Consideration on OSPF LSDB Monitoring

draft-ohara-ospf-lsdb-monitoring-consideration-01

IETF81

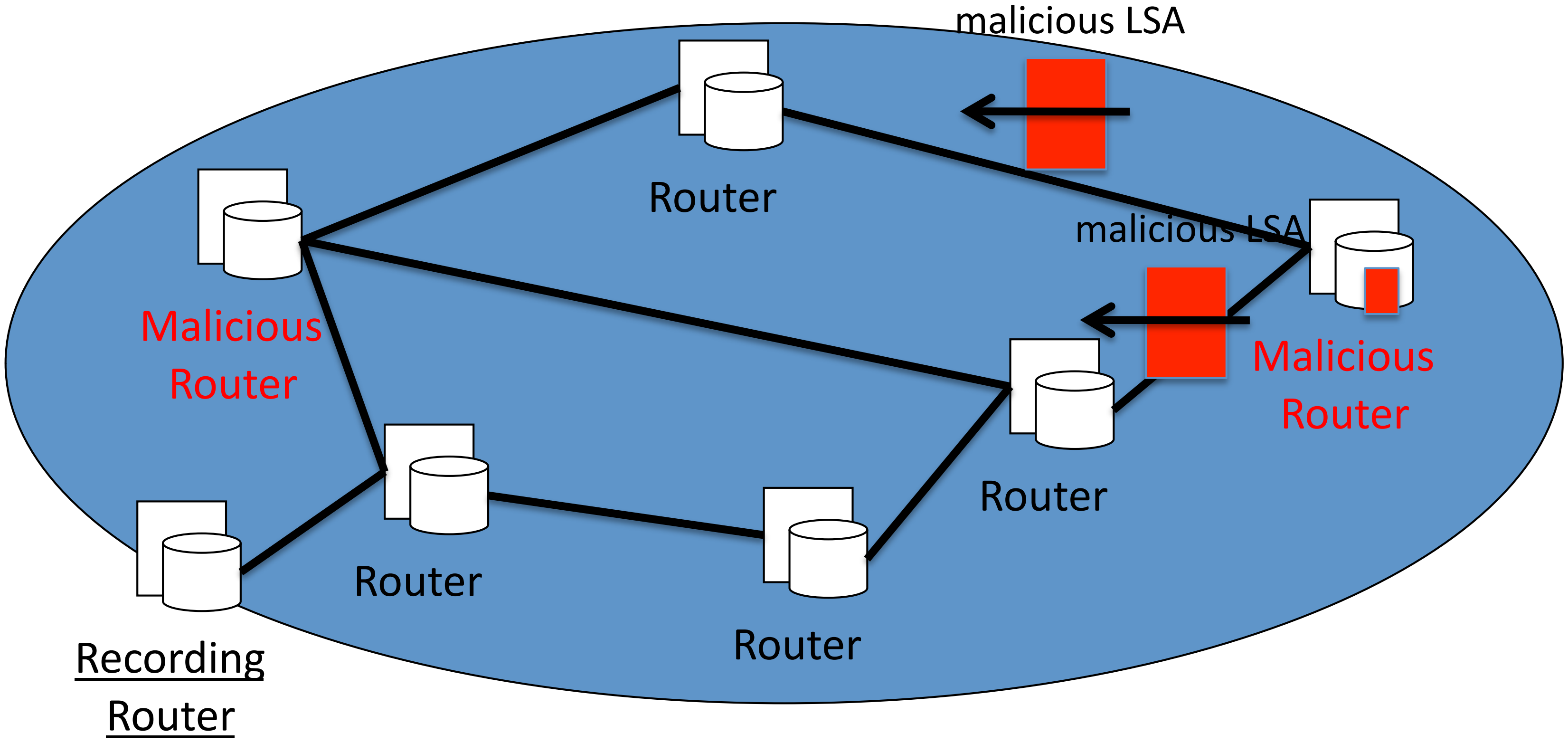
yasu@jaist.ac.jp

Summary

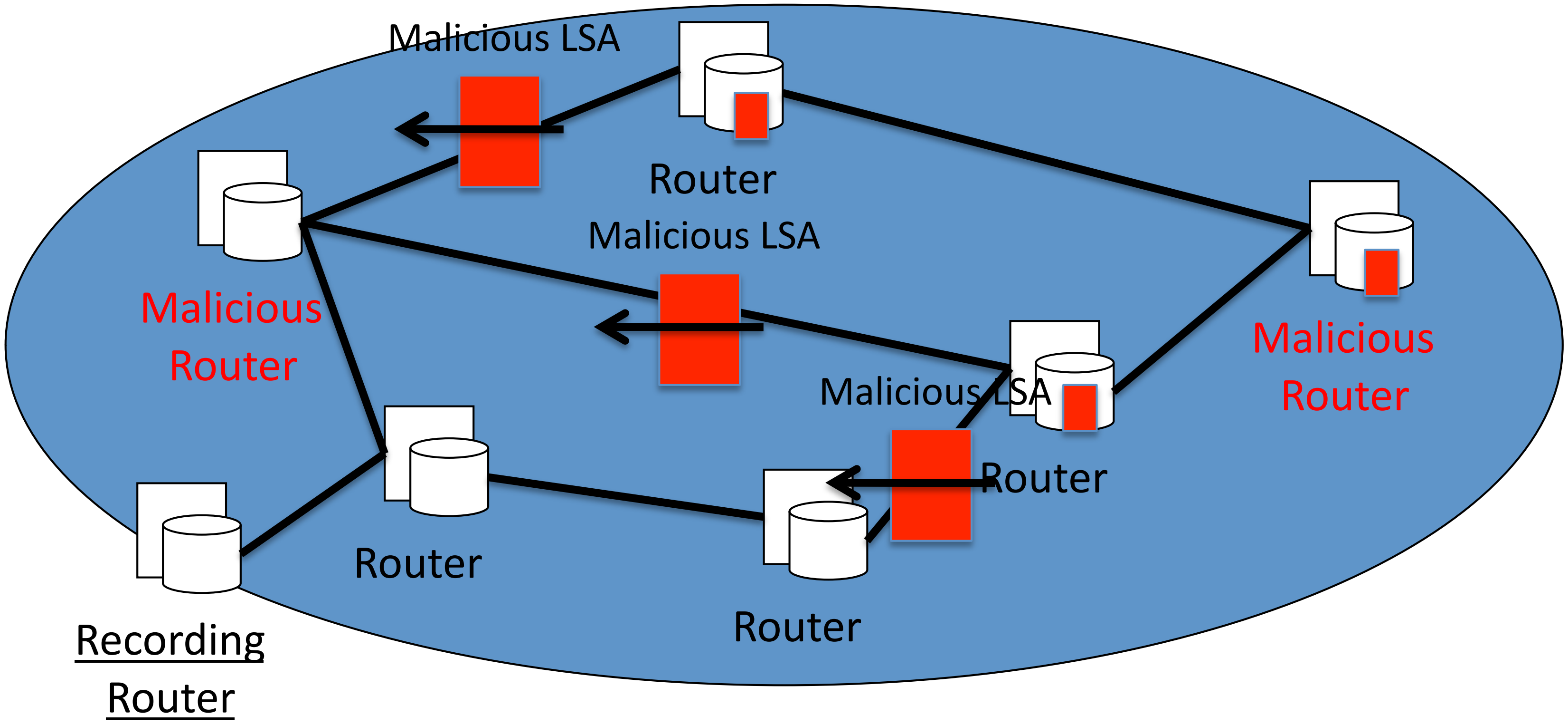
- Want to make the OSPF monitoring (in the area) simpler and more effective
- Wanted to share a possible problem
  - in a rare situation, LSDB monitoring fails.
  - cannot completely monitor OSPF acts.
  - cannot guarantee your routers are doing right.
  - Covert Channel in OSPF.
- Introduction to a simple solution
  - An effort to make OSPF more secure
  - strict LSDB synchronization (enforcing the same history)

LSDB recording may not work

Ack'ing is omitted from the illustration.

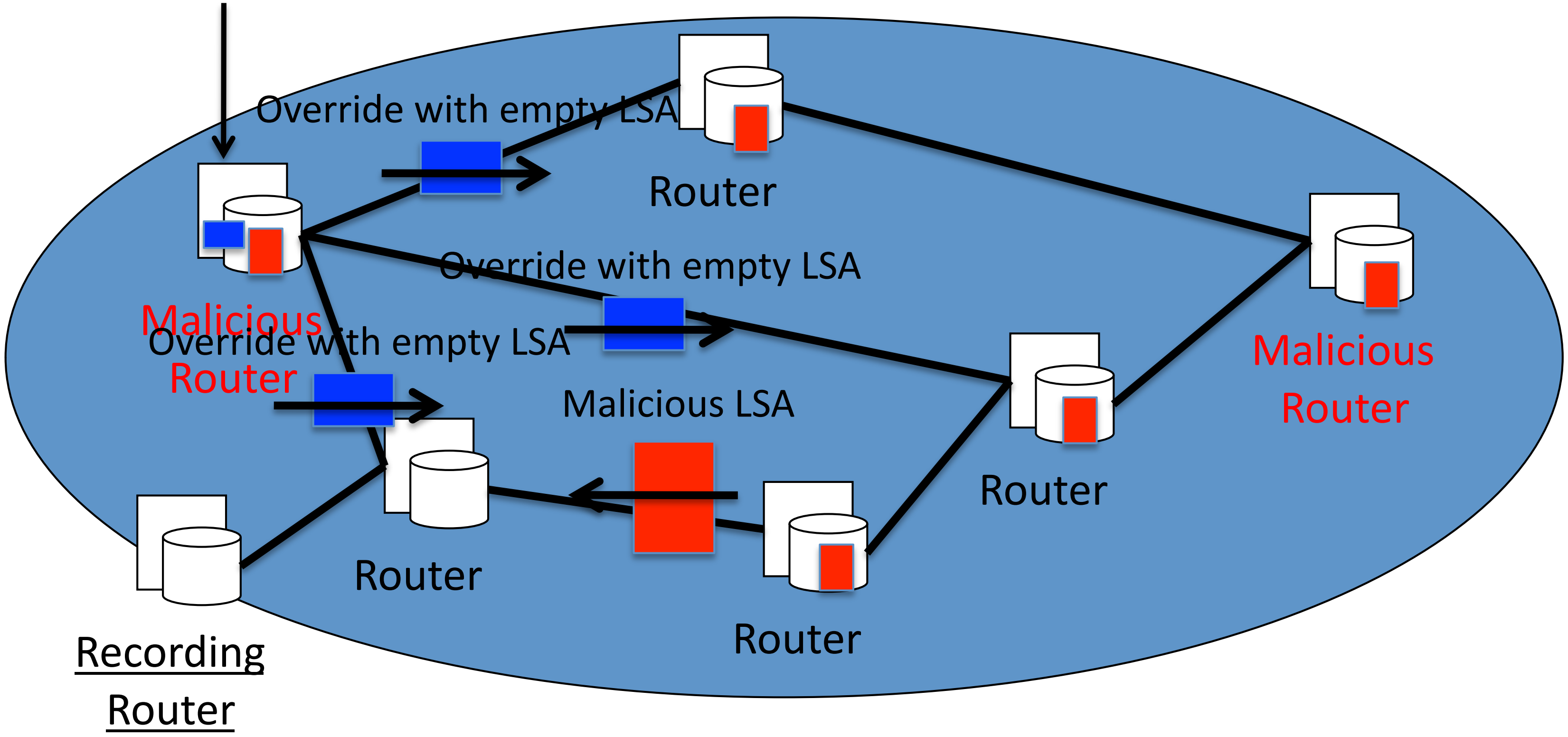


LSDB recording may not work



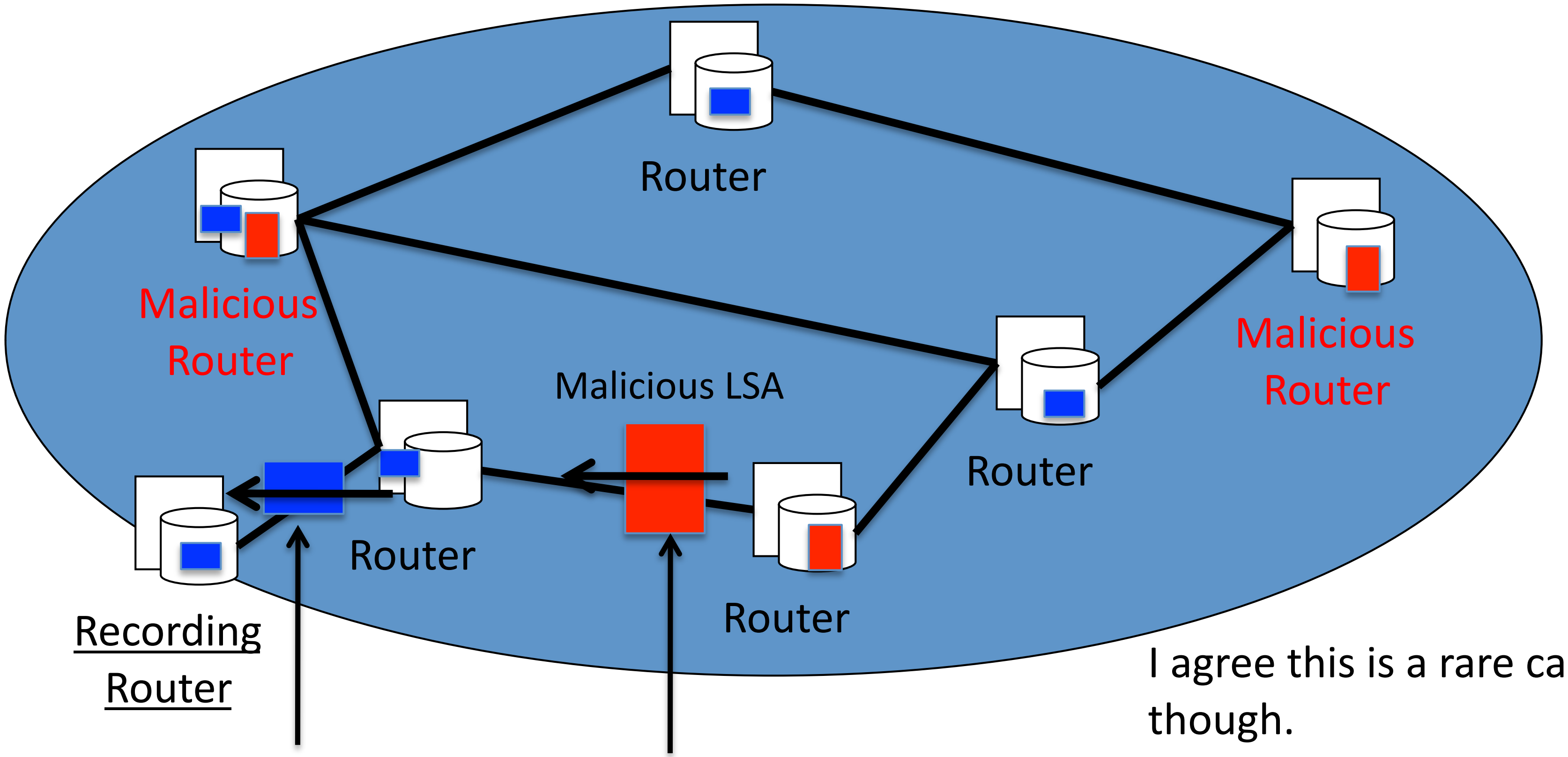
LSDB recording may not work

Tries to hide; immediately purging by premature aging.



LSDB recording may not work

Ack'ing is omitted from the illustration.



Recording Router never sees malicious contents.

Will not be accepted because this is older.

I agree this is a rare case though.

So what's the problem ?

- You will not be aware of "illegal activities" of your OSPF routers
    - e.g. say, routers made by a small unknown Japanese vendor sending info of your nets back to their Japanese company or government. (sneaking things in your net)
- How do you make sure that your OSPF routers are not doing ANY unnecessary (undesirable) activity ?
- Contributes to prevent the disaster when a buggy OSPF router starts to flood updates of other router's LSAs.

Proposed solution

- Modifications to the OSPF spec.
  1. The premature aging can happen only when the LSA contents are identical between old and new (i.e., removed and removing) LSAs.
  2. All LSAs are updated only when
     1. none of its instance is on any retrans-list, and
     2. the LS Sequence Number is incremented by 1.
  - or
- Just logging, warning.

experiment

```
Receiver       +--+         Sender
   /-----------+B10+-----------\
 +-++          +--+          ++-+
 |A9|                        |C11|
 +-++   +--+   +--+   +--+   ++-+
   \----+D12+--+E13+--+F14+----/
        ++-+   +--+   +--+
         |
        ++-+
        |G17|
        +--+
      LSDB Monitor
```

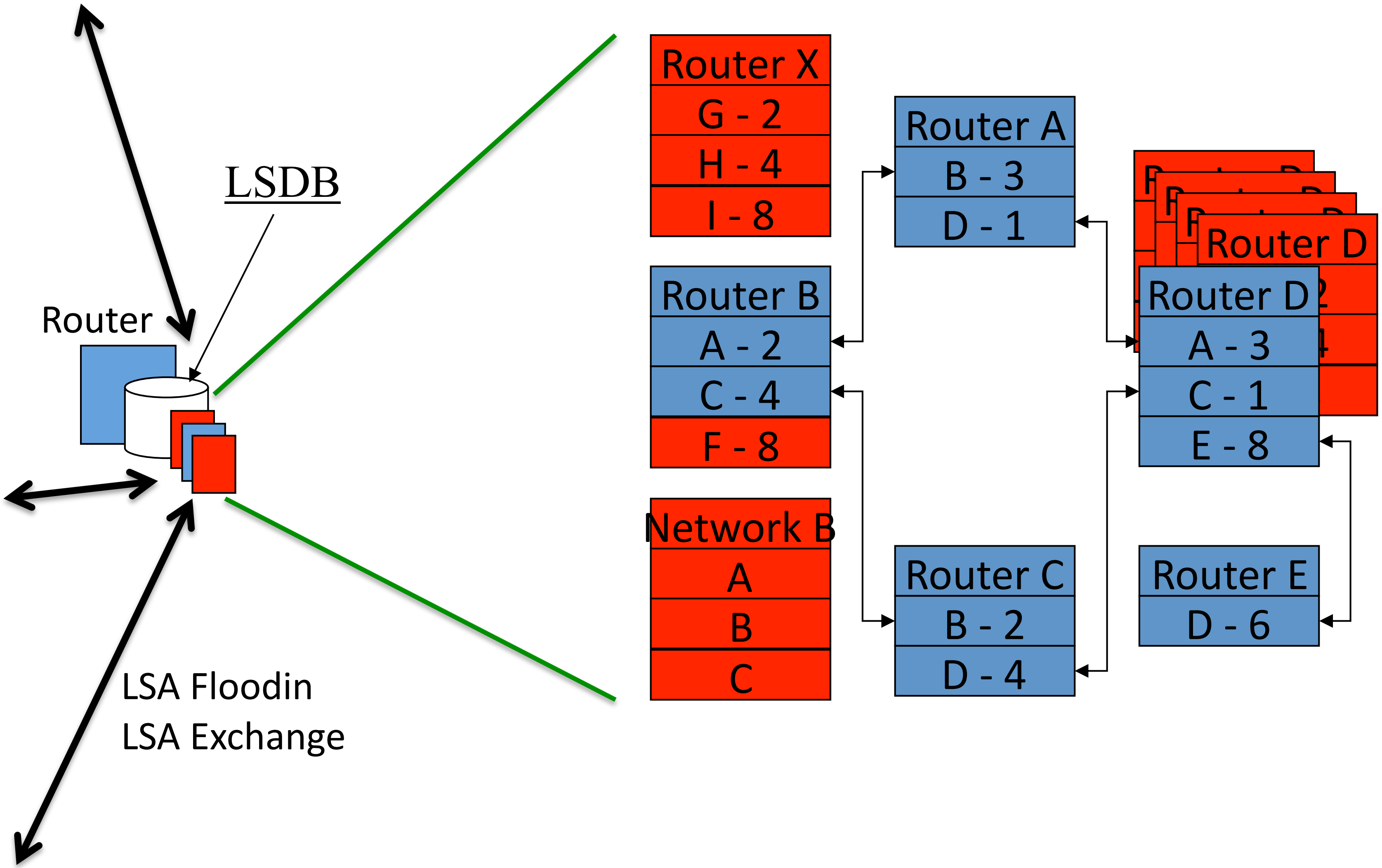
```
Type          LSId            AdvRouter          Age    SeqNum Cksm   Len
   Duration
Router        0.0.0.0         0.0.0.0           1543  80000102 c256    56
   00:25:41
Router        0.0.0.0         192.168.0.2       1204  80000297 36d0    56
   00:16:46
Router        0.0.0.0         192.168.0.9        640  800000b1 6095    56
   00:10:33
Router        0.0.0.0         192.168.0.10       640  80000002 9312    56
   00:10:37
Router        0.0.0.0         192.168.0.11      1534  8000010b d0c5    56
   00:25:30
Router        0.0.1.35        192.168.0.11         4  800003b5 9840    56
   00:00:00
Router        0.0.0.0         192.168.0.12      1006  80000003 4abe    72
   00:16:46
Router        0.0.0.0         192.168.0.13      1512  80000100 3766    56
   00:25:11
Router        0.0.0.0         192.168.0.14      1484  8000011d 0d71    56
   00:24:41
Router        0.0.0.0         192.168.0.17       982  80000003 63bc    40
   00:16:21
Network       0.0.0.2         192.168.0.10       641  80000001 715c    32
   00:10:38
Network       0.0.0.3         192.168.0.11       609  80000003 7552    32
   00:10:05
Network       0.0.0.3         192.168.0.12       409  80000002 6d5a    32
   00:06:49
Network       0.0.0.2         192.168.0.13       417  80000002 a51e    32
```

```
root@i010 (1)# tail -f /var/log/zebra-ospf6d.log
2011/07/27 11:39:55 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 11:39:55 OSPF6:     Age:    5 SeqNum: 0x8000035f Cksum:
   45e9 Len: 56
2011/07/27 11:40:00 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 11:40:00 OSPF6:     Age:    2 SeqNum: 0x80000360 Cksum:
   43ea Len: 56
2011/07/27 11:40:05 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 11:40:05 OSPF6:     Age:    5 SeqNum: 0x80000361 Cksum:
   41eb Len: 56
2011/07/27 11:40:10 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 11:40:10 OSPF6:     Age:    2 SeqNum: 0x80000362 Cksum:
   3fec Len: 56
2011/07/27 11:40:15 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 11:40:15 OSPF6:     Age:    5 SeqNum: 0x80000363 Cksum:
   3ded Len: 56
2011/07/27 11:40:20 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 11:40:20 OSPF6:     Age:    2 SeqNum: 0x80000364 Cksum:
```

```
root@i017 (1)# tail -f /var/log/zebra-ospf6d.log
2011/07/27 19:45:03 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 19:45:03 OSPF6:     Age:    9 SeqNum: 0x8000035f Cksum:
   45e9 Len: 56
2011/07/27 19:45:13 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 19:45:13 OSPF6:     Age:    9 SeqNum: 0x80000361 Cksum:
   41eb Len: 56
2011/07/27 19:45:23 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 19:45:23 OSPF6:     Age:   10 SeqNum: 0x80000363 Cksum:
   3ded Len: 56
2011/07/27 19:45:33 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 19:45:33 OSPF6:     Age:   10 SeqNum: 0x80000365 Cksum:
   39ef Len: 56
2011/07/27 19:45:43 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 19:45:43 OSPF6:     Age:   10 SeqNum: 0x80000367 Cksum:
   35f1 Len: 56
2011/07/27 19:45:53 OSPF6:     [Router Id:0.0.1.35 Adv:
   192.168.0.11]
2011/07/27 19:45:53 OSPF6:     Age:    9 SeqNum: 0x80000369 Cksum:
```

end

Unused LSA



LSDB

Router

LSA Floodin

LSA Exchange

Router X
G - 2
H - 4
I - 8

Router B
A - 2
C - 4
F - 8

Network B
A
B
C

Router A
B - 3
D - 1

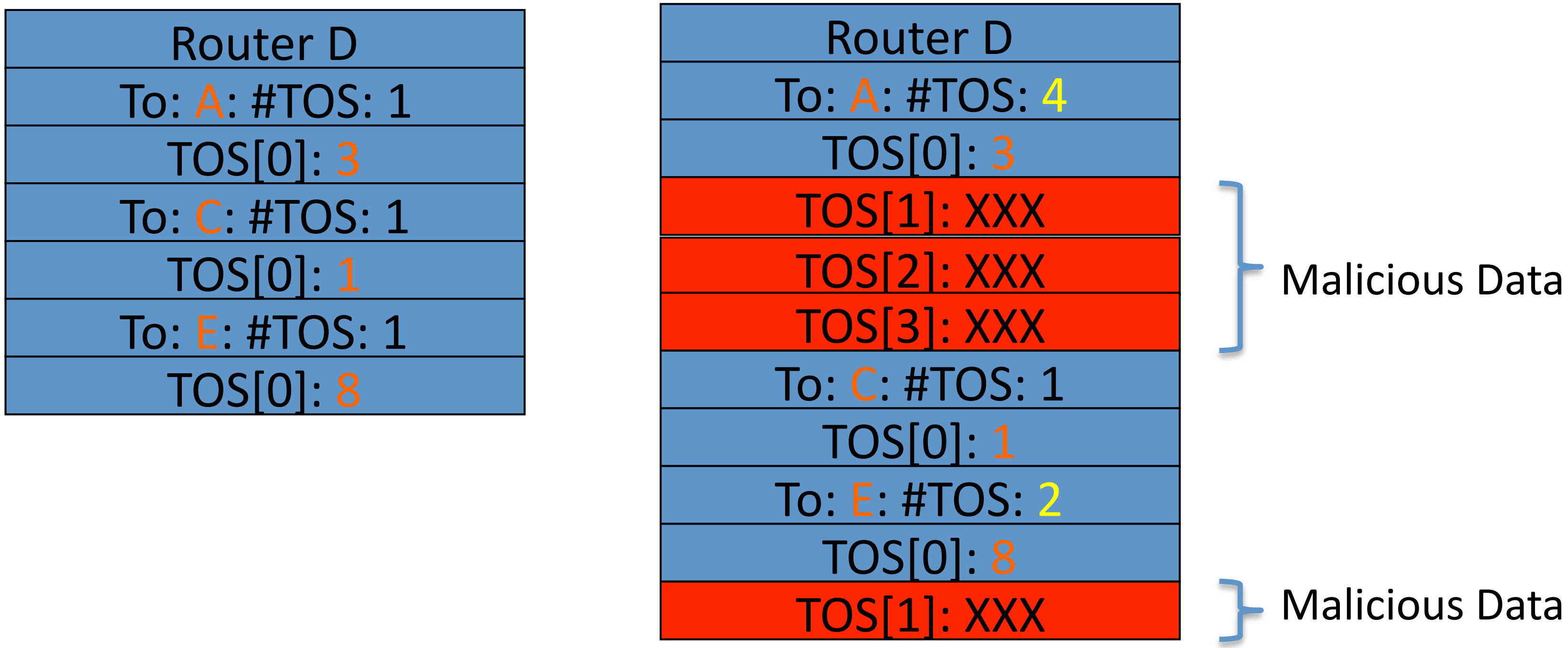
Router C
B - 2
D - 4

Router D

Router D
A - 3
C - 1
E - 8

Router E
D - 6

Unused ToS



Usual LSA

Router D
To: A: #TOS: 1
TOS[0]: 3
To: C: #TOS: 1
TOS[0]: 1
To: E: #TOS: 1
TOS[0]: 8

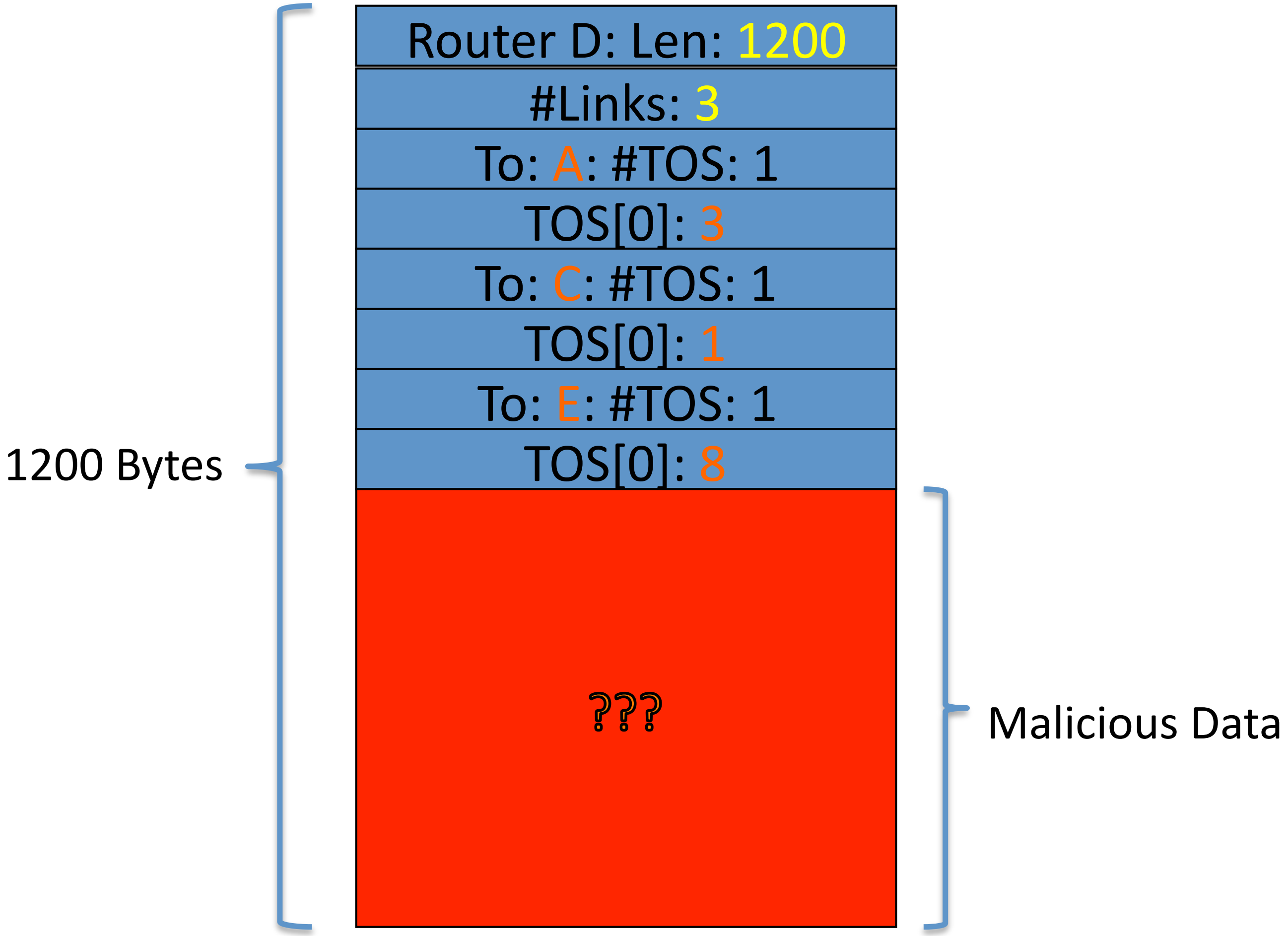
LSA with unused ToS

Router D
To: A: #TOS: 4
TOS[0]: 3
TOS[1]: XXX
TOS[2]: XXX
TOS[3]: XXX
To: C: #TOS: 1
TOS[0]: 1
To: E: #TOS: 2
TOS[0]: 8
TOS[1]: XXX

Malicious Data

Malicious Data

Blank fields



Router D: Len: 1200

#Links: 3

To: A: #TOS: 1

TOS[0]: 3

To: C: #TOS: 1

TOS[0]: 1

To: E: #TOS: 1

TOS[0]: 8

???

1200 Bytes

Malicious Data