

# 컴퓨터네트워크 과제

## <OSPF Packet Capture Using Wireshark>

2017320122 김정규

### OSPF

OSPF란 Open Shortest Path First의 준말로 동적 라우팅 프로토콜로 대표적인 링크 상태 라우팅 프로토콜이다. 여기서 링크 상태 프로토콜이란, 인터넷에서 연결된 링크의 상태를 감시하여 최적의 경로를 선택한다는 것이다. 최적의 경로가 의미하는 것은 이것이 최단 거리 이거나, 또는 연결된 링크가 10M와 100M 등 속도를 비교를 하여 더욱 전송 속도가 빠른 링크가 될 수 있는 것이다. 주로 중-대규모 네트워크를 구성할 때 많이 사용하며 구역(area) 개념을 사용해 빠른 업데이트와 라우팅 테이블을 효과적으로 관리할 수 있다. VLSM을 지원하며, 여러 개의 라우팅 경로를 하나로 묶어주는 기능이 매우 뛰어나다. 각 구역이 설정을 기반으로 하기 때문에 한 구역의 변동사항은 다른 구역에 영향을 주지 않게 설정할 수 있어 안정적인 네트워크 구성이 가능하다. VLSM이 의미하는 것은 Variable Length Subnet Mask라는 의미로서, 네트워크를 묶을 때 호스트 숫자를 256개 단위로 묶거나 128개 단위 또는 64개 단위로 묶는 등, 가변적으로 네트워크의 규모를 형성할 수 있다는 의미이다. 즉 이렇게 네트워크를 가변으로 구성이 가능하므로 효율적인 네트워크의 구성이 가능하다.

### OSPF와 라우터

OSPF는 다른 서브넷에 대한 여러 링크의 트래픽 부하 균형을 맞추기 위해 백업 라우터를 포함한 여러 라우터로 복잡한 네트워크를 지원한다. 동일한 브로드캐스트 도메인이거나 포인트 투 포인트 링크의 양쪽 끝에 있는 인접 라우터는 OSPF 프로토콜을 통해 서로 통신한다. 라우터는 서로 탐지했을 때 보조를 형성한다. 이는 라우터가 Hello 프로토콜 패킷에서 자신을 식별할 때 시작된다. 이러한 식별에 따라 양방향 상태와 가장 기본적인 관계를 확립한다. 이더넷 또는 프레임 릴레이 네트워크의 라우터는 라우터 사이의 트래픽을 줄이는 허브 역할을 하는 지정 라우터(DR)와 백업 지정 라우터(BDR)를 선택한다. OSPF는 유니캐스트와 멀티캐스트 전송 모드를 모두 사용하여 "Hello" 패킷과 링크 상태 업데이트를 전송한다.

링크 상태 라우팅 프로토콜로서 OSPF는 다른 라우터와 라우팅 업데이트를 교환하기 위한 인접 관계를 설정 및 유지한다. 인접 관계 테이블을 인접 데이터베이스라고 한다. OSPF 라우터 2개가 동일한 서브넷의 멤버로 동일한 영역 ID, 서브넷 마스크, 타이머 및 인증을 공유하는 경우 인접 라우터가 된다. 본질적으로 OSPF 인접성은 두 라우터 사이의 관계로서, 서로 보고 이해할 수 있게 해주는 것이다. OSPF 인접 네트워크는 어떠한 라우팅 정보도 교환하지 않으며, 이들이 교환하는 패킷은 Hello 패킷이다. OSPF의 인접성은 선택된 이웃 간에 형성되어 라우팅 정보를 교환할 수 있다. 그러기 위해선 두 라우터는 먼저 이웃하고 있어야 한다. 또한 적어도 하나 이상의 라우터가 지정 라우터이어야 하며, 혹은 백업 지정 라우터(다중 액세스 유형 네트워크 상에서)이거나 지점 간 또는 지점 간 네트워크 유형에 의해 상호 연결되어야 두 라우터가 인접하게 된다. 이러한 관계를 형성하기 위해, 관계를 형성하는 데 사용되는 인터페이스는 동일한 OSPF 영역에 있어야 한다. 인터페이스는 여러 영역에 속하도록 구성될 수 있지만, 일반적으로 실행되지는 않는다. 두 번째 영역에서 구성되었을 때, 인터페이스는 보조 인터페이스로 구성되어야 한다.

## OSPF 메시지

OSPF는 다른 라우팅 프로토콜과 달리 사용자 데이터그램 프로토콜(UDP)이나 전송 제어 프로토콜(TCP)과 같은 전송 프로토콜을 통해 데이터를 전송하지 않는다. 대신에 OSPF는 IP 데이터그램을 직접 형성하여 IP 프로토콜 필드에 대한 프로토콜 번호 89를 사용하여 packaging한다. OSPF는 다양한 통신 유형에 대해 다음 5가지의 서로 다른 메시지 유형이 존재한다.

### 1) Hello Message

Hello 메시지는 인사말의 한 형태로 사용되는데, 라우터가 로컬 링크와 네트워크에서 다른 인접한 라우터를 발견할 수 있도록 한다. 메시지는 인접 기기들 간의 관계를 설정하고 OSPF가 자율 시스템이나 영역에서 어떻게 사용될 것인지에 대한 주요 매개변수를 전달한다. 정상 작동 중에 라우터는 정기적으로 이웃에게 hello 메시지를 보낸다(hello interval). 만일 라우터가 이웃으로부터 hello 메시지 수신을 중지하면, 정해진 기간(dead interval) 후에 라우터는 이웃이 다운되었다고 가정한다.

### 2) Database Description (DBD)

데이터베이스 설명 메시지에는 자율 시스템 또는 영역의 토폴로지에 대한 설명이 포함되어 있다. 그들은 한 라우터에서 다른 라우터로 영역에 대한 링크 상태 데이

터베이스(LSDB)의 내용을 전달한다. 대형 LSDB를 통신하려면 송신 장치를 마스터 장치로 지정하고 메시지를 순차적으로 전송하여 여러 메시지를 전송해야 할 수 있으며, 슬레이브(LSDB 수신자)는 acknowledgments로 응답한다.

### 3) Link State Request (LSR)

링크 상태 요청 메시지는 한 라우터에 의해 다른 라우터에서 LSDB 부분에 대한 업데이트된 정보를 요청하기 위해 사용된다. 메시지는 요청 장치가 더 많은 최신 정보를 원하는 링크를 지정한다.

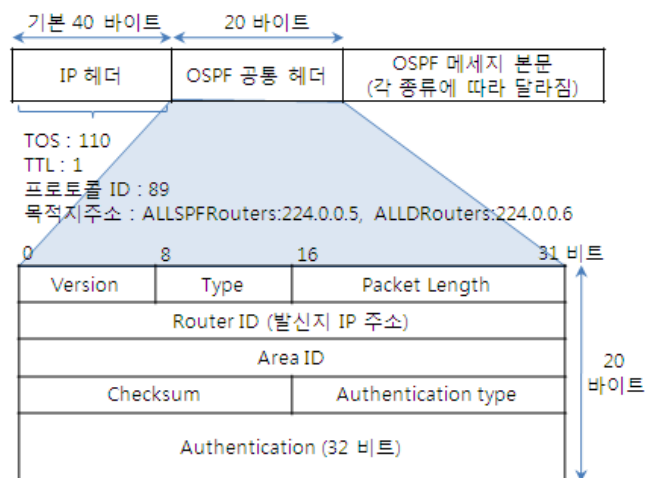
### 4) Link State Update (LSU)

링크 상태 업데이트 메시지에는 LSDB의 특정 링크 상태에 대한 업데이트된 정보가 포함되어 있다. 이들은 링크 상태 업데이트 메시지에 응답하여 전송되며, 또한 정기적으로 라우터에 의해 브로드캐스트 또는 멀티캐스트된다. 그들의 콘텐츠는 그것들을 받는 라우터의 LSDB에 있는 정보를 업데이트하는데 사용된다.

### 5) Link State Acknowledgment (LSAck)

링크 상태 확인 메시지는 링크 상태 업데이트 메시지의 수신을 명시적으로 승인함으로써 링크 상태 교환 프로세스에 신뢰성을 제공한다.

이러한 OSPF 메시지들은 24바이트의 공통 헤더를 가진다. 이 헤더는 Version, Type, Length, Router ID, Area ID, Checksum, Authentication type, Authentication value의 필드들로 이루어져 있다. 자세한 구조는 하단의 그림과 같다.



<OSPF 메시지 헤더 포맷>

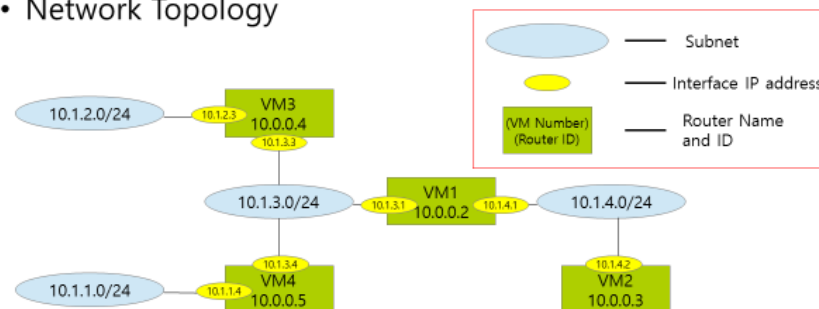
- ㄱ. Version (8 비트) : 패킷의 버전
- ㄴ. Type (8 비트) : 전송되는 메시지의 종류를 다음과 같이 표시
  - type 1 : Hello Packet
  - type 2 : Database Description Packet
  - type 3 : Link State Request Packet
  - type 4 : Link State Update
  - type 5 : Link State Acknowledgement
- ㄷ. Length (16 비트) : OSPF 헤더를 포함한 전체 길이
- ㄹ. Router ID (32 비트) :
  - OSPF 패킷의 발신지(생성지)가 되는 라우터를 식별하는 ID
  - 통상, 발신지 라우터 IP 주소
- ㅁ. Area ID (32 비트) : OSPF 패킷을 생성 및 발송하는 라우터가 속한 OSPF Area의 식별 ID
- ㅂ. Checksum (16 비트) : 16 bit CRC
  - . 인증 관련 필드들을 제외한 나머지에 대해 체크섬 계산(IP 패킷 체크섬 계산 방식과 유사)
- ㅅ. Authentication type (16 비트)
  - 0 : No Authentication, 1 : Simple Password Authentication, 2 : MD5
- ㅇ. Authentication value (64 비트)
  - 위 Authentication type에 따라 달라짐

## SPF 패킷 캡처

지금까지 정리한 OSPF의 개념과 역할에 따른 메시지의 이해를 기반으로 버추얼 머신의 우분투 4개로 OSPF 통신을 진행하였으며 과정에서 나타난 패킷들을 Wireshark로 캡처하고 분석하였다. 사용한 머신들 간의 네트워크 토폴로지와 각 머신들에서의 캡처본은 다음과 같다.

## Environment Setup

### • Network Topology



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
2	3.488470954	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
3	9.999279643	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
4	13.477618062	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
5	19.998788354	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
6	23.488694241	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
7	29.999578231	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
8	33.497818782	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
9	39.998716671	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
10	43.486384138	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
11	49.458576537	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
12	55.999338962	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
13	59.999618061	PcsCompu_8c:e0:10	ARP	62	Who has 10.1.4.1? Tell 10.1.4.2	
14	59.999884896	PcsCompu_85:2e:66	ARP	62	Who has 10.1.4.1? Tell 10.1.4.2	
15	59.999834840	10.1.1.1	10.1.4.1	OSPF	68	Description
16	59.999800201	10.1.1.1	10.1.4.2	OSPF	68	Description
17	59.999746138	10.1.1.1	10.1.4.2	OSPF	88	Description
18	59.999756338	10.1.1.1	10.1.4.1	OSPF	72	LS Request
19	59.999712939	10.1.1.1	10.1.4.2	OSPF	112	LS Update
20	59.999743581	10.1.1.1	10.1.4.1	OSPF	88	Description
21	59.999750019	10.1.1.1	10.1.4.2	OSPF	72	LS Request
22	59.999758295	10.1.1.1	10.1.4.1	OSPF	100	LS Update
23	59.999718886	10.1.1.1	10.1.4.2	OSPF	68	Description
24	59.999752538	10.1.1.1	224.0.0.5	OSPF	144	LS Update
25	59.999722271	10.1.1.1	224.0.0.5	OSPF	80	LS Acknowledge
26	59.999736509	10.1.1.1	224.0.0.5	OSPF	120	LS Acknowledge
27	59.999823999	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
28	59.999800459	10.1.1.1	224.0.0.5	OSPF	100	LS Update
29	59.999797821	PcsCompu_85:2e:66	ARP	62	Who has 10.1.4.2? Tell 10.1.4.1	
30	59.999817942	PcsCompu_8c:e0:10	ARP	62	Who has 10.1.4.2? Tell 10.1.4.1	
31	59.999834549	10.1.1.1	224.0.0.5	OSPF	144	LS Acknowledge
32	57.241954873	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
33	59.999535495	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
34	60.411577595	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
35	63.498178386	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
36	63.488741138	10.1.1.1	10.1.3.1	OSPF	68	Description
37	63.488733462	10.1.1.1	10.1.3.3	OSPF	68	Description
38	63.488806070	10.1.1.1	10.1.3.3	OSPF	120	Description
39	63.489554486	10.1.1.1	10.1.3.1	OSPF	96	LS Request
40	63.489427478	10.1.1.1	10.1.3.3	OSPF	100	LS Update
41	63.489938230	10.1.1.1	10.1.3.1	OSPF	88	Description
42	63.489991277	10.1.1.1	10.1.3.3	OSPF	72	LS Request
43	63.500233816	10.1.1.1	10.1.3.1	OSPF	100	LS Update
44	63.500288932	10.1.1.1	10.1.3.3	OSPF	68	Description
45	63.500308538	10.1.1.1	224.0.0.5	OSPF	144	LS Update
46	63.500327221	10.1.1.1	224.0.0.5	OSPF	100	LS Update

> Frame 36: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0

> Linux cooked capture

0000 00 00 00 01 00 06 00 00 27 29 55 20 00 00 00 ..... ']'-----

0010 45 c8 00 34 25 00 00 01 39 75 57 0a 01 83 03 E-Alt- Ym-----

0020 0a 01 83 03 02 02 00 20 0a 00 00 04 00 00 00 .....

0030 50 c3 00 00 00 00 00 00 00 00 05 dc 02 07 .....

0040 20 0a 30 21 .....o!

vm\_lspc.pcapng

Packets: 106 Displayed: 106 (100.0%)

Profile: Default

<VM1 Capture>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.1.1.1	224.0.0.5	OSPF	80	Hello Packet
2	0.01231929	10.1.1.1	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
3	0.513130883	10.1.1.1	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
4	0.549342084	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
5	0.549689787	PcsCompu_8c:e0:10		ARP	44	Who has 10.1.4.1? Tell 10.1.4.2
6	0.550278336	PcsCompu_85:2e:66		ARP	62	10.1.4.1 is at 00:00:27:a5:2e:66
7	0.550223838	10.1.1.1	10.1.4.1	OSPF	68	Description
8	0.550644099	10.1.1.1	10.1.4.2	OSPF	68	Description
9	0.550736696	10.1.1.1	10.1.4.2	OSPF	88	Description
10	0.550815790	10.1.1.1	10.1.4.1	OSPF	72	LS Request
11	0.551081126	10.1.1.1	10.1.4.2	OSPF	112	LS Update
12	0.551186384	10.1.1.1	10.1.4.1	OSPF	88	Description
13	0.551458420	10.1.1.1	10.1.4.2	OSPF	72	LS Request
14	0.551531519	10.1.1.1	10.1.4.1	OSPF	100	LS Update
15	0.551865840	10.1.1.1	10.1.4.2	OSPF	68	Description
16	0.551983881	10.1.1.1	224.0.0.5	OSPF	144	LS Update
17	0.551970881	10.1.1.1	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
18	1.307491821	10.1.1.1	224.0.0.5	OSPF	80	LS Acknowledge
19	1.307137942	10.1.1.1	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
20	1.587945582	10.1.1.1	224.0.0.5	OSPF	120	LS Acknowledge
21	4.752365340	10.1.1.1	224.0.0.5	OSPF	100	LS Update
22	5.840531214	PcsCompu_85:2e:66		ARP	62	Who has 10.1.4.2? Tell 10.1.4.1
23	5.846550870	PcsCompu_8c:e0:10		ARP	44	10.1.4.2 is at 00:00:27:9c:e0:10
24	6.811053080	10.1.1.1	224.0.0.5	OSPF	80	LS Acknowledge
25	7.797224996	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
26	10.354550857	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
27	14.957197487	10.1.1.1	224.0.0.5	OSPF	100	LS Update
28	14.251231816	10.1.1.1	224.0.0.5	OSPF	120	LS Acknowledge
29	15.687924423	10.1.1.1	224.0.0.5	OSPF	112	LS Update
30	17.893232778	10.1.1.1	224.0.0.5	OSPF	80	LS Acknowledge
31	17.794532706	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
32	20.359562338	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
33	25.740837182	10.1.1.1	224.0.0.5	OSPF	136	LS Update
34	25.790418438	10.1.1.1	224.0.0.5	OSPF	112	LS Update
35	26.312495817	10.1.1.1	224.0.0.5	OSPF	120	LS Acknowledge
36	27.794808957	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
37	30.363982241	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
38	37.795465289	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
39	40.568824536	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
40	47.794433712	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
41	50.374485633	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
42	57.794608955	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
43	60.370944829	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
44	67.794268388	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet

> Frame 12: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

> Linux cooked capture

> Internet Protocol Version 4, Src: 10.1.4.2, Dst: 10.1.4.1

> Open Shortest Path First

0000 00 04 00 01 00 06 00 00 27 5c e0 00 00 00 00 .....  
0010 45 c0 00 48 78 4d 00 00 01 39 24 4c 0a 01 84 02 E-Hdr- YSL----  
0020 0a 01 84 01 02 02 00 14 0a 00 00 03 00 00 00 ..... 4 .....  
0030 93 34 00 00 00 00 00 00 00 00 00 05 dc 02 01 .....  
0040 20 0a 30 21 .....o!

vmz.vpc.pcapng

Packets: 45 | Displayed: 45 (100.0%)

Profile: Default

<VM2 Capture>

vm2\_capt.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter:  Expression:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.1.1.4	224.0.0.5	OSPF	80	Hello Packet
2	0.811231929	10.1.1.4	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
3	0.511110893	10.1.1.4	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
4	0.545342084	10.1.1.1	224.0.0.5	OSPF	84	Hello Packet
5	0.549689787	PcsCompu_3c1e:10	10.1.1.4	ARP	44	Who has 10.1.1.4? Tell 10.1.1.4
6	0.550827036	PcsCompu_a5:2e:06	10.1.1.4	ARP	62	10.1.1.4 is at 08:00:27:a5:2e:06
7	0.552223352	10.1.1.4	10.1.1.4	OSPF	68	Description
8	0.550640499	10.1.1.4	10.1.1.4	OSPF	68	Description
9	0.550735696	10.1.1.4	10.1.1.4	OSPF	88	Description
10	0.550815790	10.1.1.4	10.1.1.4	OSPF	72	LS Request
11	0.551081126	10.1.1.4	10.1.1.4	OSPF	112	LS Update
12	0.551186384	10.1.1.4	10.1.1.4	OSPF	88	Description
13	0.551456426	10.1.1.4	10.1.1.4	OSPF	72	LS Request
14	0.551515155	10.1.1.4	10.1.1.4	OSPF	100	LS Update
15	0.551665846	10.1.1.4	10.1.1.4	OSPF	68	Description
16	0.551981031	10.1.1.4	224.0.0.5	OSPF	164	LS Update
17	0.551670903	10.1.1.4	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
18	1.574319121	10.1.1.4	224.0.0.5	OSPF	80	LS Acknowledge
19	1.575319441	10.1.1.4	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
20	1.587942562	10.1.1.4	224.0.0.5	OSPF	120	LS Acknowledge
21	4.752362340	10.1.1.4	224.0.0.5	OSPF	100	LS Update
22	5.445512124	PcsCompu_a5:2e:06	10.1.1.4	ARP	62	Who has 10.1.1.4? Tell 10.1.1.4
23	5.446530079	PcsCompu_3c1e:10	10.1.1.4	ARP	44	10.1.1.4 is at 08:00:27:3c1e:10
24	6.481951900	10.1.1.4	224.0.0.5	OSPF	80	LS Acknowledge
25	7.795214996	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
26	10.354550857	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
27	14.907197487	10.1.1.4	224.0.0.5	OSPF	100	LS Update
28	15.731310186	10.1.1.4	224.0.0.5	OSPF	120	LS Acknowledge
29	15.687920423	10.1.1.4	224.0.0.5	OSPF	112	LS Update
30	17.492121776	10.1.1.4	224.0.0.5	OSPF	80	LS Acknowledge
31	17.794519706	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
32	20.359563338	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
33	25.710637162	10.1.1.4	224.0.0.5	OSPF	136	LS Update
34	25.709436136	10.1.1.4	224.0.0.5	OSPF	112	LS Update
35	26.312495817	10.1.1.4	224.0.0.5	OSPF	120	LS Acknowledge
36	27.794809557	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
37	30.361982241	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
38	37.795405289	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
39	40.348824536	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
40	47.794637372	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
41	50.374409633	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
42	57.794658055	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
43	60.378944029	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
44	67.794268308	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet

> Frame 12: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

> Linux cooked capture

> Internet Protocol Version 4, Src: 10.1.1.4, Dst: 10.1.1.1

> Open Shortest Path First

```

0000  00 04 00 01 00 00 00 27 5c e0 10 00 00 00 00 00 00  .....
0010  45 c0 00 40 78 4d 00 00 10 24 c0 01 04 02 00 00 00  E-Hell-VSL...
0020  80 01 04 01 02 02 02 14 0a 00 00 03 00 00 00 00 00  4.....
0030  93 3d 00 00 00 00 00 00 00 00 00 05 dc 02 01 00 00  .....

```

vm2\_capt.pcapng

Packets: 45 - Displayed: 45 (100.0%)

Profile: Default

<VM3 Capture>

vm4\_capt.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter:  Expression:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.1.1.4	224.0.0.5	OSPF	80	Hello Packet
2	0.801000087	10.1.1.4	224.0.0.5	OSPF	80	Hello Packet
3	0.811090945	10.1.1.4	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
4	0.811170987	10.1.1.4	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
5	0.843128172	10.1.1.4	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
6	0.875644683	10.1.1.4	224.0.0.22	IGMPv3	56	Membership Report / Join group 224.0.0.5 for any sources
7	2.140472170	10.1.1.4	224.0.0.5	OSPF	80	Hello Packet
8	2.433648943	10.1.1.1	224.0.0.5	OSPF	88	Hello Packet
9	2.872781469	10.1.1.4	224.0.0.5	OSPF	84	Hello Packet
10	2.874064574	10.1.1.4	224.0.0.5	OSPF	68	Description
11	4.802274084	10.1.1.3	224.0.0.5	OSPF	88	Hello Packet
12	4.802447365	10.1.1.4	10.1.1.3	OSPF	68	Description
13	4.802532170	10.1.1.4	10.1.1.3	OSPF	68	Description
14	4.802616044	10.1.1.3	10.1.1.4	OSPF	68	Description
15	4.802825400	10.1.1.1	10.1.1.4	OSPF	168	Description
16	4.802825400	10.1.1.1	10.1.1.4	OSPF	168	Description
17	4.803081011	10.1.1.4	10.1.1.1	OSPF	120	LS Request
18	4.803180995	10.1.1.4	10.1.1.3	OSPF	120	LS Request
19	4.803234324	10.1.1.1	10.1.1.4	OSPF	208	LS Update
20	4.803362013	10.1.1.3	10.1.1.4	OSPF	208	LS Update
21	4.803433700	10.1.1.4	10.1.1.3	OSPF	88	Description
22	4.803510910	10.1.1.4	10.1.1.1	OSPF	88	Description
23	4.803590709	10.1.1.4	10.1.1.3	OSPF	168	LS Acknowledge
24	4.803754572	10.1.1.1	10.1.1.4	OSPF	72	LS Request
25	4.803741873	10.1.1.3	10.1.1.4	OSPF	72	LS Request
26	4.803830966	10.1.1.4	10.1.1.1	OSPF	100	LS Update
27	4.803964299	10.1.1.4	10.1.1.3	OSPF	100	LS Update
28	4.804170212	10.1.1.1	10.1.1.4	OSPF	68	Description
29	4.804266580	10.1.1.1	224.0.0.5	OSPF	136	LS Update
30	4.804384002	10.1.1.3	10.1.1.4	OSPF	68	Description
31	4.804374506	10.1.1.4	10.1.1.1	OSPF	88	LS Acknowledge
32	4.164476504	10.1.1.4	224.0.0.5	OSPF	112	LS Update
33	4.164086493	10.1.1.1	224.0.0.5	OSPF	112	LS Update
34	5.821604204	10.1.1.3	224.0.0.5	OSPF	120	LS Acknowledge
35	5.520954004	10.1.1.4	224.0.0.6	OSPF	100	LS Acknowledge
36	8.097161302	PcsCompu_3c1c:55	10.1.1.4	ARP	62	Who has 10.1.1.4? Tell 10.1.1.1
37	8.097275938	PcsCompu_32:87:69	10.1.1.4	ARP	44	10.1.1.4 is at 08:00:27:32:87:69
38	9.271361900	PcsCompu_32:87:69	10.1.1.4	ARP	44	Who has 10.1.1.1? Tell 10.1.1.4
39	9.271460809	PcsCompu_32:87:69	10.1.1.4	ARP	44	Who has 10.1.1.3? Tell 10.1.1.4
40	9.271707282	PcsCompu_3c1c:55	10.1.1.4	ARP	62	10.1.1.1 is at 08:00:27:3c1c:55
41	9.271718032	PcsCompu_29:5b:2d	10.1.1.4	ARP	62	10.1.1.3 is at 08:00:27:29:5b:2d
42	9.337879675	PcsCompu_29:5b:2d	10.1.1.4	ARP	62	Who has 10.1.1.4? Tell 10.1.1.3
43	9.337893206	PcsCompu_32:87:69	10.1.1.4	ARP	44	10.1.1.4 is at 08:00:27:32:87:69
44	12.166561340	10.1.1.4	224.0.0.5	OSPF	80	Hello Packet
45	12.439758097	10.1.1.1	224.0.0.5	OSPF	88	Hello Packet

> Frame 1: 88 bytes on wire (640 bits), 88 bytes captured (640 bits) on interface 0

> Linux cooked capture

> Internet Protocol Version 4, Src: 10.1.1.4, Dst: 224.0.0.5

```

0000  00 04 00 01 00 00 00 27 5c 5e c4 00 00 00 00 00 00  .....
0010  45 c0 00 40 69 4d 00 00 10 24 c0 01 04 04 00 00 00  E-BJ-VBQ...
0020  09 00 00 05 02 01 00 2c 0a 00 00 05 00 00 00 00 00  .....
0030  72 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00  .....
0040  00 5e c2 0a 00 00 23 0a 00 00 00 00 00 00 00 00  .....

```

vm4\_capt.pcapng

Packets: 65 - Displayed: 65 (100.0%)

Profile: Default

<VM4 Capture>

상기의 캡처본을 살펴보면 패킷의 정보에 앞서 설명한 패킷의 종류인 Hello, Description, Request, Update, Acknowledg가 모두 포함되어 있다는 사실을 알 수 있다. 여기서 각 머신마다 캡처한 패킷들은 크게 황색과 녹색으로 나뉜다. 황색 패킷들은 자신의 인터페이스들이 속한 서브넷들에 달린 모든 인터페이스가 보내는 멀티캐스트를 받을 수 있다. 반면 Description, Request, Update, Acknowledge에 해당하는, 다시 말해 라우팅 테이블을 바꾸는 역할인 녹색 패킷들은 같은 서브넷에 연결된 인터페이스끼리만 주고받는다라는 사실을 알 수 있다. 여기서 VM4를 기준으로 패킷들을 비교해보자. 황색 hello 패킷은 10.1.1.4, 10.1.3.1, 10.1.3.3, 10.1.3.4에서 224.0.0.5로 보내는 것을 받고 있는 반면, 라우팅 테이블 작업을 하는 녹색 패킷들은 10.1.3.4 <-> 10.1.3.1쌍과 10.1.3.4 <-> 10.1.3.3쌍에서 오간다. 이 패킷들은 멈추지 않고 지속적으로 나타나는데, 이를 확인해보면 자신들끼리도 여러 번 받고 있다는 사실을 알 수 있다. 이것이 시사하는 바는 현재 만들어진 최선의 라우팅 테이블을 보낸다 해도 그 후에 다른 머신에 의해 개선이 되고 이 과정을 반복하기 때문이다. 이 패킷들을 통해 알 수 있는 OSPF의 흐름과 동작의 구체적인 과정은 다음으로 정리할 수 있다.

1) OSPF를 설정한 라우터들끼리 hello 패킷을 교환해서 Neighbor 혹은 adjacent Neighbor 를 맺음

-> adjacent Neighbor : 라우팅 정보(LSA)를 교환하는 이웃

-> LSA(Link State Advertisement) : OSPF 에서의 라우팅 정보

2) adjacent neighbor인 라우터 간 라우팅 정보(LSA)를 서로 교환하고 전송 받은 LSA를 Link-state Database에 저장

3) LSA를 모두 교환하고 SPF(Shortest Path First) 또는 다익스트라 알고리즘을 이용하여 각 목적지까지의 최적 경로 계산 후 라우팅 테이블에 올림

4) 그 후에도 주기적으로 hello 패킷을 교환하면서 정상 동작 중인지 확인

5) 네트워크의 상태가 변하면 다시 위의 과정을 반복하여 Routing table 생성

## 참고문헌

John T. Moy, *OSPF Complete Implementation*, Addison-Wesley Professional, 2008.