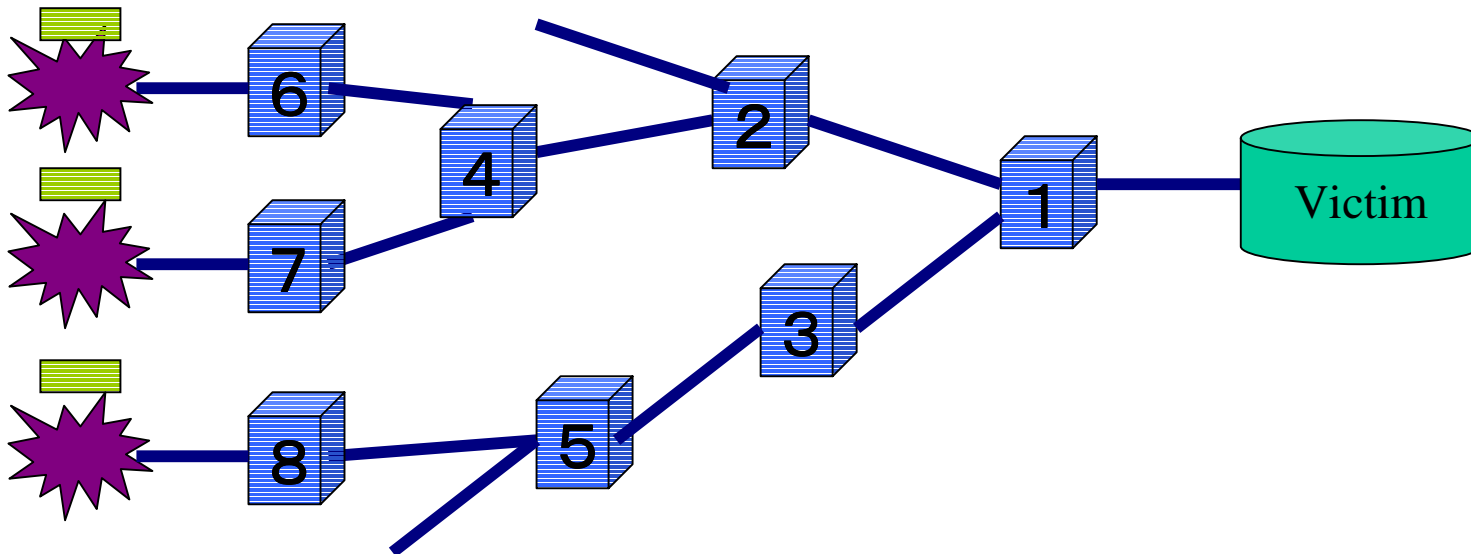
Marking

- Router mark a passing router information into flowlabel
- Victim make attack paths from received flowlabels.



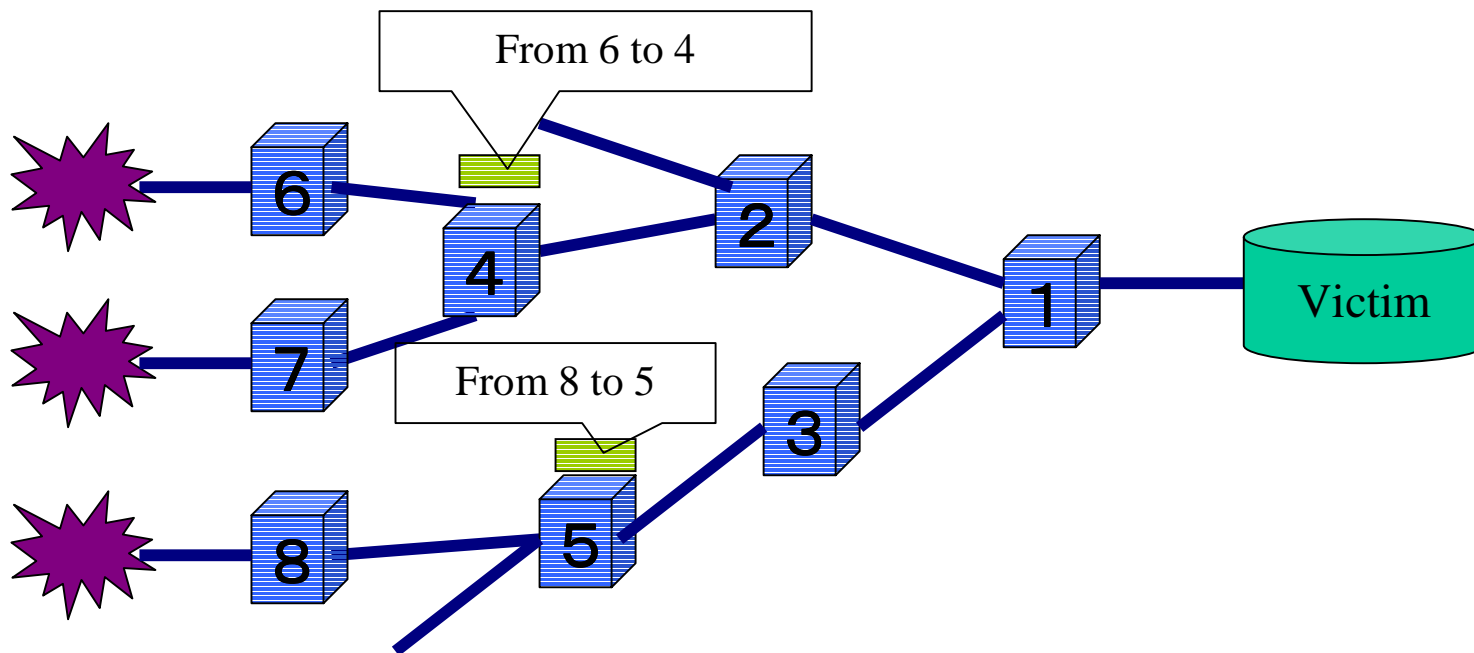
Marking

- Router mark a passing router information into flowlabel
- Victim make attack paths from received flowlabels.



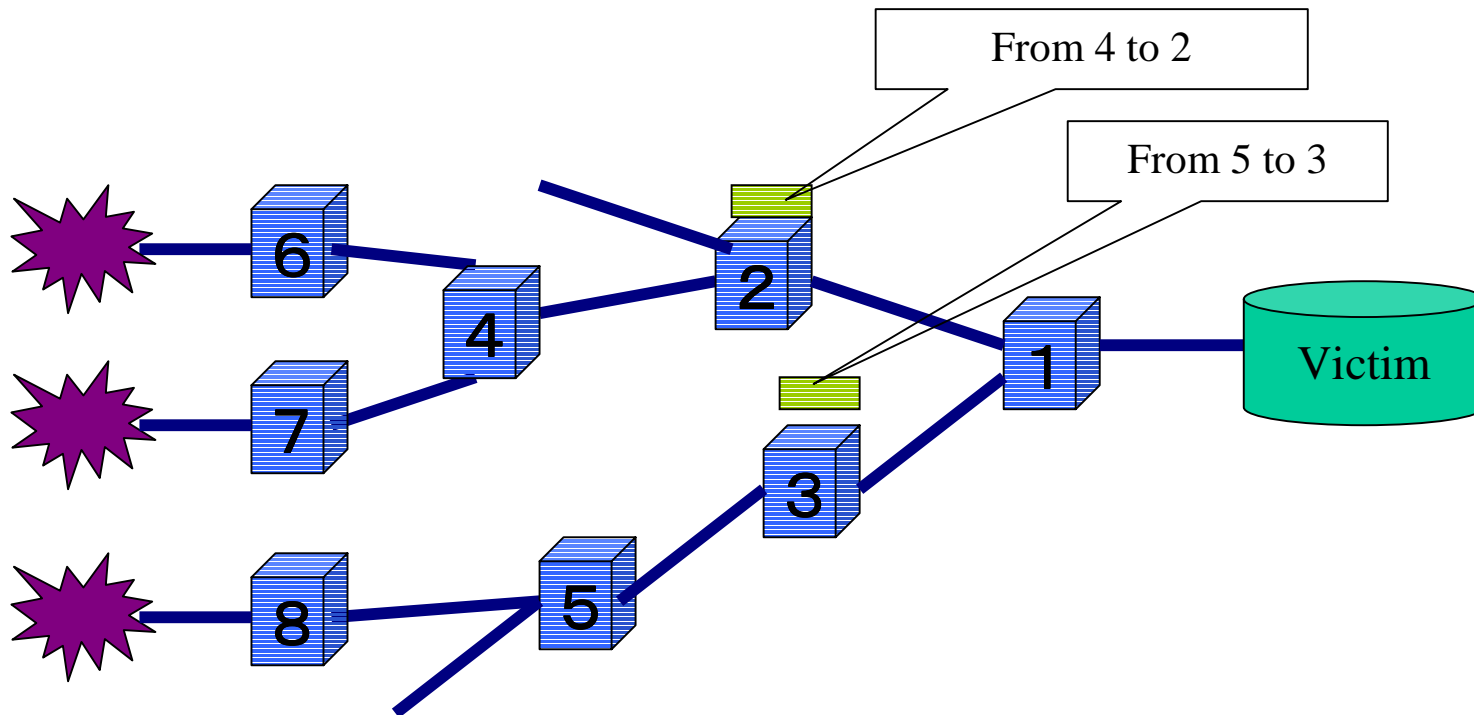
Marking

- Router mark a passing router information into flowlabel
- Victim make attack paths from received flowlabels.



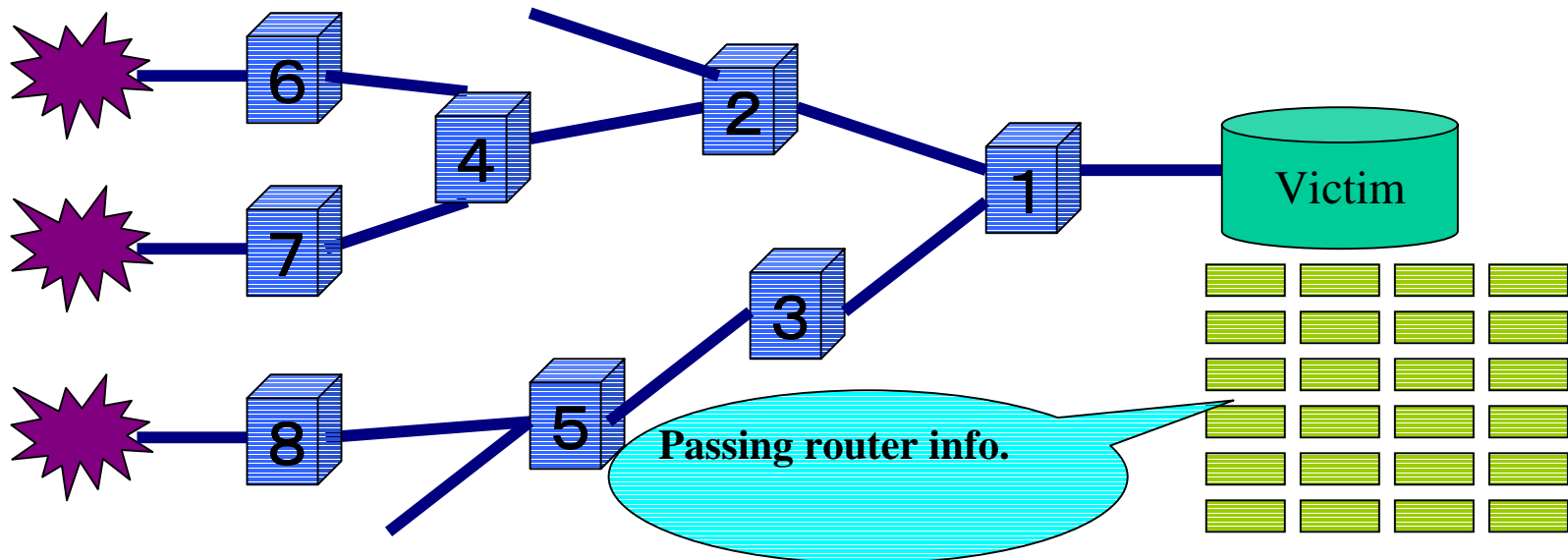
Marking

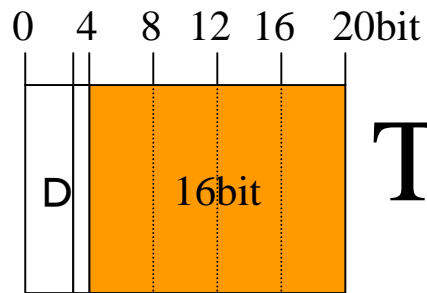
- Router mark a passing router information into flowlabel
- Victim make attack paths from received flowlabels.



Marking

- Router mark a passing router information into flowlabel
- Victim make attack paths from received flowlabels.





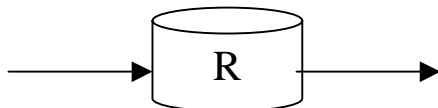
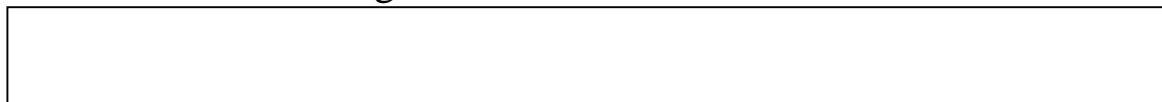
Traceback message field

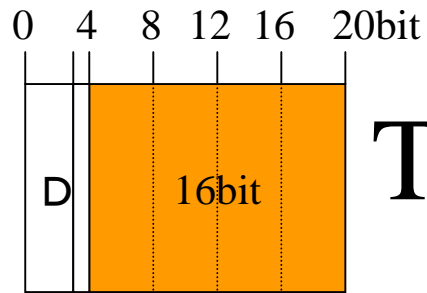
Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.

SHIFT 1bit →

Passing router information 256bit

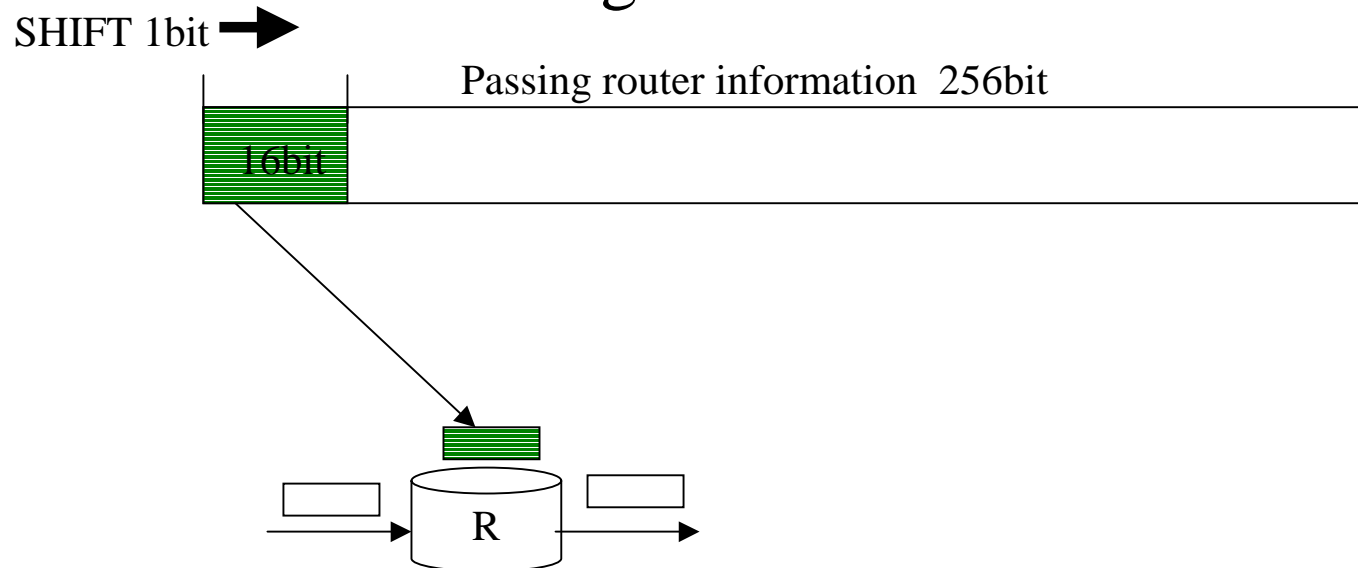


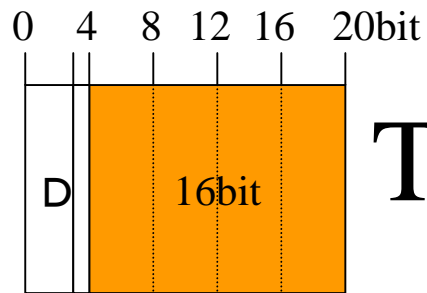


Traceback message field

Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.



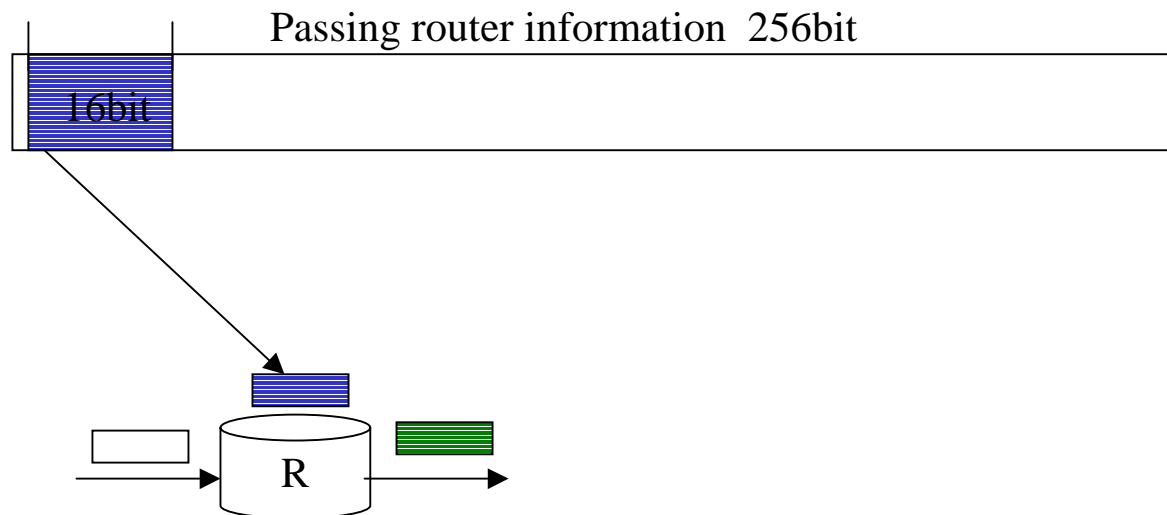


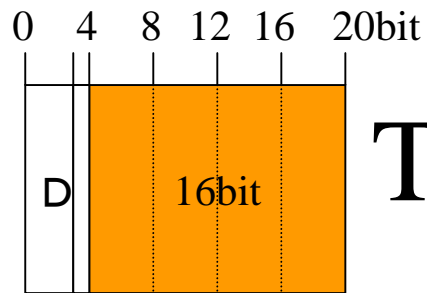
Traceback message field

Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.

SHIFT 1bit →



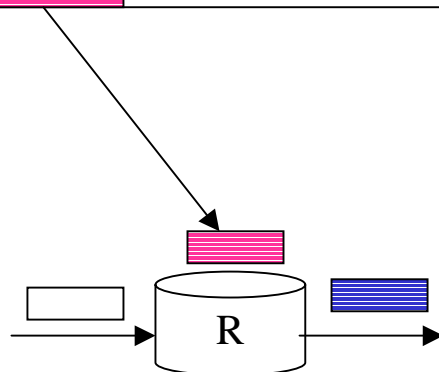
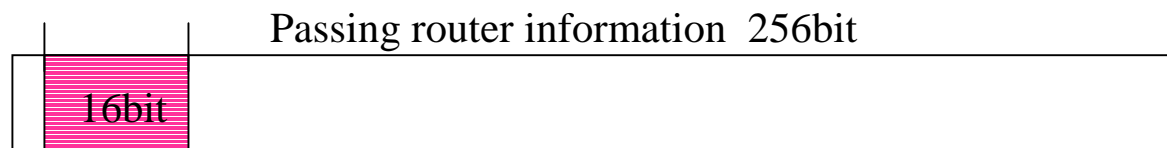


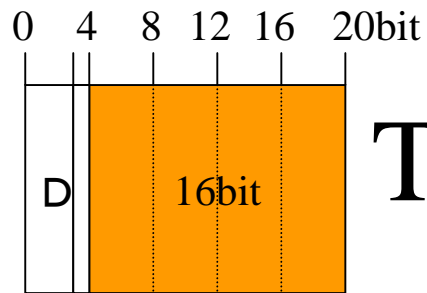
Traceback message field

Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.

SHIFT 1bit →



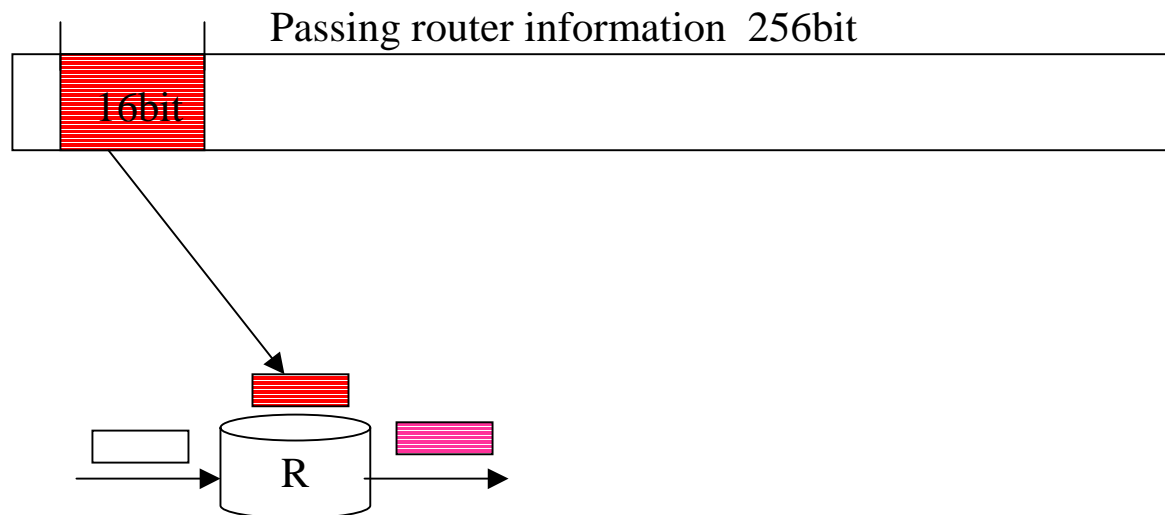


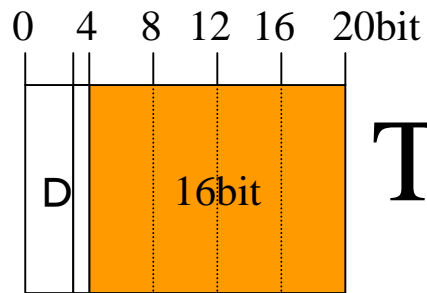
Traceback message field

Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.

SHIFT 1bit →

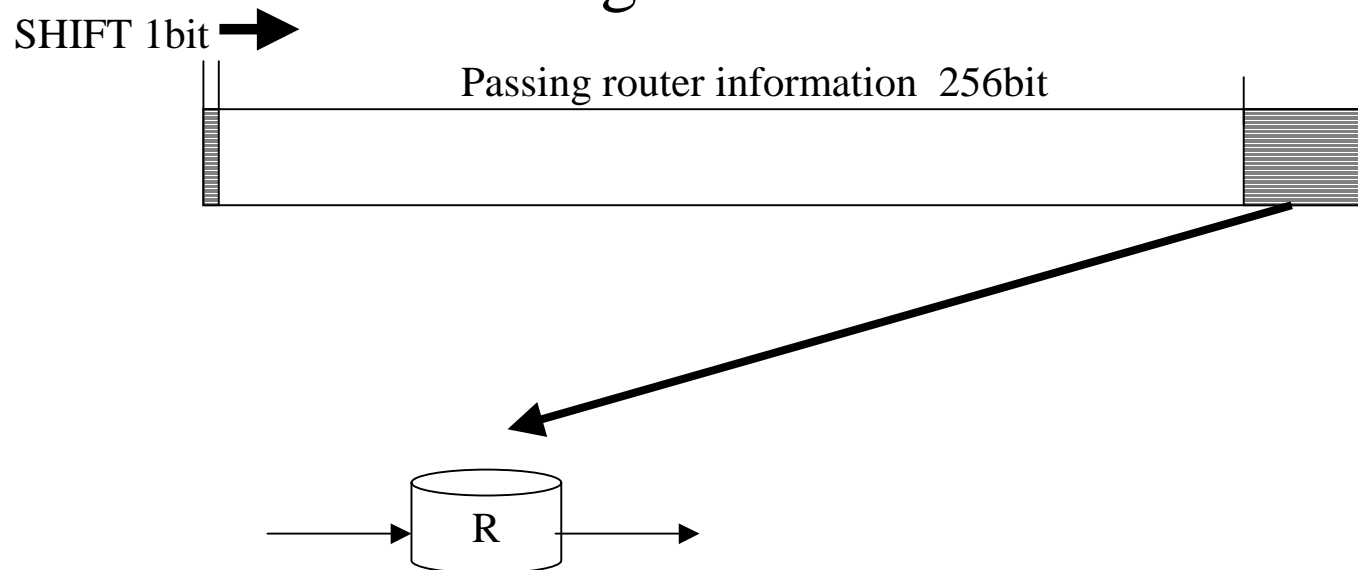


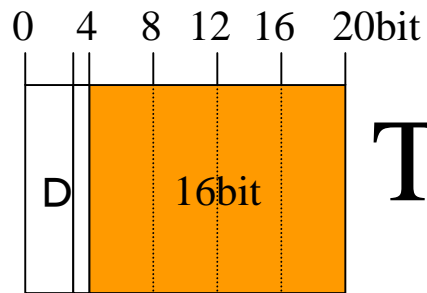


Traceback message field

Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.

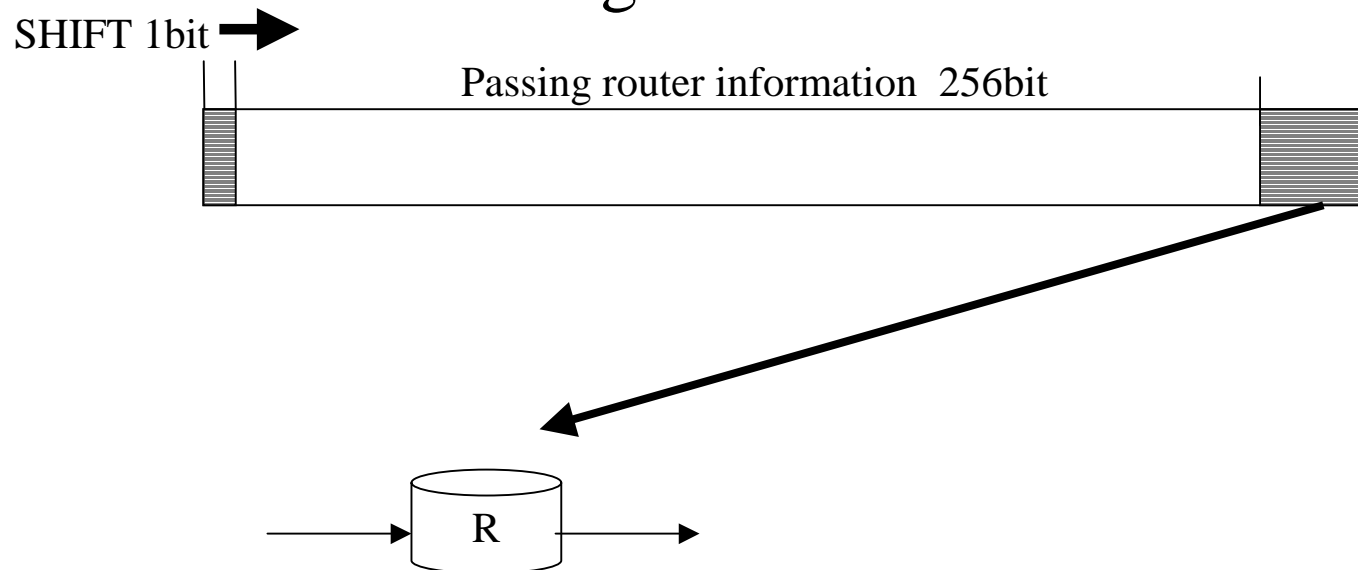


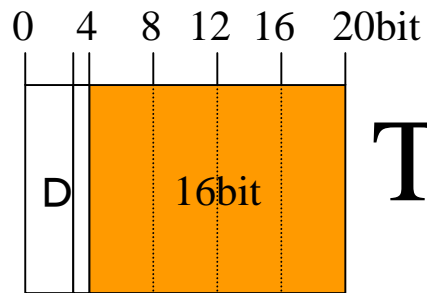


Traceback message field

Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.

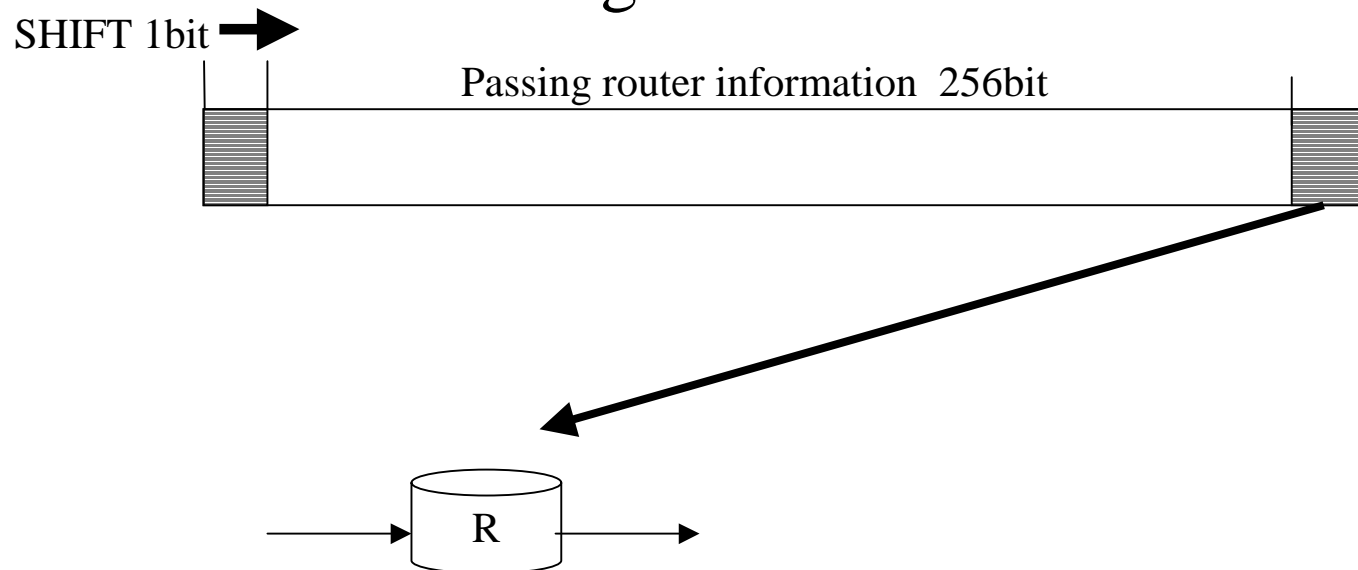


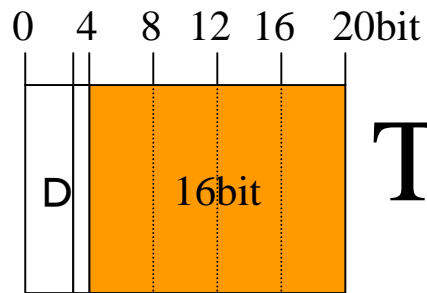


Traceback message field

Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.

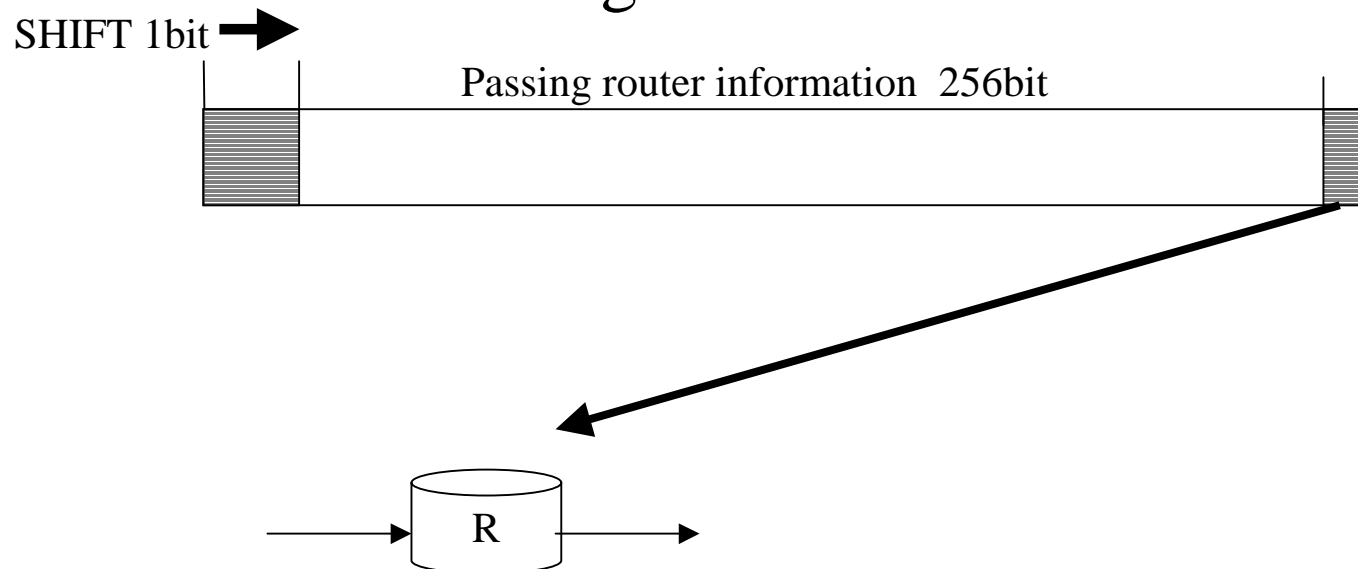


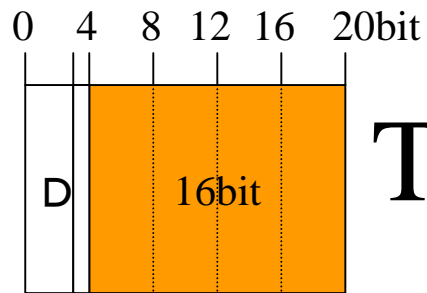


Traceback message field

Traceback message field is using for sending a passing router information to destination node.

Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.

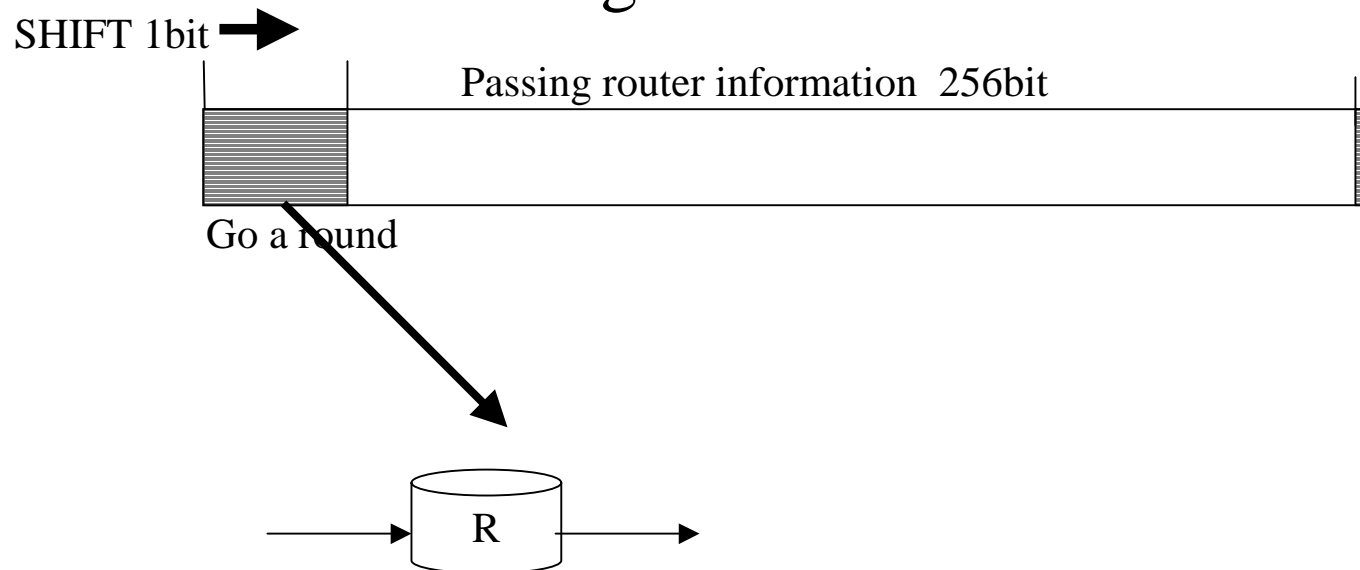




Traceback message field

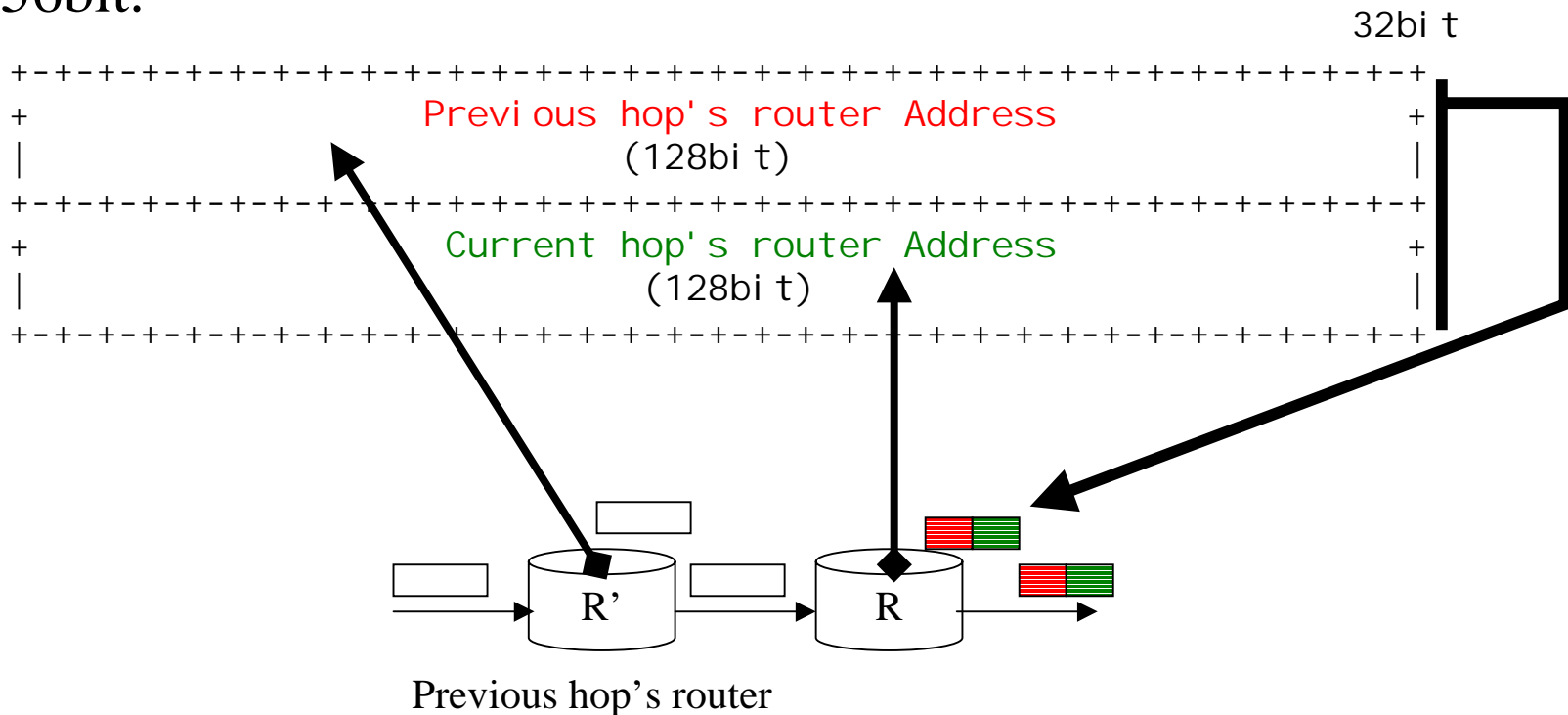
Traceback message field is using for sending a passing router information to destination node.

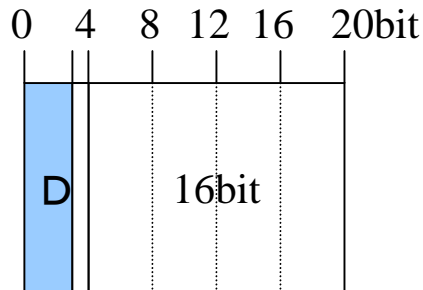
Passing router information is fragmented into 128 pieces of Traceback message(16bit) using 16bit window shifting 1bit.



Passing router information

Passing router information is constructed previous hop's router address and own router address and the size of this is 256bit.



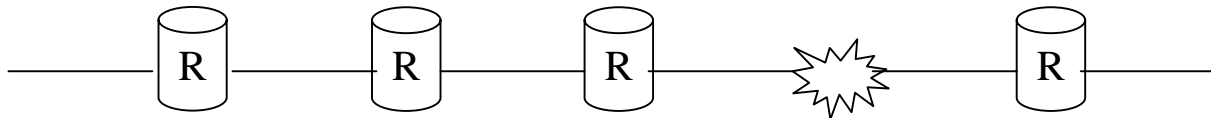


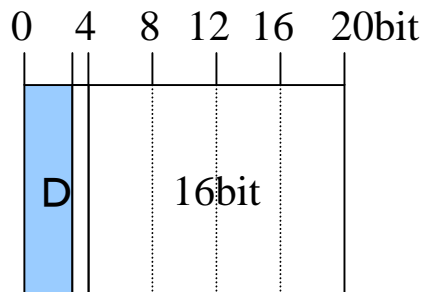
Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.

IP FlowLabel

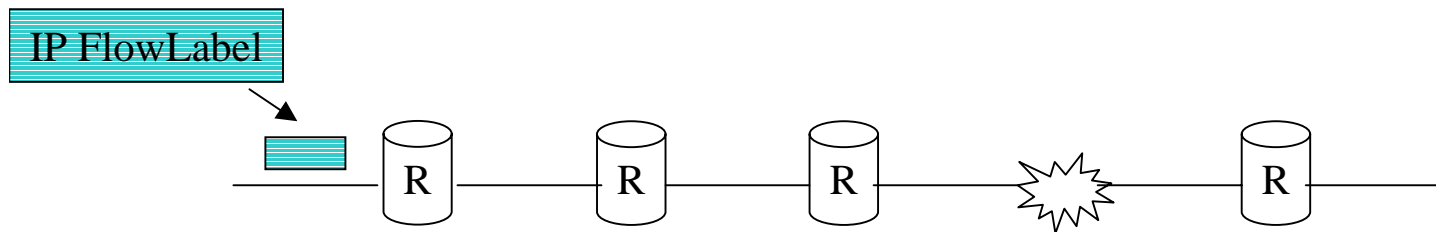


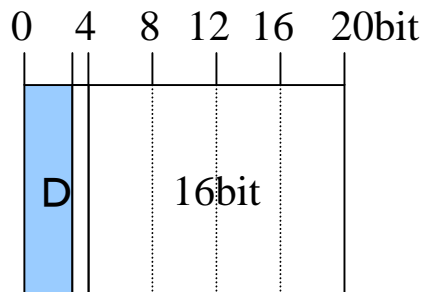


Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.

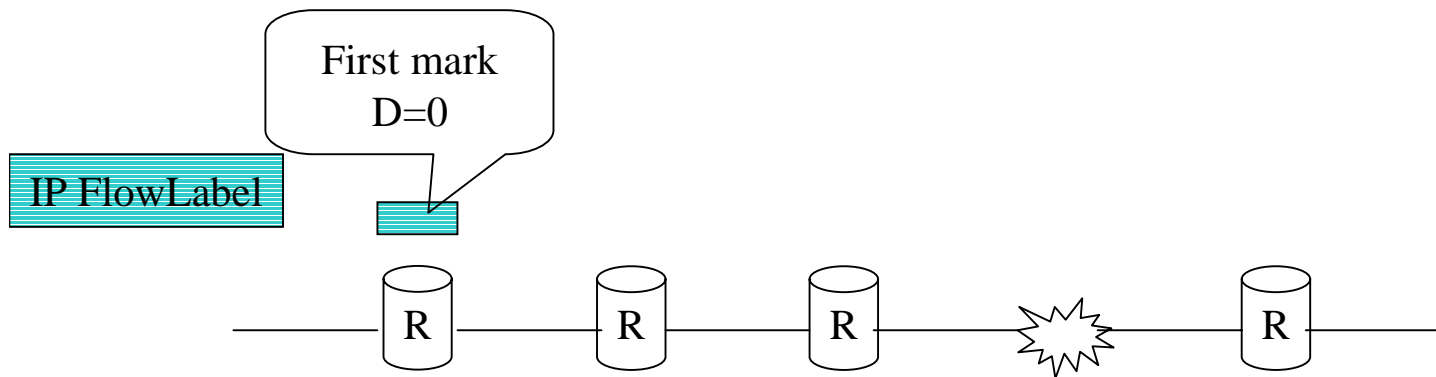


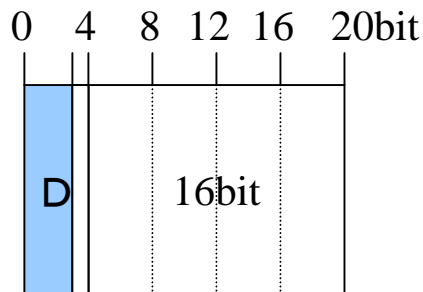


Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.



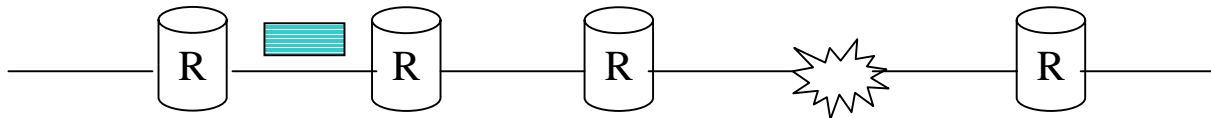


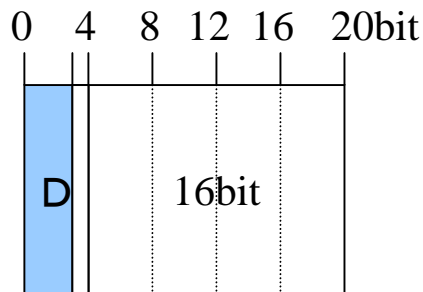
Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.

IP FlowLabel

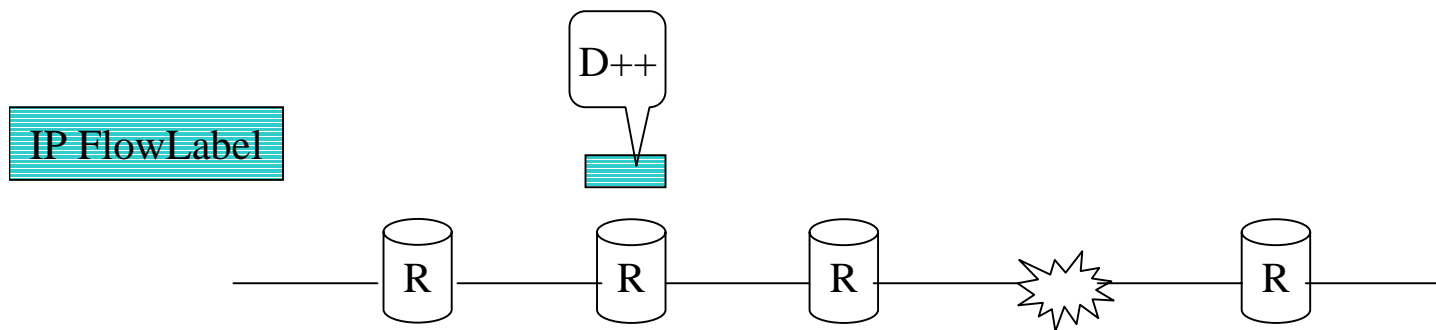


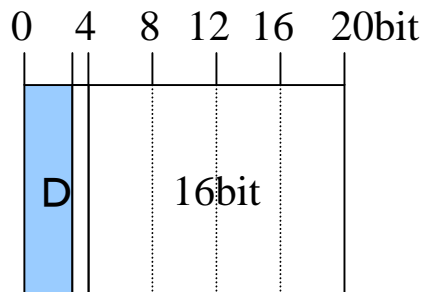


Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.



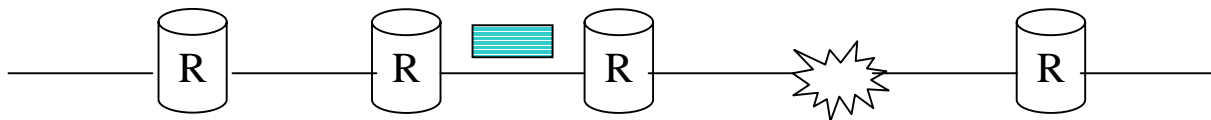


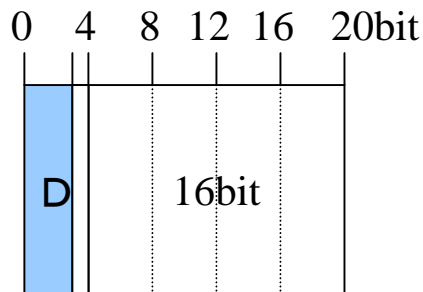
Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.

IP FlowLabel

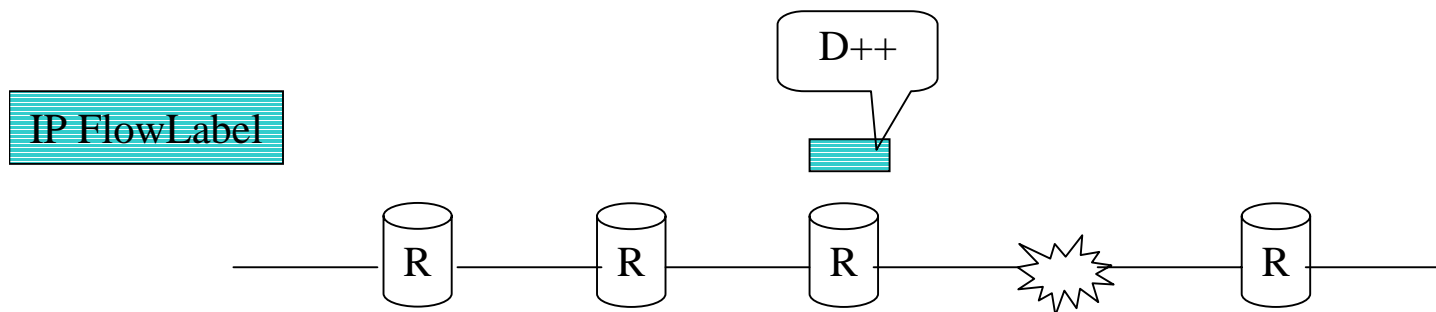


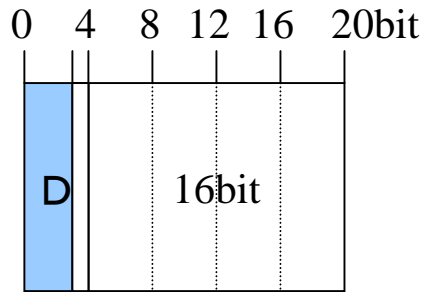


Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.

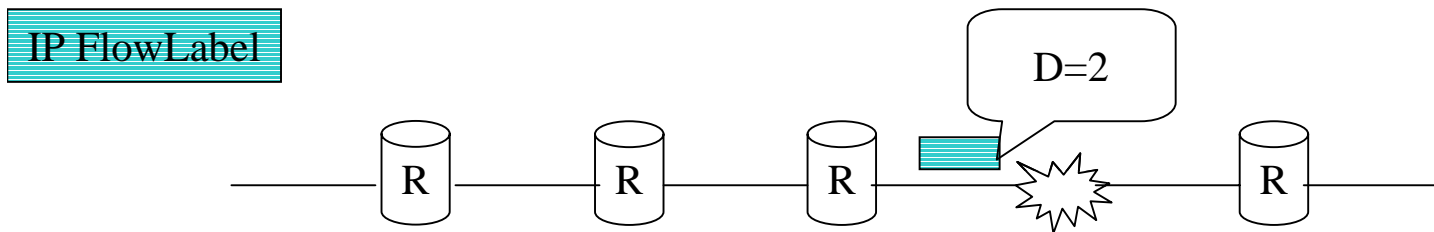


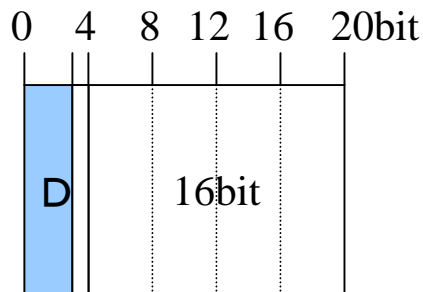


Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.



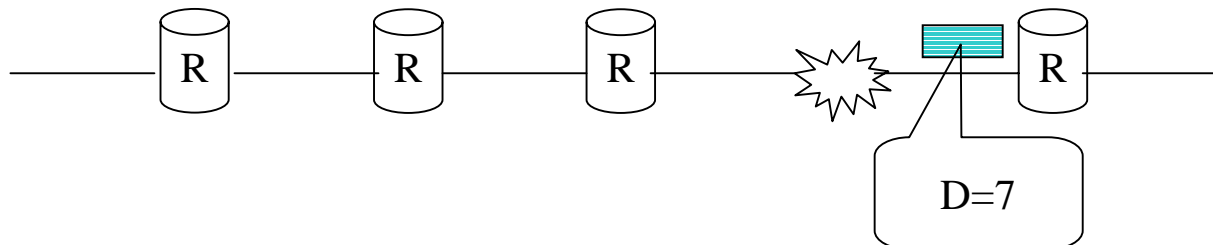


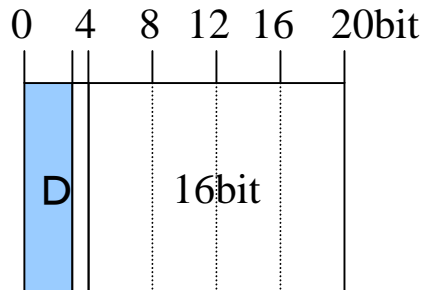
Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.

IP FlowLabel

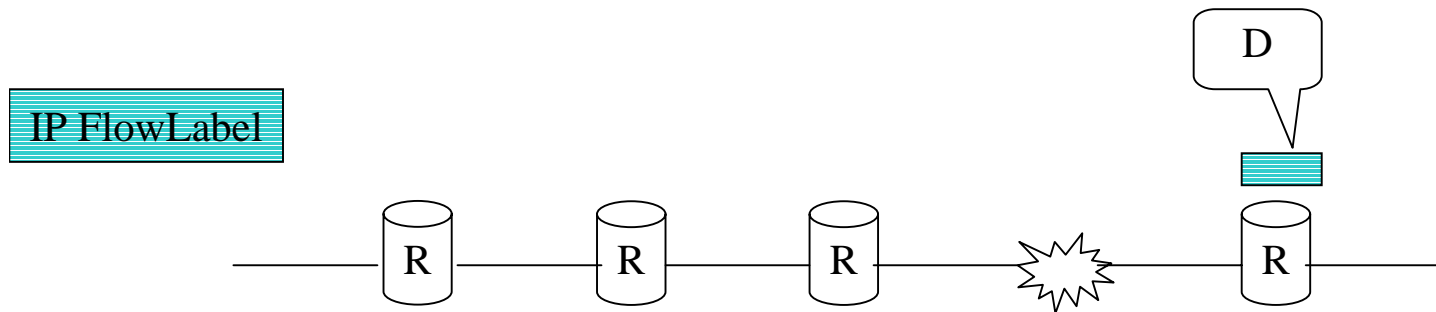


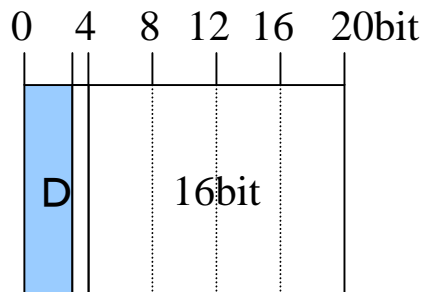


Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.

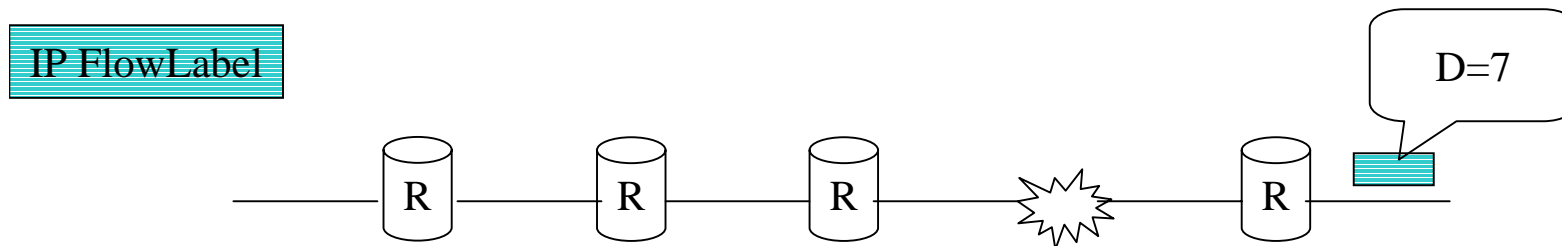




Distance field

Distance field indicates hop counts from first marked router and is increased by each passing routers.

When value for the distance field becomes seven(111), the router must not add.



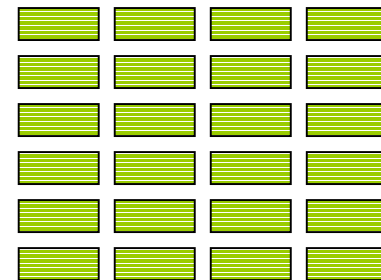
Making an attack path

Victim make an attack path from “set of passige router”



Making an attack path

Victim make an attack path from “set of passige router”



Making an attack path

Victim make an attack path from “set of passage router”



Distance 1: 2→1 3→1

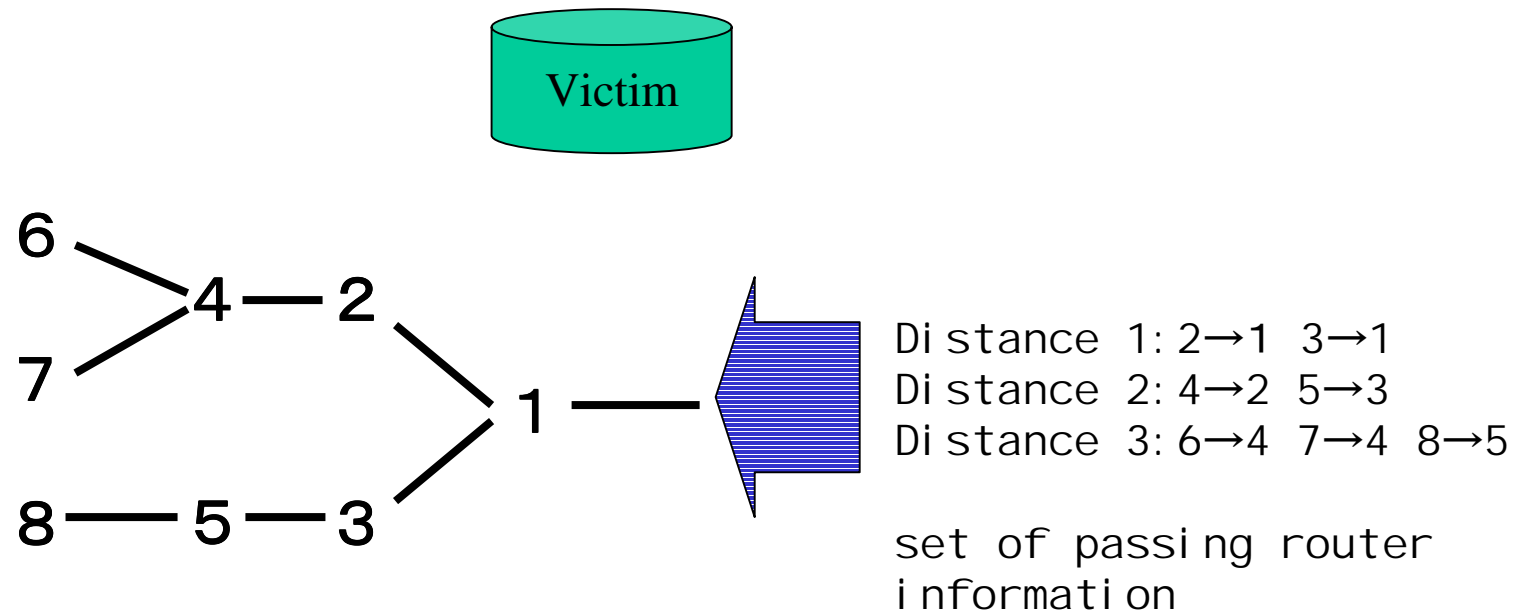
Distance 2: 4→2 5→3

Distance 3: 6→4 7→4 8→5

set of passing router
information

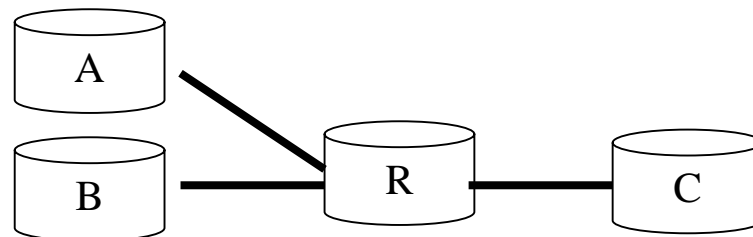
Making an attack path

Victim make an attack path from “set of passage router”



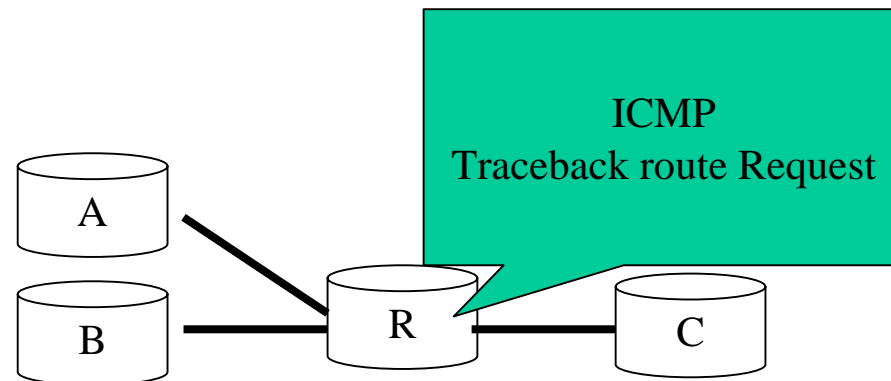
ICMP Traceback route message

- Attack path making from Traceback messages might not be correct for illegal Flowlabel made by attackers.
- ICMP Traceback route request is used to look up entry of passing router information.



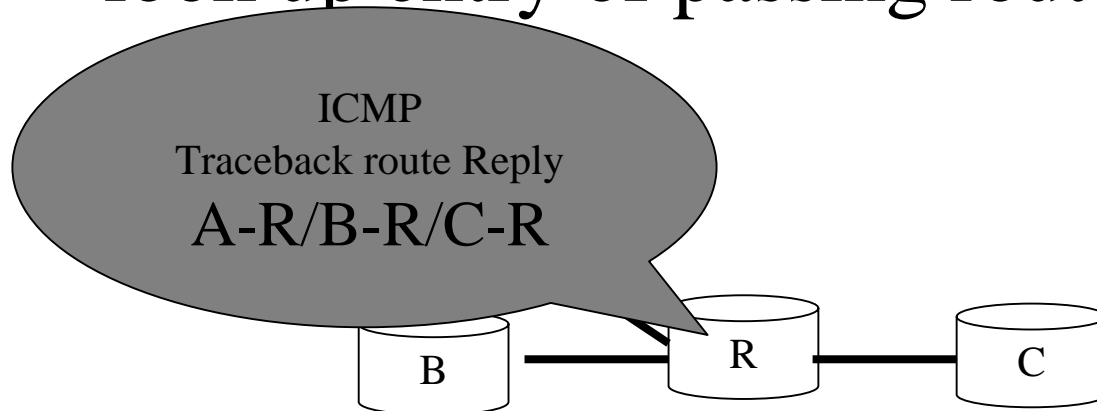
ICMP Traceback route message

- Attack path making from Traceback messages might not be correct for illegal Flowlabel made by attackers.
- ICMP Traceback route request is used to look up entry of passing router information.



ICMP Traceback route message

- Attack path making from Traceback messages might not be correct for illegal Flowlabel made by attackers.
- ICMP Traceback route request is used to look up entry of passing router information.



ICMP Traceback route message(2)

- From the reply message, the victim can exclude the pair which does not exist. So, Victim is able to make more accurate attack paths

Distance 1: 2→1 3→1 6-9

Distance 2: 4→2 5→3 3-9

Distance 3: 6→4 7→4 8→5

set of passing router
information

ICMP Traceback route message(2)

- From the reply message, the victim can exclude the pair which does not exist. So, Victim is able to make more accurate attack paths

Distance 1: 2→1 3→1 6-9

Distance 2: 4→2 5→3 3-9

Distance 3: 6→4 7→4 8→5

ICMP TRACEBACK ROUTE REQUEST/REPLY

set of passing router
information

ICMP Traceback route message(2)

- From the reply message, the victim can exclude the pair which does not exist. So, Victim is able to make more accurate attack paths

Distance 1: 2→1 3→1 ~~6→9~~
Distance 2: 4→2 5→3 ~~3→9~~
Distance 3: 6→4 7→4 8→5

set of passing router
information

What do next?

- We will make the implementations of this proposal on KAME.
- Update this proposal.
- Try on WIDE-6bone and report results of this at 51th IETF.