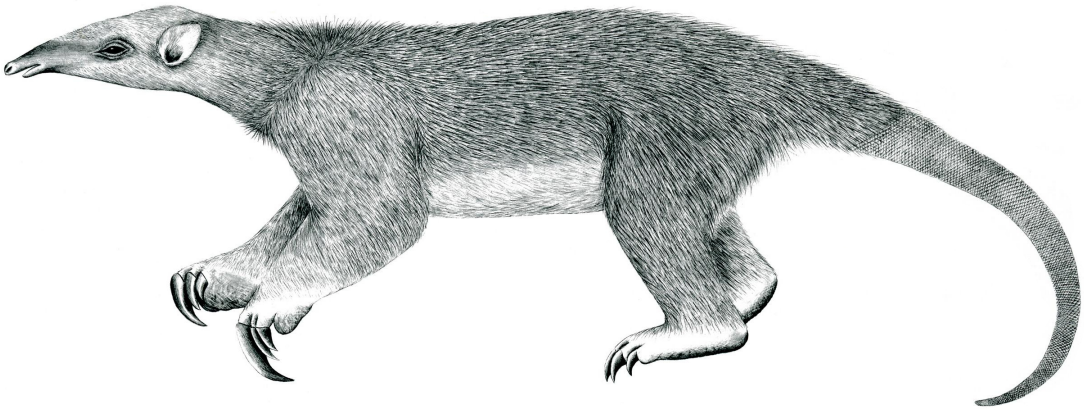
Tranalyzer2

ospfDecode

Open Shortest Path First (OSPF)



Tranalyzer Development Team

Contents

1 ospfDecode

1.1 Description

This plugin analyzes OSPFv4/6 traffic and provides absolute and relative statistics to the PREFIX_ospfStats.txt file. In addition, the rospf script extracts the areas, networks and netmasks, along with the routers and their interfaces (Section 1.7).

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
OSPF_OUTPUT_HLO	1	Output hello messages	
OSPF_OUTPUT_DBD	1	Output database description messages (routing tables)	
OSPF_OUTPUT_MSG	1	Output all other messages	
OSPF_OUTPUT_STATS	1	Output statistics file	
OSPF_MASK_AS_IP	1	Netmasks representation: 0: hex, 1: IPv4	
OSPF_AREA_AS_IP	0	Areas representation: 0: int, 1: IPv4, 2: hex	
OSPF_LSID_AS_IP	0	Link State ID representation:: 0: int, 1: IPv4	
OSPF_TYP_STR	1	Message type representation: 0: hex, 1: string	
OSPF_LSTYP_STR	1	LS type representation: 0: int, 1: string	
OSPF_NEIGMAX	10	Maximum neighbors to store	
OSPF_NUMTYP	10	Maximum number of LS types to store	OSPF_TYP_STR=1

In addition, the suffix for the output files can be controlled with the following flags:

Name	Default	Description
OSPF_SUFFIX	"_ospfStats.txt"	Statistics
OSPF_HELLO_SUFFIX	"_ospfHello.txt"	OSPFv2/3 hello messages
OSPF_DBD_SUFFIX	"_ospfDBD.txt"	OSPFv2/3 database description (routing tables)
OSPF2_MSG_SUFFIX	"_ospf2Msg.txt"	All other messages from OSPFv2 (Link State Request/Update/Ack)
OSPF3_MSG_SUFFIX	"_ospf3Msg.txt"	All other messages from OSPFv3 (Link State Request/Update/Ack)

1.2.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- OSPF_SUFFIX
- OSPF_HELLO_SUFFIX
- OSPF_DBD_SUFFIX
- OSPF2_MSG_SUFFIX
- OSPF3_MSG_SUFFIX

1.3 Flow File Output

The ospfDecode plugin outputs the following columns:

Column	Type	Description	Flags
ospfStat	H8	Status	
ospfVersion	H8	Version	
ospfType	H8/RS	Message type	OSPF_TYP_STR=0/1
ospfLSType	H64	Update LS type	
ospfAuType	H16	Authentication type	
ospfAuPass	RS	Authentication password (if ospfAuType == 0x4)	
ospfArea	U32/IP4/H32	Area ID	OSPF_AREA_AS_IP=0/1/2
ospfSrcRtr	IP4	Hello source router	
ospfBkupRtr	IP4	Hello backup router	
ospfNeighbors	R(IP4)	Hello neighbor router	

1.3.1 ospfStat

The hex based status variable (ospfStat) is defined as follows:

	ospfStat	Description
2^0	(=0x01)	OSPF detected
2^1	(=0x02)	OSPFv2 message had invalid TTL ($\neq 1$)
2^2	(=0x04)	OSPFv2 message had invalid destination
2^3	(=0x08)	OSPF message had invalid type
2^4	(=0x10)	OSPF unknown version
2^5	(=0x20)	—
2^6	(=0x40)	—
2^7	(=0x80)	OSPF message was malformed (snapped, covert channels?, ...)

The invalid checksum status 0x08 is currently not implemented.
The malformed status 0x10 is currently used to report cases such as possible covert channels, e.g., authfield used when auType was NULL.

1.3.2 ospfType

The hex based message type variable ospfType is defined as follows:

	ospfType	Description
2^0	(=0x01)	Not valid
2^1	(=0x02)	Hello
2^2	(=0x04)	Database Description
2^3	(=0x08)	Link State Request

	ospfType	Description
2^4	(=0x10)	Link State Update
2^5	(=0x20)	Link State Acknowledgement
2^6	(=0x40)	—
2^7	(=0x80)	—

1.3.3 ospfLSType

The hex based message type variable ospfLSType is defined as follows:

	ospfLSType	Description
2^0	(=0x0000 0000 0000 0001)	Reserved
2^1	(=0x0000 0000 0000 0002)	OSPFv2/3 Router-LSA
2^2	(=0x0000 0000 0000 0004)	OSPFv2/3 Network-LSA
2^3	(=0x0000 0000 0000 0008)	OSPFv2 Summary-LSA (IP network) OSPFv3 Inter-Area-Prefix-LSA
2^4	(=0x0000 0000 0000 0010)	OSPFv2 Summary-LSA (ASBR) OSPFv3 Inter-Area-Router-LSA
2^5	(=0x0000 0000 0000 0020)	OSPFv2/3 AS-External-LSA
2^6	(=0x0000 0000 0000 0040)	OSPFv2 Multicast group LSA (not implemented by Cisco) Deprecated in OSPFv3
2^7	(=0x0000 0000 0000 0080)	OSPFv2 Not-so-stubby area (NSSA) External LSA OSPFv3 NSSA-LSA
2^8	(=0x0000 0000 0000 0100)	OSPFv2 External attribute LSA for BGP OSPFv3 Link-LSA
2^9	(=0x0000 0000 0000 0200)	OSPFv2 Opaque LSA: Link-local scope OSPFv3 Intra-Area-Prefix-LSA
2^{10}	(=0x0000 0000 0000 0400)	OSPFv2 Opaque LSA: Area-local scope OSPFv3 Intra-Area-TE-LSA
2^{11}	(=0x0000 0000 0000 0800)	OSPFv2 Opaque LSA: autonomous system scope OSPFv3 GRACE-LSA
2^{12}	(=0x0000 0000 0000 1000)	OSPFv3 Router Information (RI)
2^{13}	(=0x0000 0000 0000 2000)	OSPFv3 Inter-AS-TE-v3 LSA
2^{14}	(=0x0000 0000 0000 4000)	OSPFv3 L1VPN LS
2^{15}	(=0x0000 0000 0000 8000)	OSPFv3 Autoconfiguration (AC) LSA
2^{16}	(=0x0000 0000 0001 0000)	OSPFv3 Dynamic Flooding LSA
2^{17}–2^{32}	are unassigned	
2^{33}	(=0x0000 0002 0000 0000)	OSPFv3 E-Router-LSA
2^{34}	(=0x0000 0004 0000 0000)	OSPFv3 E-Network-LSA
2^{35}	(=0x0000 0008 0000 0000)	OSPFv3 E-Inter-Area-Prefix-LSA

	ospfLSType	Description
2^{36}	(=0x0000 0010 0000 0000)	OSPFv3 E-Inter-Area-Router-LSA
2^{37}	(=0x0000 0020 0000 0000)	OSPFv3 E-AS-External-LSA
2^{38}	(=0x0000 0040 0000 0000)	Unused (not to be allocated)
2^{39}	(=0x0000 0080 0000 0000)	OSPFv3 E-Type-7-LSA
2^{40}	(=0x0000 0100 0000 0000)	OSPFv3 E-Link-LSA
2^{41}	(=0x0000 0200 0000 0000)	OSPFv3 E-Intra-Area-Prefix-LSA

1.3.4 ospfAuType

The hex based authentication type variable ospfAuType is defined as follows:

ospfAuType	Description
2^1 (=0x0002)	Null authentication
2^2 (=0x0004)	Simple password
2^3 (=0x0008)	Cryptographic authentication

1.4 Packet File Output

In packet mode (-s option), the ospfDecode plugin outputs the following columns:

Column	Type	Description	Flags
ospfStat	H8	Status	
ospfVersion	U8	Version	
ospfArea	U32/IP4/H32	Area ID	OSPF_AREA_AS_IP=0/1/2
ospfType	S	Message Type	
ospfLSType	H64	Update LS Type	

1.5 Plugin Report Output

The following information is reported:

- Aggregated ospfStat
- Aggregated ospfType for OSPFv2 and OSPFv3
- Number of OSPFv2 packets
- Number of OSPFv3 packets

1.6 Additional Output

- PREFIX_ospfStats.txt: global statistics about OSPF traffic
- PREFIX_ospfHello.txt Hello messages (see Section 1.7)

- `PREFIX_ospfDBD.txt`: Routing tables (see `OSPF_OUTPUT_DBD` in Section 1.2)
- `PREFIX_ospf2Msg.txt`: All other messages from OSPFv2 (see `OSPF_OUTPUT_MSG` in Section 1.2)
- `PREFIX_ospf3Msg.txt`: All other messages from OSPFv3 (see `OSPF_OUTPUT_MSG` in Section 1.2)

1.7 Post-Processing

1.7.1 rospf

Hello messages can be used to discover the network topology and are stored in the `PREFIX_ospfHello.txt` file. The script `rospf` extracts the areas, networks, netmasks, routers and their interfaces:

```
./scripts/rospf PREFIX_ospfHello.txt
```

```
Name    Area    Network          Netmask
N1      0       192.168.21.0     0xffffff00
N2      1       192.168.16.0     0xffffff00
N3      1       192.168.22.0     0xfffffffc
...

Router    Interface_n      Network_n
R1        192.168.22.29    N11    192.168.21.4    N5    192.168.22.25    N10
R2        192.168.22.5     N12    192.168.16.1    N0    192.168.22.1     N6
R3        192.168.22.10    N13    192.168.21.2    N5    192.168.22.6     N12
...

Router    Connected Routers
R0        R2    R4    R6    R7    R8
R1        R2    R4
R2        R0    R1    R4    R8
...
```

1.7.2 dbd

If `OSPF_OUTPUT_DBD` is activated (Section 1.2), database description messages are stored in a file `PREFIX_ospfDBD.txt`. The `dbd` script formats this file to produce an output similar to that of standard routers:

```
./scripts/dbd PREFIX_ospfDBD.txt
```

```
OSPF Router with ID (192.168.22.10)

Router Link States (Area 1)

Link ID          ADV Router       Age    Seq#          Checksum
192.168.22.5     192.168.22.5     4      0x80000002    0x38ce
192.168.22.10    192.168.22.10    837    0x80000002    0x6b0f
192.168.22.9     192.168.22.9     837    0x80000002    0x156c

Net Link States (Area 1)

Link ID          ADV Router       Age    Seq#          Checksum
192.168.22.6     192.168.22.10    4      0x80000001    0x150b
192.168.22.9     192.168.22.9     838    0x80000001    0x39e0
```

```
Summary Net Link States (Area 1)

Link ID         ADV Router       Age    Seq#           Checksum
192.168.17.0    192.168.22.9     735    0x80000001     0x5dd9
192.168.17.0    192.168.22.10    736    0x80000001     0x57de
192.168.18.0    192.168.22.9     715    0x80000001     0x52e3
...
```