Journal of Electrical and Electronic Engineering
2015; 3(2-1): 39-45
Published online January 17, 20145 (http://www.sciencepublishinggroup.com/j/jeee)
doi: 10.11648/j.jeee.s.2015030201.19
ISSN: 2329-1613 (Print); ISSN: 2329-1605 (Online)

A new attack on link-state database in open shortest path first routing protocol

Esmail Kaffashi[1], Ahmad Madadi Mousavi[1], Hamid Rezaei Rahvard[2], Sahar Hemmatian Bojnordi[3], Forough Khademsadegh[1], Soheila Amirian[1]

[1]Information Technology and Computer Engineering Department, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran
[2]Pardazeshgaran Gam Aval, Mashhad, Iran
[3]Industrial department, University of Applied Science, SID Bojnourd Center, Bojnourd, Iran

Email address:
Esmail2001201@Gmail.com (E. Kaffashi), A.madadi@Gmail.com (A. M. Mousavi), HamiD.Rezaei04@Gmail.com (H. R. Rahvard), Saharhematian2012@Gmail.com (S. H. Bojnordi), Forooghkhadem@Gmail.com (F. Khademsadegh), Soh.amirian@Gmail.com (S. Amirian)

To cite this article:
Esmail Kaffashi, Ahmad Madadi Mousavi, Hamid Rezaei Rahvard, Sahar Hemmatian Bojnordi, Forough Khademsadegh, Soheila Amirian. A New Attack on Link-State Database in Open Shortest Path First Routing Protocol. *Journal of Electrical and Electronic Engineering*. Special Issue: Research and Practices in Electrical and Electronic Engineering in Developing Countries. Vol. 2, No. 6-1, 2014, pp. 39-45.
doi: 10.11648/j.jeee.s.2015030201.19

Abstract: Open Shortest Path First (OSPF) protocol known as interior gateway of routing protocol is a major competitor for Cisco's EIGRP of a special routing protocol. Most attacks on this protocol are based on LSA fake router which the attacker has control over it. These attacks can affect the part of the routing domain or cause severe damage based on the strategic location of the router in the AS to bring domain routing. Attacks that cause much damage to a network security mechanism and enables fight-back will not have effect on routing domain. In this paper we will describe an attack that can arbitrarily change the routing domain routing table with harmfully threats without fight back mechanism enabled.

Keywords: Security, Routing Protocols, Link-State, OSPF, New Attack

1. Introduction

Open Shortest Path First (OSPF) is a complexity routing protocol of link-state [8, 10]. Link-State routing protocol is much faster and more convenient way to reach your destination and obtains in comparison to Distance Vector protocol Msyrbaby [1]. Routers using Link-State algorithm creates a map of a network that allow them to choose the best path accurately. OSPF uses of Link-State algorithm to calculate the shortest path to all destinations and select the best-known [1]. In this process, we analyzed the algorithm.

When the situation of a link was changed and the device detected a link change began to publish an LSA message about links. After the publication of the LSA message, router send it to all neighboring devices via a special multi-cast message [4]. As depicted in Figure 1, the schema of LSA message sending in a hypothetical network is presented.

Each router makes up to date own by using the received LSA or Link-State Database (LSDB), furthermore, the router sends LSA to its other neighbors. When the database of each router is completed, the shortest path to the destination is measured in a tree that Dijkstra's algorithm uses it to calculate the shortest path tree destinations, costs and next hope to reach its destination in routing table form [3, 13].

If no changes happen in the OSPF net such as change in link cost or adding and omitting, an OSPF net continues smoothly. Any changes which are announced through link-state packets, Dijkstra algorithm finds the shortest route to be calculated again.

An area is defined as a group of contiguous networks and host. All routers in the same area share a common area ID. All routers within the same area have the same topology table as well.

As mentioned previously, OSPF LSA uses a Link-State updates for exchange uses. Any change in routing information is sent to all network routers, area concept was introduced in order to limit the part of the Link-State updates explosion occur. Dijkstra's algorithm to compute a function of a router is limited to changes within an area [3]. All routers within an area of Link-State databases are complete and accurate.

This protocol is designed to be used within a single Autonomous System or AS and can be divided into different groups of the network called area. Each area has its own database; the topological database for each area will be hidden from other areas, which will reduce traffic on the network. All areas must be connected to an area called Backbone.

Routers belonging to a single area are called Internal Router. Routers which belong to more than one area are called Area Border Routers (ABRs). The router will start to exchange routing information with an external AS Autonomous System Boundary Router (ASBR) is called. Figure 2 shows the layout of the routers in the area [6].

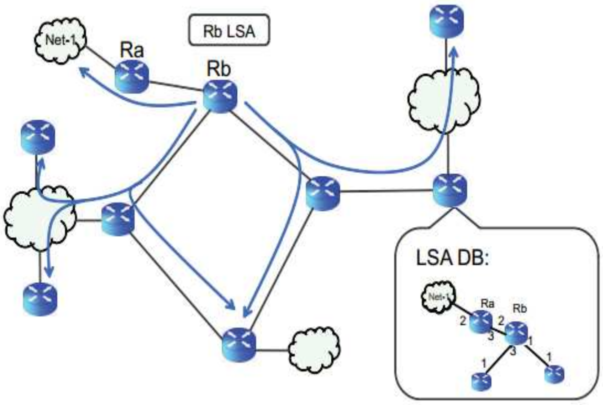


Figure 1. *An example of LAS sending.*

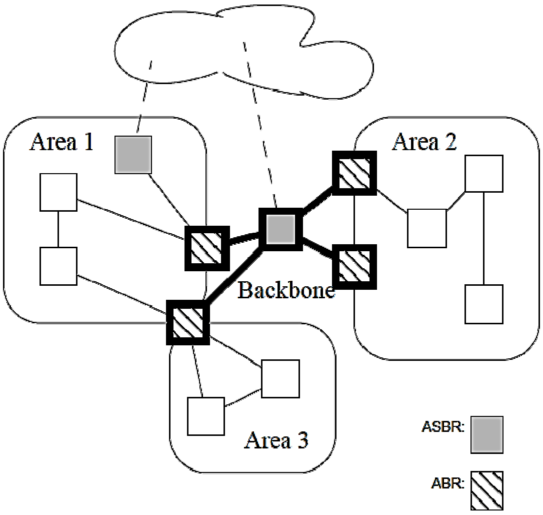


Figure 2. *The role of routers in area [6]*

This project will include the following milestones:

1 Careful reading of RFC 2328 (OSPF v2).
2 Research on known vulnerabilities of attacks on traffic of this protocol.
3 A new method of attack on the protocol.
4 Conclusions from the findings.

2. Vulnerability and Risk

Protect infrastructure and network infrastructure is very important. The mean of the Internal / Insider routers are the trusted network and has been accepted as a router in the network and the company is in the process of information exchange and the face of the routers External / Outsider reverse the Internal / Insider will [13].

2.1. Basic OSPF Vulnerability

OSPF risks arise mainly from the following vulnerabilities:

- Distance attack: even if the OSPF routing protocol to be used as the range, but in many situations and conditions routers OSPF unicast packets that will be sent to the address it receives and accepts (in paragraph 8.1 of RFC2328) [8].
- The fight-back mechanisms: in OSPF, this mechanism can be explained as follows: when a router LSA has the right to see their fake just to send LSA and to inform the public that the LSA has been true and the other false. But this mechanism is not very effective because in RFC2328 OSPF v2 is related to the mechanism, there are no words to and there is no official word fight. Procedures for the inactivation mechanism during attacks there [9, 10].
- Abusing the fight-back mechanisms: Can help to implement a DOS attack. Update an LSA storm may make the mistake of trying to make the LSA wrong. Even though this is an acceptable and effective response.
- External routes: Routes that are received from external sources such as other area or AS other, we can not validate them in areas that are not defined as stub is reproduced [13].

2.2. Vulnerabilities in Protocols

This protocol has more security mechanisms for authentication, such as checksam received packets over the communication link. OSPF is generally 5 types of messages:

1 Hello
2 Database Description
3 Link-State Request
4 Link-State Update
5 Link-State Acknowledgement [9]

Message type attacks can be performed on each of the 5 and the fields that are defined for these messages can use to your advantage to get a more sophisticated ground attack [8]. The JiNao, 4 presented the attacks that can be said is essentially a denial of service attack. Below the name of four attacks are mentioned [7]:

1 Max Age
2 Sequence++
3 Max Sequence#
4 Bogus LSA

Age of the field in the packet header of the attack 1 LSA message is abuse or episodes 2 and 3 of the Sequence Number field of the message header of the previous abuse [1, 3].

2.3. Sources of Vulnerability

These attacks are the main ways of taking system resources such as CPU, RAM or disk space, or network connections by which they aim to avoid a system or network is usually associated with a particular sector or other networks. Because sometimes hackers use to destroy your network Prdarnd resources such attacks are also known to attack non-symmetric or asymmetric attack [13].

3. Understanding the Attack

Suppose that, a remote attacker could leverage the insider to attack the router, Some vulnerabilities have been reported as CVE-2010-0581, CVE-2010-0580, CVE-2009-2865 CVE-2010-0581 that an attacker can execute code with a SIP packet to and routers with Broadcom chipsets or just a new bug has been discovered by a team DefenseCode which allows an attacker without authentication to run their code on the root surface [2, 13].

To attack the protocols that are stable, we can use other poor protocols. For example, we can use the RIP protocol, which is completely unsafe and send the OSPF or BGP message in wrong routes, and circumvent their natural protection. Another critical point in OSPF networks is DR routers that can be attacked and disrupt the network [10].

Two new attacks on this protocol are designed to follow the rules of the protocol is as follows:

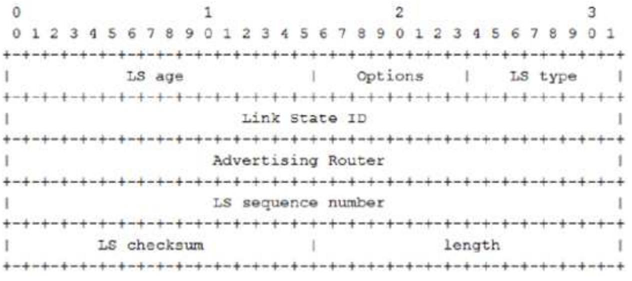
1 Wrong adjacent from the remote: it allows attackers to trick a remote router and by fake LSAs define a new link to the router that this link does not exist in real. This attack focuses on the routers adjacency process. This attack can create a Block-Hole for a particular subnet.

2 Fake LSA messages: this attack is of those high damage attacks on the network and will also enable the fight-back security mechanism. But what is more important is that the mechanism itself is used in the attack, in attack implementation focus point is on the creation and transfer of the fight-back messages [9].

In the following description, we will describe attack which is optimized version of the fake LSA.

3.1. New Attack on Routing Tables

The header of a LSA instance is shown in Figure 3:



```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            LS age             |    Options    |    LS type    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Link State ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Advertising Router                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     LS sequence number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         LS checksum           |             length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3. *LSA Header Format [7]*

Structure descriptions are:

- LS Age: elapsed time of the creation of the LSA indicates that on seconds.
- Options: used for optional feature.
- LS Type: specifies the type of LSA (e.g. Router, Network, Summary, etc.) will be discussed further on Router LSA.
- Link State ID: AS topology is part of the LSA to describe it will specify section.
- Advertising Router: Router ID of the router that created the LSA.
- LS Sequence Number: number of LSA that each LSA specifies its own unique number.
- LS Checksum: Checksum refers to the entire contents of the LSA.
- Length: shows LSA content length to bits [7].

In attack we do need to focus on two fields, here are two fields when creating Router LSA:

- Link State ID: each router creates the LSA, should be assigned LS ID the same as the router ID of the router.
- Advertising ID: specifies the router LSA's original creation (i.e. the origin of creation LSA).

Based on OSPF regulation each router creates own LSA and is not expected to cause the router to other routers to generate router LSA, as described above, then the two fields must have the same value [3]. In OSPF to check the same for these two fields, the specific operation is not performed and this will send the LSA so that the two fields have different values [5]. Based on section 13.4, a router can activate fight-back when you receive a fake LSA:

"The Advertising Router is equal to the router's own Router ID"

This means that the Advertising Router from fake LSA equal to victim router’s Router ID, fight-back victim will not be activated by the victim router even if the LS ID is equal to the Router ID of the victim router. Explanation may be that we assume the attacker will send Router LSA from some of Rv victims:

1 LS ID: is equal to the ID of Rv Router.

2 Advertising Router: every value except the ID of Rv Router.

According to the rules of OSPF it can be assured that fight-back will not be activated even in other routers in the AS with Rv Router and they put a fake LSA in their LSDB, but we have a problem. In section 12.1 of RFC is determined based on the following three fields identifies uniquely the LSA or not:

1 LS Type

2 Advertising Router

3 LS ID

Therefore fake LSA is not valid in the LSDB because they are different (Advertising Router is not equal) and cannot trust until fake LSA are not deleted from LS DB [2, 3]. OSPF as discussed in RFC where there is doubt that it can be used and have a successful attack [8]. Section 16.1 is said route calculation on LSDB is based on the Vertex ID:

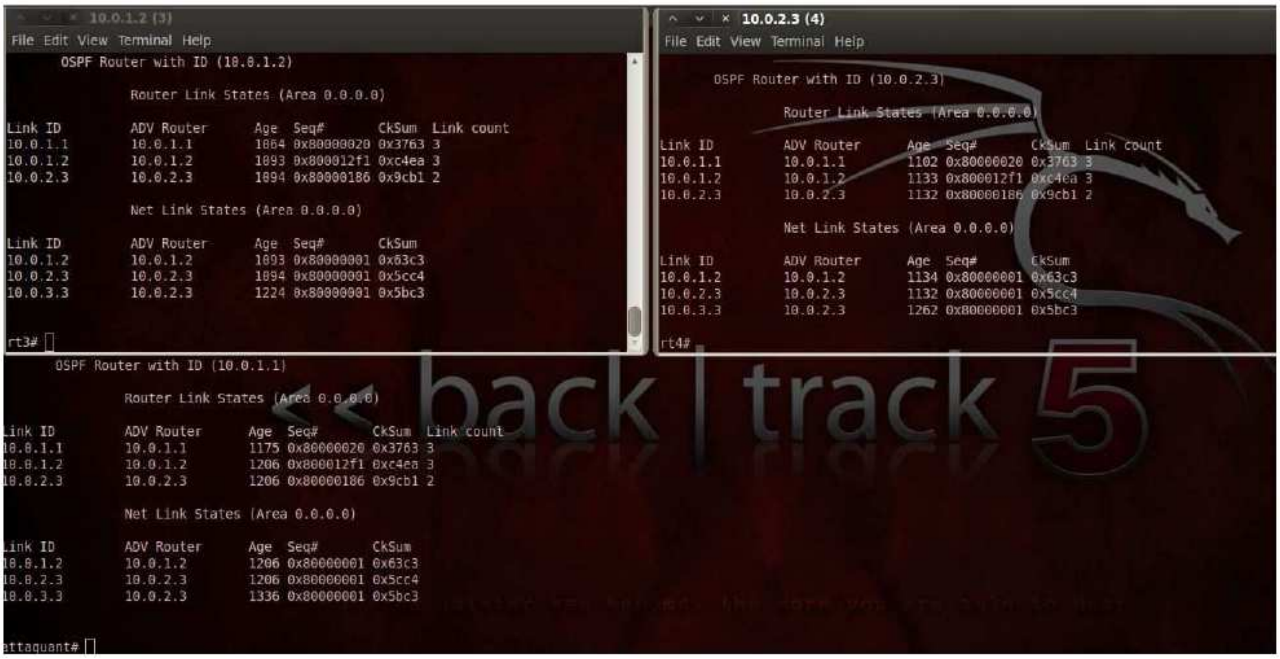
“This is a lookup ... based on the Vertex ID“.

The description of OSPF Link State ID field is the same as Vertex ID. When routers create routing table they act on the basis of this field. This will be an ambiguity in the description of the protocol and on the other side of the LSA are identified and described three fields before the other calculations will be based on the Link State ID field. This ambiguity raises the question: When the LSA fetch from LSDB for the fetch calculation then which LSA is fetched, authentic and original LSA or fake LSA? Remember that both the fake and the original LSA all are in the LSDB as there. Both LSA and Link

State ID field has the same value. OSPF is not able to answer the question, so the answer depends on the implementation [3, 8].

Most networks that have implemented OSPF, is based on Cisco IOS. According to infonetrics research, almost 75 percent enterprise networks use Cisco's in world [11]. To implement attack, we use GNS3 and SCAPY with the latest stable version of IOS on the C7200 router and we test it with M1-150 version provided by Cisco.

We send fake LSA with higher sequence number than the original LSA. Fake LSA is not only in the LSDB but also in the entire LSDB will be replaced within the AS. All routers have the victim router. In Figure 4, the result of running attack can be seen and the whole process is shown in Figure 5-10.



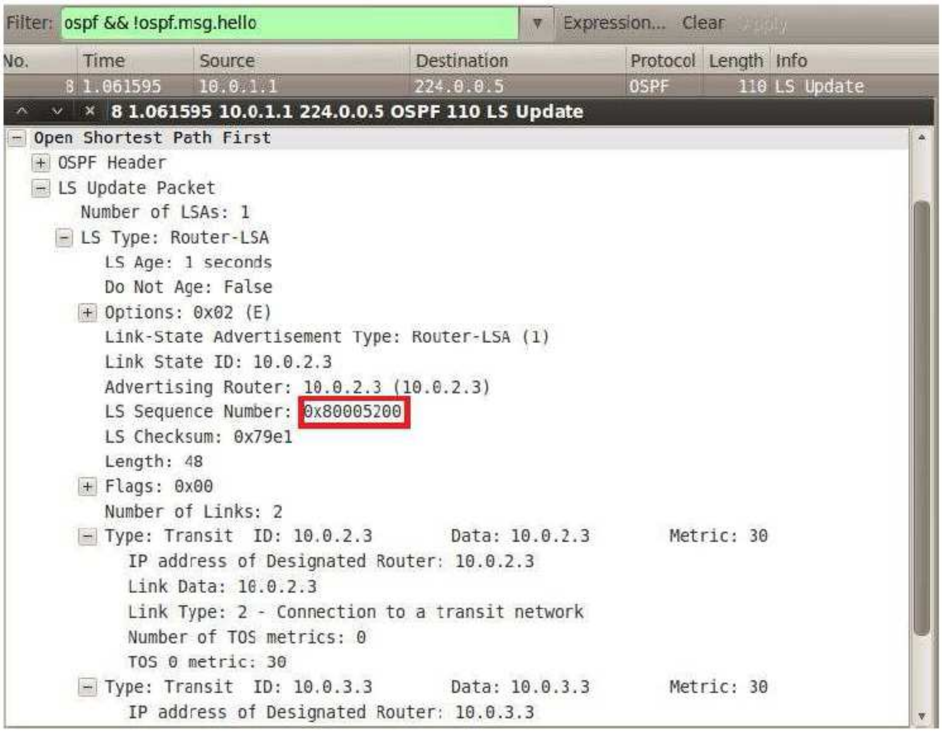
```
       OSPF Router with ID (10.0.1.2)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.0.1.1        10.0.1.1        1864 0x80000020 0x3763 3
10.0.1.2        10.0.1.2        1893 0x800012f1 0xc4ea 3
10.0.2.3        10.0.2.3        1894 0x80000186 0x9cb1 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.0.1.2        10.0.1.2        1893 0x80000001 0x63c3
10.0.2.3        10.0.2.3        1894 0x80000001 0x5cc4
10.0.3.3        10.0.2.3        1224 0x80000001 0x5bc3

rt3#
```

```
       OSPF Router with ID (10.0.2.3)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.0.1.1        10.0.1.1        1102 0x80000020 0x3763 3
10.0.1.2        10.0.1.2        1133 0x800012f1 0xc4ea 3
10.0.2.3        10.0.2.3        1132 0x80000186 0x9cb1 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.0.1.2        10.0.1.2        1134 0x80000001 0x63c3
10.0.2.3        10.0.2.3        1132 0x80000001 0x5cc4
10.0.3.3        10.0.2.3        1262 0x80000001 0x5bc3

rt4#
```

```
       OSPF Router with ID (10.0.1.1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.0.1.1        10.0.1.1        1175 0x80000020 0x3763 3
10.0.1.2        10.0.1.2        1206 0x800012f1 0xc4ea 3
10.0.2.3        10.0.2.3        1206 0x80000186 0x9cb1 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.0.1.2        10.0.1.2        1206 0x80000001 0x63c3
10.0.2.3        10.0.2.3        1206 0x80000001 0x5cc4
10.0.3.3        10.0.2.3        1336 0x80000001 0x5bc3

attaquant#
```

Figure 4. *OSPF database before the attack*

Using Wireshark, we follow OSPF: first appears the tigger packet use to force a response the rt4 router (id = 10.0.2.3). Sequence is set to: 80005200 and the metric (30) is false, it should provoke a fight-back from rt4.

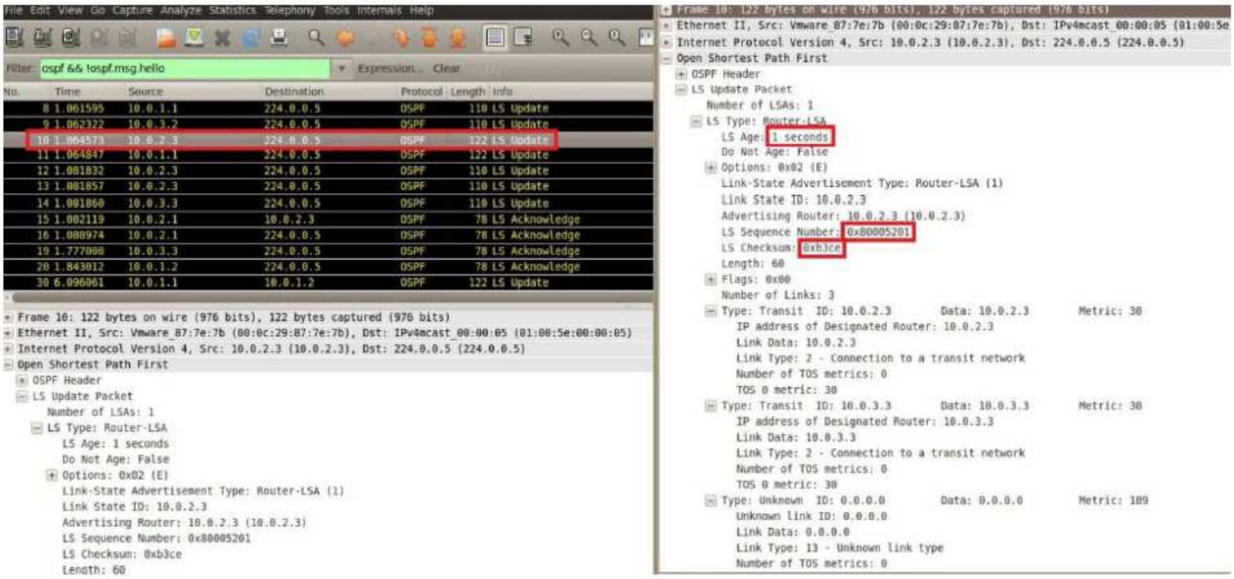


Filter: ospf && !ospf.msg.hello

```
No.   Time        Source      Destination   Protocol  Length  Info
    8 1.061595    10.0.1.1    224.0.0.5     OSPF         110  LS Update
```

```
8 1.061595 10.0.1.1 224.0.0.5 OSPF 110 LS Update
⊟ Open Shortest Path First
  ⊞ OSPF Header
  ⊟ LS Update Packet
      Number of LSAs: 1
    ⊟ LS Type: Router-LSA
        LS Age: 1 seconds
        Do Not Age: False
      ⊞ Options: 0x02 (E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 10.0.2.3
        Advertising Router: 10.0.2.3 (10.0.2.3)
        LS Sequence Number: 0x80005200
        LS Checksum: 0x79e1
        Length: 48
      ⊞ Flags: 0x00
        Number of Links: 2
      ⊟ Type: Transit   ID: 10.0.2.3       Data: 10.0.2.3       Metric: 30
          IP address of Designated Router: 10.0.2.3
          Link Data: 10.0.2.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 30
      ⊟ Type: Transit   ID: 10.0.3.3       Data: 10.0.3.3       Metric: 30
          IP address of Designated Router: 10.0.3.3
```

Figure5. *Sending a packet specially crafted to spoof an R1 LSA.*

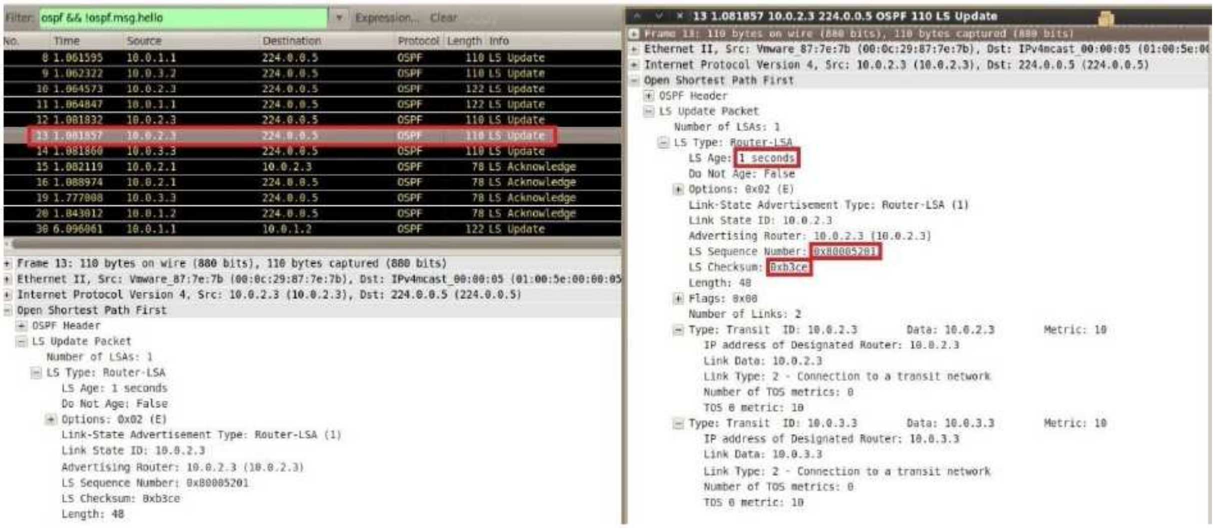

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear

```
Filter: ospf && !ospf.msg.hello
No.   Time        Source      Destination   Protocol Length Info
   8 1.061595    10.0.1.1    224.0.0.5     OSPF     110 LS Update
   9 1.062322    10.0.3.2    224.0.0.5     OSPF     110 LS Update
  10 1.064573    10.0.2.3    224.0.0.5     OSPF     122 LS Update
  11 1.064847    10.0.1.1    224.0.0.5     OSPF     122 LS Update
  12 1.081832    10.0.2.3    224.0.0.5     OSPF     110 LS Update
  13 1.081857    10.0.2.3    224.0.0.5     OSPF     110 LS Update
  14 1.081860    10.0.3.3    224.0.0.5     OSPF     110 LS Update
  15 1.082119    10.0.2.1    10.0.2.3      OSPF      78 LS Acknowledge
  16 1.088974    10.0.2.1    224.0.0.5     OSPF      78 LS Acknowledge
  19 1.777008    10.0.3.3    224.0.0.5     OSPF      78 LS Acknowledge
  20 1.843012    10.0.1.2    224.0.0.5     OSPF      78 LS Acknowledge
  30 6.096061    10.0.1.1    10.0.1.2      OSPF     122 LS Update
```

```
+ Frame 10: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
+ Ethernet II, Src: Vmware_87:7e:7b (00:0c:29:87:7e:7b), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05)
+ Internet Protocol Version 4, Src: 10.0.2.3 (10.0.2.3), Dst: 224.0.0.5 (224.0.0.5)
- Open Shortest Path First
  + OSPF Header
  - LS Update Packet
      Number of LSAs: 1
    - LS Type: Router-LSA
        LS Age: 1 seconds
        Do Not Age: False
      + Options: 0x02 (E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 10.0.2.3
        Advertising Router: 10.0.2.3 (10.0.2.3)
        LS Sequence Number: 0x80005201
        LS Checksum: 0xb3ce
        Length: 60
```

```
+ Frame 10: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
+ Ethernet II, Src: Vmware_87:7e:7b (00:0c:29:87:7e:7b), Dst: IPv4mcast_00:00:05 (01:00:5e
+ Internet Protocol Version 4, Src: 10.0.2.3 (10.0.2.3), Dst: 224.0.0.5 (224.0.0.5)
- Open Shortest Path First
  + OSPF Header
  - LS Update Packet
      Number of LSAs: 1
    - LS Type: Router-LSA
        LS Age: 1 seconds
        Do Not Age: False
      + Options: 0x02 (E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 10.0.2.3
        Advertising Router: 10.0.2.3 (10.0.2.3)
        LS Sequence Number: 0x80005201
        LS Checksum: 0xb3ce
        Length: 60
      + Flags: 0x00
        Number of Links: 3
      - Type: Transit  ID: 10.0.2.3        Data: 10.0.2.3        Metric: 30
          IP address of Designated Router: 10.0.2.3
          Link Data: 10.0.2.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 30
      - Type: Transit  ID: 10.0.3.3        Data: 10.0.3.3        Metric: 30
          IP address of Designated Router: 10.0.3.3
          Link Data: 10.0.3.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 30
      - Type: Unknown  ID: 0.0.0.0         Data: 0.0.0.0         Metric: 109
          Unknown link ID: 0.0.0.0
          Link Data: 0.0.0.0
          Link Type: 13 - Unknown link type
          Number of TOS metrics: 0
```

Figure 6. *Sending the disguised LSA craft to match the LSA fight-back from rt4*



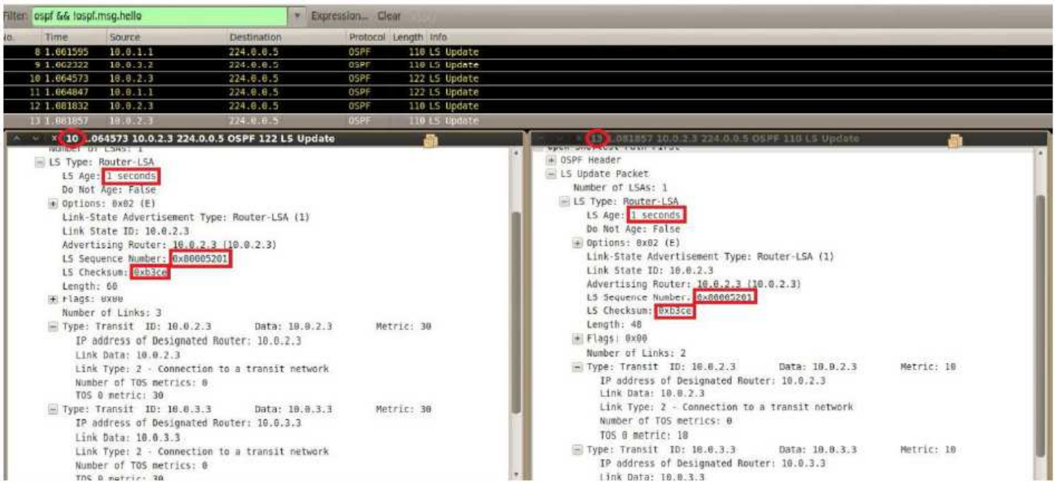
```
Filter: ospf && !ospf.msg.hello
No.   Time        Source      Destination   Protocol Length Info
   8 1.061595    10.0.1.1    224.0.0.5     OSPF     110 LS Update
   9 1.062322    10.0.3.2    224.0.0.5     OSPF     110 LS Update
  10 1.064573    10.0.2.3    224.0.0.5     OSPF     122 LS Update
  11 1.064847    10.0.1.1    224.0.0.5     OSPF     122 LS Update
  12 1.081832    10.0.2.3    224.0.0.5     OSPF     110 LS Update
  13 1.081857    10.0.2.3    224.0.0.5     OSPF     110 LS Update
  14 1.081860    10.0.3.3    224.0.0.5     OSPF     110 LS Update
  15 1.082119    10.0.2.1    10.0.2.3      OSPF      78 LS Acknowledge
  16 1.088974    10.0.2.1    224.0.0.5     OSPF      78 LS Acknowledge
  19 1.777008    10.0.3.3    224.0.0.5     OSPF      78 LS Acknowledge
  20 1.843012    10.0.1.2    224.0.0.5     OSPF      78 LS Acknowledge
  30 6.096061    10.0.1.1    10.0.1.2      OSPF     122 LS Update
```

```
+ Frame 13: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
+ Ethernet II, Src: Vmware_87:7e:7b (00:0c:29:87:7e:7b), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05
+ Internet Protocol Version 4, Src: 10.0.2.3 (10.0.2.3), Dst: 224.0.0.5 (224.0.0.5)
- Open Shortest Path First
  + OSPF Header
  - LS Update Packet
      Number of LSAs: 1
    - LS Type: Router-LSA
        LS Age: 1 seconds
        Do Not Age: False
      + Options: 0x02 (E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 10.0.2.3
        Advertising Router: 10.0.2.3 (10.0.2.3)
        LS Sequence Number: 0x80005201
        LS Checksum: 0xb3ce
        Length: 48
```

```
13 1.081857 10.0.2.3 224.0.0.5 OSPF 110 LS Update
+ Frame 13: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
+ Ethernet II, Src: Vmware_87:7e:7b (00:0c:29:87:7e:7b), Dst: IPv4mcast_00:00:05 (01:00:5e:0
+ Internet Protocol Version 4, Src: 10.0.2.3 (10.0.2.3), Dst: 224.0.0.5 (224.0.0.5)
- Open Shortest Path First
  + OSPF Header
  - LS Update Packet
      Number of LSAs: 1
    - LS Type: Router-LSA
        LS Age: 1 seconds
        Do Not Age: False
      + Options: 0x02 (E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 10.0.2.3
        Advertising Router: 10.0.2.3 (10.0.2.3)
        LS Sequence Number: 0x80005201
        LS Checksum: 0xb3ce
        Length: 48
      + Flags: 0x00
        Number of Links: 2
      - Type: Transit  ID: 10.0.2.3        Data: 10.0.2.3        Metric: 10
          IP address of Designated Router: 10.0.2.3
          Link Data: 10.0.2.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 10
      - Type: Transit  ID: 10.0.3.3        Data: 10.0.3.3        Metric: 10
          IP address of Designated Router: 10.0.3.3
          Link Data: 10.0.3.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 10
```

Figure 7. *R1 sends the fight-back that will be rejected due to the previous packet craft at step 2.*

Comparison of two packets:

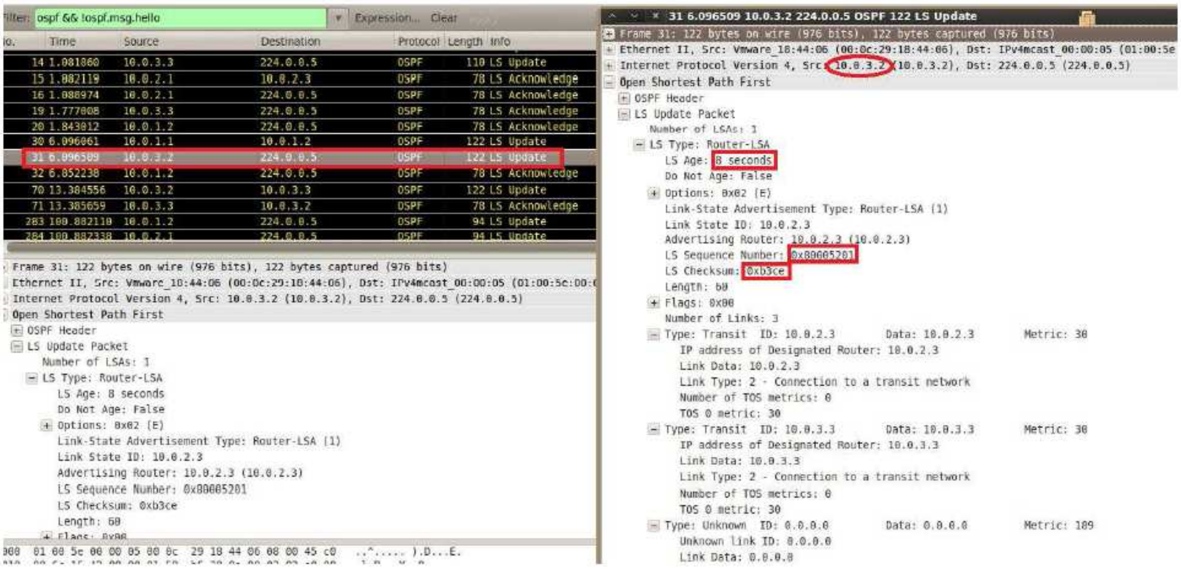


```
Filter: ospf && !ospf.msg.hello
No.   Time        Source      Destination   Protocol Length Info
   8 1.061595    10.0.1.1    224.0.0.5     OSPF     110 LS Update
   9 1.062322    10.0.3.2    224.0.0.5     OSPF     110 LS Update
  10 1.064573    10.0.2.3    224.0.0.5     OSPF     122 LS Update
  11 1.064847    10.0.1.1    224.0.0.5     OSPF     122 LS Update
  12 1.081832    10.0.2.3    224.0.0.5     OSPF     110 LS Update
  13 1.081857    10.0.2.3    224.0.0.5     OSPF     110 LS Update
```

```
10 1.064573 10.0.2.3 224.0.0.5 OSPF 122 LS Update
      Number of LSAs: 1
    - LS Type: Router-LSA
        LS Age: 1 seconds
        Do Not Age: False
      + Options: 0x02 (E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 10.0.2.3
        Advertising Router: 10.0.2.3 (10.0.2.3)
        LS Sequence Number: 0x80005201
        LS Checksum: 0xb3ce
        Length: 60
      + Flags: 0x00
        Number of Links: 3
      - Type: Transit  ID: 10.0.2.3        Data: 10.0.2.3        Metric: 30
          IP address of Designated Router: 10.0.2.3
          Link Data: 10.0.2.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 30
      - Type: Transit  ID: 10.0.3.3        Data: 10.0.3.3        Metric: 30
          IP address of Designated Router: 10.0.3.3
          Link Data: 10.0.3.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 30
```

```
13 1.081857 10.0.2.3 224.0.0.5 OSPF 110 LS Update
- Open Shortest Path First
  + OSPF Header
  - LS Update Packet
      Number of LSAs: 1
    - LS Type: Router-LSA
        LS Age: 1 seconds
        Do Not Age: False
      + Options: 0x02 (E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 10.0.2.3
        Advertising Router: 10.0.2.3 (10.0.2.3)
        LS Sequence Number: 0x80005201
        LS Checksum: 0xb3ce
        Length: 48
      + Flags: 0x00
        Number of Links: 2
      - Type: Transit  ID: 10.0.2.3        Data: 10.0.2.3        Metric: 10
          IP address of Designated Router: 10.0.2.3
          Link Data: 10.0.2.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 10
      - Type: Transit  ID: 10.0.3.3        Data: 10.0.3.3        Metric: 10
          IP address of Designated Router: 10.0.3.3
          Link Data: 10.0.3.3
```

Figure 8. *both packets contains the same sequence number, checksum and age (+/- 15 min)*

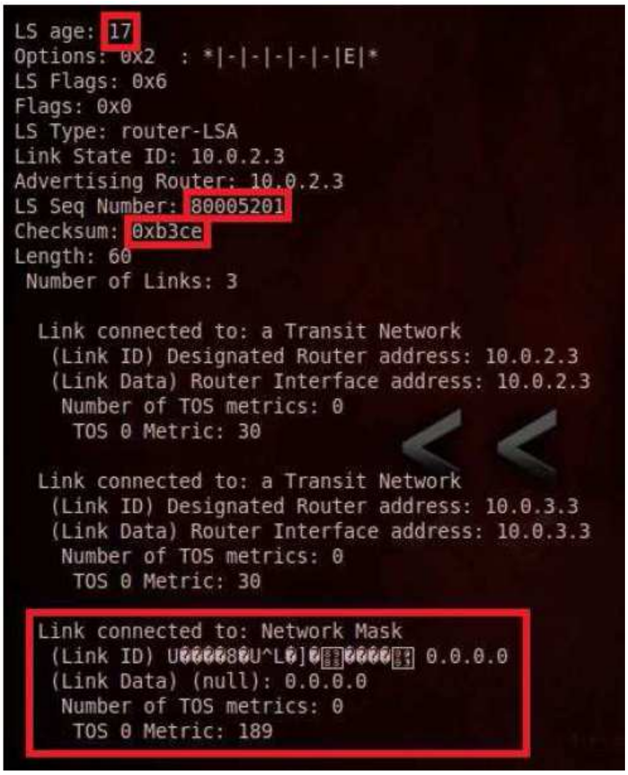


```
No.      Time        Source      Destination   Protocol Length Info
 14 1.081860       10.0.3.3    224.0.0.5     OSPF     110 LS Update
 15 1.082119       10.0.2.1    10.0.2.3      OSPF      78 LS Acknowledge
 16 1.088974       10.0.2.1    224.0.0.5     OSPF      78 LS Acknowledge
 19 1.777808       10.0.3.3    224.0.0.5     OSPF      78 LS Acknowledge
 20 1.843012       10.0.1.2    224.0.0.5     OSPF      78 LS Acknowledge
 30 6.096061       10.0.1.1    10.0.1.2      OSPF     122 LS Update
 31 6.096509       10.0.3.2    224.0.0.5     OSPF     122 LS Update
 32 6.852238       10.0.1.2    224.0.0.5     OSPF      78 LS Acknowledge
 70 13.384556      10.0.3.2    10.0.3.3      OSPF     122 LS Update
 71 13.385659      10.0.3.3    10.0.3.2      OSPF      78 LS Acknowledge
283 100.882110     10.0.1.2    224.0.0.5     OSPF      94 LS Update
284 100.882338     10.0.2.1    224.0.0.5     OSPF      94 LS Update

Frame 31: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: Vmware_18:44:06 (00:0c:29:18:44:06), Dst: IPv4mcast_00:00:05 (01:00:5c:00:(
Internet Protocol Version 4, Src: 10.0.3.2 (10.0.3.2), Dst: 224.0.0.5 (224.0.0.5)
Open Shortest Path First
 ⊞ OSPF Header
 ⊟ LS Update Packet
     Number of LSAs: 1
   ⊟ LS Type: Router-LSA
       LS Age: 8 seconds
       Do Not Age: False
     ⊞ Options: 0x02 (E)
       Link-State Advertisement Type: Router-LSA (1)
       Link State ID: 10.0.2.3
       Advertising Router: 10.0.2.3 (10.0.2.3)
       LS Sequence Number: 0x80005201
       LS Checksum: 0xb3ce
       Length: 60
     ⊞ Flags: 0x00
0000  01 00 5e 00 00 05 00 0c  29 18 44 06 08 00 45 c0   ..^..... ).D...E.
```

```
31 6.096509 10.0.3.2 224.0.0.5 OSPF 122 LS Update
⊞ Frame 31: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
⊞ Ethernet II, Src: Vmware_18:44:06 (00:0c:29:18:44:06), Dst: IPv4mcast_00:00:05 (01:00:5e
⊞ Internet Protocol Version 4, Src: 10.0.3.2 (10.0.3.2), Dst: 224.0.0.5 (224.0.0.5)
⊟ Open Shortest Path First
  ⊞ OSPF Header
  ⊟ LS Update Packet
      Number of LSAs: 1
    ⊟ LS Type: Router-LSA
        LS Age: 8 seconds
        Do Not Age: False
      ⊞ Options: 0x02 (E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 10.0.2.3
        Advertising Router: 10.0.2.3 (10.0.2.3)
        LS Sequence Number: 0x80005201
        LS Checksum: 0xb3ce
        Length: 60
      ⊞ Flags: 0x00
        Number of Links: 3
      ⊟ Type: Transit  ID: 10.0.2.3        Data: 10.0.2.3        Metric: 30
          IP address of Designated Router: 10.0.2.3
          Link Data: 10.0.2.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 30
      ⊟ Type: Transit  ID: 10.0.3.3        Data: 10.0.3.3        Metric: 30
          IP address of Designated Router: 10.0.3.3
          Link Data: 10.0.3.3
          Link Type: 2 - Connection to a transit network
          Number of TOS metrics: 0
          TOS 0 metric: 30
      ⊟ Type: Unknown  ID: 0.0.0.0         Data: 0.0.0.0         Metric: 189
          Unknown link ID: 0.0.0.0
          Link Data: 0.0.0.0
```

Figure 9. *R2 flood the disguised LSA, R1 receives it and drops the packet, seeing it as the one it has sent as step 3.*

We then check the rt3 router' database that should be corrupted:



```
LS age: 17
Options: 0x2  : *|-|-|-|-|-|E|*
LS Flags: 0x6
Flags: 0x0
LS Type: router-LSA
Link State ID: 10.0.2.3
Advertising Router: 10.0.2.3
LS Seq Number: 80005201
Checksum: 0xb3ce
Length: 60
 Number of Links: 3

  Link connected to: a Transit Network
   (Link ID) Designated Router address: 10.0.2.3
   (Link Data) Router Interface address: 10.0.2.3
    Number of TOS metrics: 0
     TOS 0 Metric: 30

  Link connected to: a Transit Network
   (Link ID) Designated Router address: 10.0.3.3
   (Link Data) Router Interface address: 10.0.3.3
    Number of TOS metrics: 0
     TOS 0 Metric: 30

  Link connected to: Network Mask
   (Link ID) U����8�U^L�]�▯����▯ 0.0.0.0
   (Link Data) (null): 0.0.0.0
    Number of TOS metrics: 0
     TOS 0 Metric: 189
```

Figure 10. *OSPF database after the attack*

4. Discussion and Conclusion

Attacks were according to RFC2328 and new attack due to ambiguity in the definition of the protocol is achieved. These attacks may be the basis for the creation of more efficient attacks and destructive affects, however Cisco devices are vulnerable to the attack. All beliefs are broken about the attacks to this protocol and by the presented attacks a router can easily control all routing domains without enabling fight-back security mechanism.

References

[1] Russell Chris, Security of IP Routing Protocols, SANS Institute, Global Information Assurance Certification Paper, October 7, 2001.

[2] Andrew A. Vladimirov, Konstantin V. Gavrilenko, Hacking Exposed Cisco Networks, McGraw-Hill Companies, 2006.

[3] Michael Sudkovitch, David I. Roitman, OSPF Security Project – Technion Institute of Technology, 2010.

[4] Vanessa Antoine, Raymond Bongiorni et al, Router Security Configuration Guide, National Security Agency [C4-040R-02], 2005.

[5] Faraz Shamim, Zaheer Aziz, Troubleshooting IP Routing Protocols (CCIE® Professional Development), Cisco Press, 2002.

[6] Brian Vetter, Feiyi Wang, S. Felix Wu, an Experimental Study of Insider Attacks for the OSPF Routing Protocol, In 5th IEEE International Conference on Network Protocols, 1997.

[7] S. F. Wu, H.C. Chang, F. Jou, F. Wang, F. Gong, C. Sargor, JiNao: Design and Implementation of Scalable Intrusion Detection System for the OSPF Routing Protocol, DARPA Information Survivability Conference and Exposition. DISCEX'00, 1999 , Pages 69-83, IEEE Article, 1999.

[8] John Moy, OSPF Version 2, IETF RFC 2328, April 1998. https://www.ietf.org/rfc/rfc2328.txt

[9] Emanuele Jones, Olivier Le Moigne, OSPF Security Vulnerabilities Analysis, Internet Draft: draft-jones-ospf-vuln-01.txt, IETF 58 –RPSEC Working Group, November 2003.

[10] Daniel Mende, Rene Graf, Enno Rey, Christopher Werny, Burning Asgard, an Introduction to the Tool Loki, Black Hat Digital Self Defense Conference USA, 2010 Jul 05.

[11] Wendell Odom, CCNP ROUTE 642-902, Cisco Press, 2010.

[12] Infonetics Research, "Enterprise Routers Quarterly Market Share, Size, and Forecasts", May 2012

[13] Esmail Kaffashi, Hamid Rezaei rahvard, “Discovered a new security hole in OSPF routing protocol”, 16th conference of National Association of Electrical Engineering, Iran, Kazeroon, August 2013.