ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

OSPF Route Monitoring and Efficient Quality of Service Implementation using Kruskal's Algorithm

Dipti Patnayak, Dr. A Rama Mohan Reddy

Research Scholar, Dept. of Computer Science & Engineering, Rayalseema University, Kurnool, India

Research Guide, Rayalseema University, Prof & HOD, Dept. of Computer Science & Engineering, S V University Tirupati, India

ABSTRACT: Open shortest path first is broadly spread in the network for purpose of managing the intra-domain routing. The OSPF is a Link State Protocol that the reliably floods the router using link state advertisement (LSAs) which helps in building the consistent and global view of routing topology. Reliable performance links to routing stability, but the behavior of huge operational OSPF network isn't properly understood. A case is examined where characteristics and dynamics of LSA traffic is considered for a large enterprise network. Numbers of routers are considered for the network. For construction of minimum spanning tree and the kruskal's algorithm is used.

KEYWORDS: Open Shortest Path First (OSPF) Protocol, Link State Advertisement (LSAs) Network, Kruskal's Algorithm.

I. INTRODUCTION

The stability and performance of routing system is dependent on the operational network performance. Understanding the routing protocols behaviour is necessary for the proper operation and management of IP networks [1]. Open shortest path first is focused in the work which is extensively deployed in Interior Gateway Protocol in IP networks for management of intra domain routing. Though OSPF is widely used, its behaviour in commercial and large IP networks isn't properly understood. The case study is considered for dynamic behaviour of OSPF in the environment of large enterprise IP network by making use of data gathering from novel and passive OSPF monitoring system deployment [2]. OSPF is one of the link state protocols generating the link state advertisement for creating and maintaining a local and consistent view of entire routing topology. In OSPF processing, generating and processing of LSA traffic are major chunk tasks.

Thus, understanding of LSA traffic dynamics are important to handle OSPF networks. This may also lead to models of realistic workload that are used for various purposes like realistic stability and simulations studies. The LSA traffic is investigated by introducing the general methodology and associated predictive model in order to reveal about the network topology and failure modes [5]. Under the investigation, the enterprise networks provide high available and reliable connections for application and database present in data centre from the customer's facilities. Salient features of the OSPF network are [3];

1. OSPF is used for routing in the data centre.
2. The domain of OSPF has hierarchical structure with respect to application and database servers at the root level and customers at the leaf level. The connectivity for domain use is Ethernet LANs. This is in comparison to ISP networks in which point to point link technologies are relied.
3. Customers are related over leased lines to the network of OSPF within the data centre. EIGRP is made to run over the leased lines. Customer reachability information is learnt through EIGRP is imported to OSPF domain subsequently.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

This is in contrast to many ISP networks which propagate external reachability information using an internal instance of BGP (I-BGP [1]).The LSA traffic of enterprise network is understood by the classifying the traffic into three categories:

- Refresh LSAs - these LSA classes are triggered by soft state refresh mechanism of OSPF.
- Change LSAs – these LSA classes are triggered by events leading to changes in the network status
- Duplicate LSAs—these LSA classes are extra copies which are received as redundancy result in OSPF reliable LSA flooding mechanism.

A. OSPF Fundamentals and LSAs

OSPF is link state routing protocol, which means that each router in domain discovers and builds an entire view of network topology. Each router here is indicated as node in the topology graph, and each link indicates the edge. Each link is associated with weight which is assigned to the configuration file of the router administratively. Shortest path tree is computed by each router using weighted topology graph with considering itself as root, and build the forwarding table. It is assured that packets get forwarded through the shortest paths to their destinations in terms of weights to the link.

An OSPF domain is partitioned into two level hierarchical areas for scalability as shown in Fig. 1. The backbone area is indicated by Area 0 which is resided at top level of hierarchy and it gets connected to non backbone areas which are indicated numbered as Area 1, Area 2 and so on. In OSPF each area is assigned with single link. The routers having links to multiple areas are known as border routers. A copy of topology is maintained with each router to its connected areas. The SPF is computed by router on topology graph and hence learns to communicate nodes in which area it is connected. Hence learns to communicate nodes in which area it is connected.

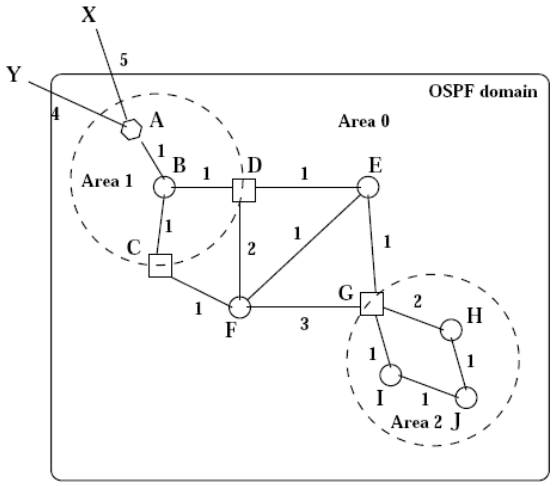


Fig. 1: Example OSPF topology, the view of that topology from router G, and the shortest path tree calculated at G.

Generally, entire topology of remote areas (i.e., the areas doesn't have links with the router) is not learnt by a router rather it learns the weights assigned to the shortest path from one area border router to each node residing in remote areas. Therefore, the router learns to use suitable border router as intermediate node to the remote node after SPF tree computation. Also the external IP prefixes (i.e., nodes associated outside the domain of OSPF) can be reachable if they are injected to OSPF domain.

B. Link State Advertisements (LSAs)

Routers running under OSPF domain describe its local connectivity in the Link state advertisements. These advertisements are reliably flooded to all routers in the network by which router builds consistent topological view of the network. Flooding is made to be reliable by allowing router to acknowledge of receiving LSA from each neighbor. This flooding takes place hop-by-hop and do not depends on routing. The router's memory for LSA is known as link state database and forms topology graph conceptually for the router.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

The term LSA is utilized for describing the OSPF messages and also entries in the link state database. There are two parts in LSA: identifier consisting of three parameters used to define topological element uniquely and rest of the content which describes status of topological element. Different LSA are used by OSPF to describe topology parts. Each router specifies links to each neighboring routers In LSA of routers for area. Only within an area, Router LSAs are flooded and said to have scope of flooding at the area level. Therefore, a border router needs to generate the separate router LSA to its connected areas. For example, Fig. 1 describes the router G linking to the routers E and F in area 0 route LSA, and in router LSA area 2, it links with H and I router. Network LSA is used for introducing routers that are attached to broadcast network by OSPF. These LSA also have scope of area level flooding.

Border routers summarize the data related to approximately one region into other through generating LSAs summary. The routers study about remote area nodes through the summary LSAs. For example, in Fig. 1, router G studies about A and B using summary LSA that is generated by C and D. As already mentioned, routing information is allowed to be imported from other routing protocols in OSPF. The router which is involved in importing routing information from other protocols is called as ASBR. External LSAs are generated by an ASBR for describing about external routing information. In Fig. 1, using external LSA which is generated by ASBR, all routers studies about X and Y. External LSA are flooded within domain irrespective to the boundaries of areas and thus can say that it is has flooding scope at the domain level.

Table 1: Summarizes This Taxonomy of OSPF's LSAs

LSA type	Information	Flooding Scope
Router	The router's OSPF links belonging to the area	Area
Network	The routers attached to the broadcast network	Area
Summary	The nodes in remote areas reachable from the border router	Area
External	The external prefixes reachable from the ASBR	Domain

A network topology changes requires appropriate LSA to originate flood by the affected routers. For an instance, when two routers comes up with an link, then router LSAs has to be originated and flooded by the two ends including the new link in it. OSPF periodically refreshes LSAs. Even in the topological changes, every router must periodically flood self originated LSAs. The default refresh period is 30 minutes [4]. Time expiration drives and jitters the refresh mechanism. Sometimes a router can get duplicate copies of changes or change triggered LSA because of LSA reliable flooding. The first copy at router received is considered as new and subsequently received copies are considered to be duplicates. Note that LSA types introduced in Table I are orthogonal to refresh or change triggered LSA, and new versus duplicate instances of an LSA.

II. METHODOLOGY

A. OSPF Operation over a Broadcast Network

As mentioned in the introduction, the enterprise network uses Ethernet LANs extensively to provide the capability of broadcast. Such broadcasting network is represented by hub-and-spoke topology by OSPF. One of router is selected as designated router. The DR generates a network of LSA that represents hub which describes links to other routers that associated to broadcast network [9]. In order to provide additional resilience, a backup Designated Router is elected by the router which is considered new DR in the case of failure of DR. There are two steps in the process of OSPF flooding over a broadcast network.

1. A router that is attached to network shares LSA to DR by passing it to special group of multicast DR-Routers. Only DR and BDR listen to this type of group.
2. The LSA is flooded back by DR to other routers on the network by passing it to special multicast group of All-Routers. In this case, all routers in network listen to this group.

The BDR also takes participation in the DR-router groups so that it is in sync with DR. But LSA is not flood by BDR to all routers till DR fails to flood [8].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

B. Enterprise Network Topology

Network Connectivity is highly reliable and available is provided by the enterprise network from the customer facilities to databases and applications present in data center. This network is designed to provide high degree of fault tolerance and reliability. Leased lines are used to interconnect Customer premise routers data center routers. An instance of EIGRP runs between leased lines end points. The main focus of the paper is the routers of the data center form an OSPF domain. In OSPF domain, customer reach ability information is imported as external LSA which is learnt through EIGRP. The small areas are formed like hub and spoke topology for scalability by dividing the OSPF domain. The databases and applications related to the servers hosting are connected to backbone area i.e., area 0 while the customers are connected to the non-backbone area routers [6].

Certain details related to the non-backbone area topology are studied here. The non-backbone area topology is shown in Fig. 2. The routers B1 and B2 are both connected to all areas (i.e, backbone area and non backbone area) and behave as border routers of OSPF domain. Every area will have two Ethernet LANs and all the routers present in the area get connected to these LANs. B1 and B2 routers provide interconnection among both two LANs by getting connected them. Other type of routers in the area gets connected to only one LANs. As customer-premise routers are not part of OSPF domain and data center routers are also not part of EIGRP domain, routers from one protocol needs to get injected to other for connectivity ensuration [11]. There router R in the area A is connected to customer router R', and it injects EIGRP routes as external LSAs into OSPF. Through configuration route is carefully injected and controlled. Enterprise network topology is depicted in Fig. 3.

C. OSPF Monitoring

The architecture in the OSPF monitor has two basic components: LSARs (LSA Reflectors) and LSAGs (LSA a Ggregators). An LSA device connects directly to network and captures OSPF LSAs, and reflects them to LSAG. The LSARs will get connected to LANs so that in receive LSAs by joining appropriate multicast group. At least one LSAS is connected to each area [9]. The partial adjacencies are formed by LSARs in point to point deployment.

1. Kruskal algorithm

The kruskal algorithm was first written Joseph Kruskal in the year 1956. In this algorithm, all the edges are arranged in non decreasing order and lowest edge is selected for minimum spanning tree construction. During implementation if any cycles are generated than the edges selected are eliminated from the graph and edges which are next lower are selected. The above step is repeated until (n-1) edges are added in the graph. Using simple data structure Kruskal's algorithm complexity is O (E log E) time, or equivalently, O (E log V) time. Where E is the number of edges in the graph and V is the number of vertices [1, 2 and 21]. The steps of Kruskal's algorithm are:

Step 1. The minimum weighted and unused edge is selected in Fuzzy graph

Step 2. The step 1 is repeated and edges are added to fuzzy graph till fuzzy circuit is created by addition of an edge.

Step 3. Repeat till fuzzy spanning tree is build.

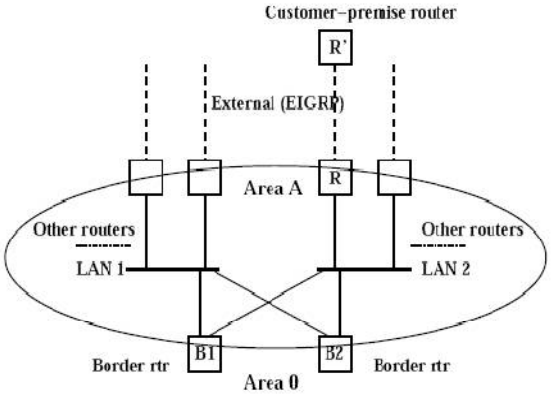


Fig. 2: Structure of a non-backbone OSPF area. All the areas are connected via two border routers B1 and B2.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

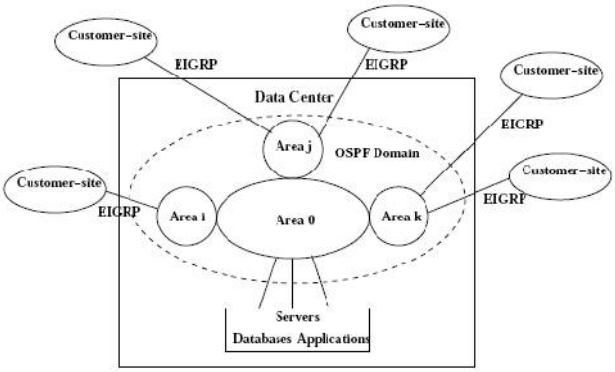


Fig. 3: Enterprise Network Topology

The Kruskal's algorithm is said to have following advantages over Dijkstra's algorithm:

- It is simpler algorithm: the kruskal's implementation need short program compared to dijkstra's implementation from the programming point of view. The kruskal's algorithm utilized two arrays known as father array and rank array from the data structural view to construct tree and Dijkstra's need minimum of three arrays, father relations weights and status along with priority queue.
- Time complexity of kruskal's algorithm is $O(m \log * n) + t(m)$, where $t(m)$ is time required for sorting m edges. Since many sorting algorithms are implemented, that are written as software and even coded in hardware. The time $t(m)$ is $m \log n$ time which is a very small constant. Beside the other end, In Dijkstra's algorithm is used for simple priority queue; each of deletion, operation and minimum operations takes c log n time with large constant c. Hence, it is observed as kruskal's algorithm is much faster than Dijkstra's algorithm.
- Since practically, sorting is done in linear time, Kruskal's algorithm runs in $O(m \log * n)$ time linearly.
- At last, it is observed as maximum spanning tree is not with respect to particular source and destination node. Hence the path with maximum bandwidth is provided by maximum spanning tree for any pair of source and destination node. On other side, dijkstra's algorithm provides path of maximum bandwidth only from fixed source and other nodes.

III. EXPERIMENTAL RESULT

The below steps are followed for LSA traffic analysis.

- Baseline: the refresh-LSA traffic is analysed for the baseline protocol, which arises from state of soft refresh. Particularly, the LSA traffic refreshment rate is predicted from data retrieved by configuration files of router, and then time series analysis is carried out for characteristics of fine time scale.
- Analyzing and fixing of anomalies: the change in LSA traffic and identification of root cause is closely observed. In the setting of this operation, the failure modes may be due to root cause of heavy hitter. Failure modes identification at incipient stages helps in proactive maintenance.
- Protocol overhead analyzing and fixing: the duplicated LSA traffic is observed and root cause for identifying the changes in the configuration to decrease the traffic is identified.
- Here we consider 3 OSPF areas. The Fig. 4 shows the different refresh, change and duplicates LSAs received by the OSPF areas.

Usually, the refresh – LSA traffic is constant for all the areas. But all the areas differ in change and duplicate LSA traffic. In the back bone area, i.e. Area 0 refresh LSA traffic is double in order of magnitude compared to change and duplicate LSA traffic. In non backbone area, though the physical topology is similar, it shows variations in change and duplicated LSA traffic [10]. In the area 2, the change LSA traffic is measurable while the duplicate LSA traffic is ignored because of negligible value. In area 3, it is observed that duplicate LSA traffic is measurable and duplicate LSA is found to be negligible.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

A. Refresh-LSA Traffic Prediction

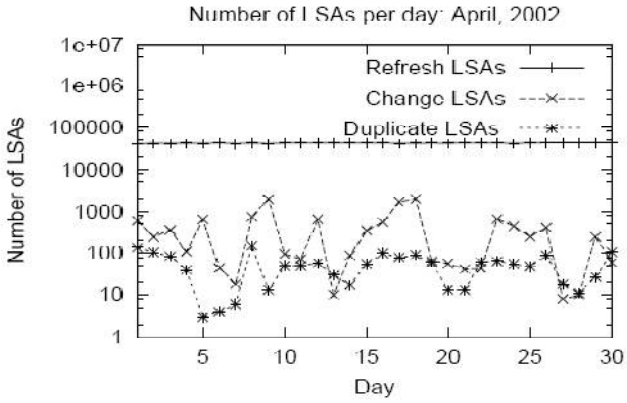
The refresh-LSAs average rate at a given router R is determined. To compute this, the set L_R of unique LSA-identifiers is constant in the database of router R's link-state i.e. the network elements which are not introduced or withdrawn.

Let us consider, in link state, database, the refresh average rate of a LSA l is denoted by F_l. Then Let assume that LSA set generated by the routers of OSPF domain is denoted by D, and the routers which receives a LSA l is denoted by S_l. Then L_R set can be represented as in Eq. (01).

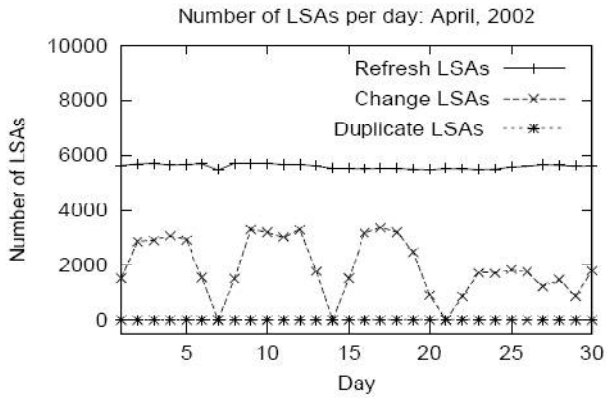
$$L_R = \{l \in D | R \in S_l\} \quad (01)$$

The Eq. (2) along with Eq. (2) determines N_R. Thus we can conclude that the refresh LSA traffic is estimated using following three parameters at a router:

$$N_R = \sum_{l \in L_R} F_l \quad (02)$$



(a) Area 0



(b) Area 2

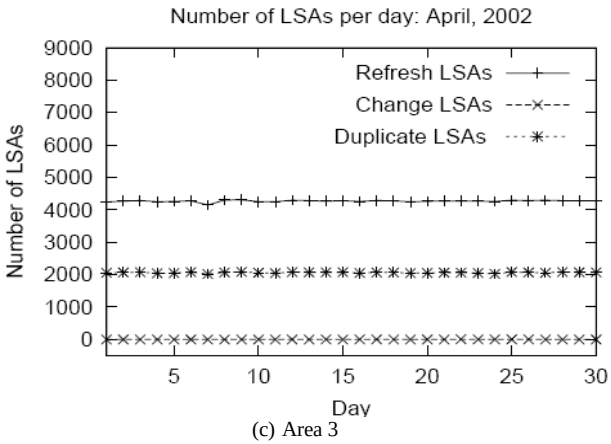
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018



(c) Area 3

Fig. 4: (a), (b), (c) Number of refresh, change and duplicate LSAs received at LSAR during each day in April.

- D, the LSA set generated by the routers present in the OSPF domain.
- For each LSA l in D, l is received by the set of routers S_l.
- In D, for each LSA l, the l is associated with refresh-rate F_l.

B. Change-LSA Traffic

The LSA are first classified as internal changes or external changes. We check for causes of internal external changes. Router and network LSAs are used to convey the internal changes within area where the changes takes place and outside areas by the summary LSAs. External LSAs are used to convey the external changes.

C. Root Cause Analysis

The area 0 is accounted for more internal changes in April. Most of the changes were because of internal error in crucial router of area 0. As this was DR in the area 0, due to error, some of the episodes at last few minutes at which damaged router will drop and adjacencies are re-established with other routers of LAN. Subsequently, flurry of change LSAs are produced at time of such kind of episodes. Each episode had only few minutes and on each day there were few episodes only. The data collected suggests that network was at risk during the episodes. These episodes accounts of total internal change-LSA of about 99% which was noticed in are 0. The basis of data collected by monitoring the OSPF, the changes the damaged router configuration in order to prevent it for DR selection and reboots it.

The network is stabilized and a topological change in area 0 is vanished. This depicts OSPF monitoring potential for failure modes localization, preventing serious failures by fixing the network in prior. The area 2 observes external change more. The external changes may cause by hanging of external links. In area 2, one of the routers maintains a link with customer premise router on which the EIGRP runs. 4 EIGRP routes are imported by router A into OSPF as external LSAs [7]. Closer observation of network conditions reveals that when the link between A and B is overhead than the EIGRP session between these routers starts hanging. Thus router A announces and withdraws EIGRP prefixes repeatedly through external LSAs.

D. Duplicate-LSA Traffic

We had observed that area 3 has received large amount of duplicate-LSA traffic while the area 2 has received very few duplicate-LSA traffic. As duplicate LSA processing will waste the resources of CPU, understanding the circumstances which may leads to the duplication of LSA traffic is necessary in some areas. Under study of enterprise network, the physical connectivity is identical at all areas. It surprises when one areas sees large amount of duplicate LSA traffic and while others not. Though the physical structure is same at all areas, the difference observed matters on low LSAs propagates through the areas. The DR and BDR behaviour is different compare to other routers present in the LAN. THE DR and BDR broadcasts the LSA to all other routers while other routers broadcasts LSA to DR and BDR only.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

The behaviour of LSA propagation depends on DR and BDR, how they are connected to the entire network. This analysis is complicated. Every area consists of two LANs; the LSAR is attached on single LAN. Let us consider LSAR resided LAN as LAN 1 and other as LAN 2. Both B1 and B2 are connected to both LANs, but other routers are connected to either of the LANs. The B1 and B2 are represented as B-pair and other routers are represented as LAN1 and LAN2 router, depending on the LAN the router is present. As B-pair is connected to both LANs, they the play the role of LAN 1 is significant to check LSAR received are duplicate LSAs or not. The B-pair router have different role in area 2 and area 3 that may arise various duplicate LSA traffic in various areas. There are four cases depending on play of B-pair routers in the LAN 1:

Case 1: {_ DR, BDR}
Case 2: { DR, regular}
Case 3: {BDR, regular}
Case 4: {regular, regular}

Table 2: DR and BDR on LAN 1 OF Various Areas

Area	DR on LAN 1	BDR on LAN 1	Cases above
Area 1	LAN 1 Router	B2	Case 3
Area 2	B2	LAN 1 Router	Case 2
Area 3	LAN 1 Router	B2	Case 3
Area 4	B2	LAN 1 Router	Case 2
Area 5	B2	B1	Case 1
Area 6	B2	B1	Case 1
Area 8	LAN 1 Router	B2	Case 3

In order to understand which the above cases leads to the cause of duplicate – LSA traffic in the LAN 1 area, LSA propagation is modelled on LAN 1. The L copies are received by B-pair routers on LAN 2 interfaces and propagate the LSA to LAN 1s LSAR. The L copies propagated through B1 and B2 are denoted as L1 and L2 respectively. Let us consider an example using case 1. Sending the LSA to LSAR by B pair routers depends on order of LSA arrived at these routers. It is necessary to one of B-pair routers to send LSA to LSAR on LAN 1. Another router also needs to send LSA to LSAR which is based on LSA order arrived at this router. If LSA on LSA2 is received first at the router, then LSA is received at LSAR and results in duplicate copy. In the case if at LAN 1 LSA is received first than LSA need not be send to LSAR. Hence no duplicate LSA will be received at LSAR

E. Avoiding Duplicate LSAs

The operator of enterprise network can prevent duplicate-LSAs by controlling the routers to become DR or BDR on LAN 1. This is based on complex election algorithm which is executed by all LAN routers. This algorithm takes priority parameter as input, each router interface is configured. As the priority is high, the probability of winning the election is also greater, even though only partial control is provided by these priorities. Thus, operator cannot force to apply case 2. Though highest priority is assigned to one of B pair and zero is assigned to other B pair by the network operator, it cannot be guaranteed that DR is the router having high priority. Here, the operator fortunately can use case 4 ensuring that none of the B pairs can become DR and BDR on LAN 1.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

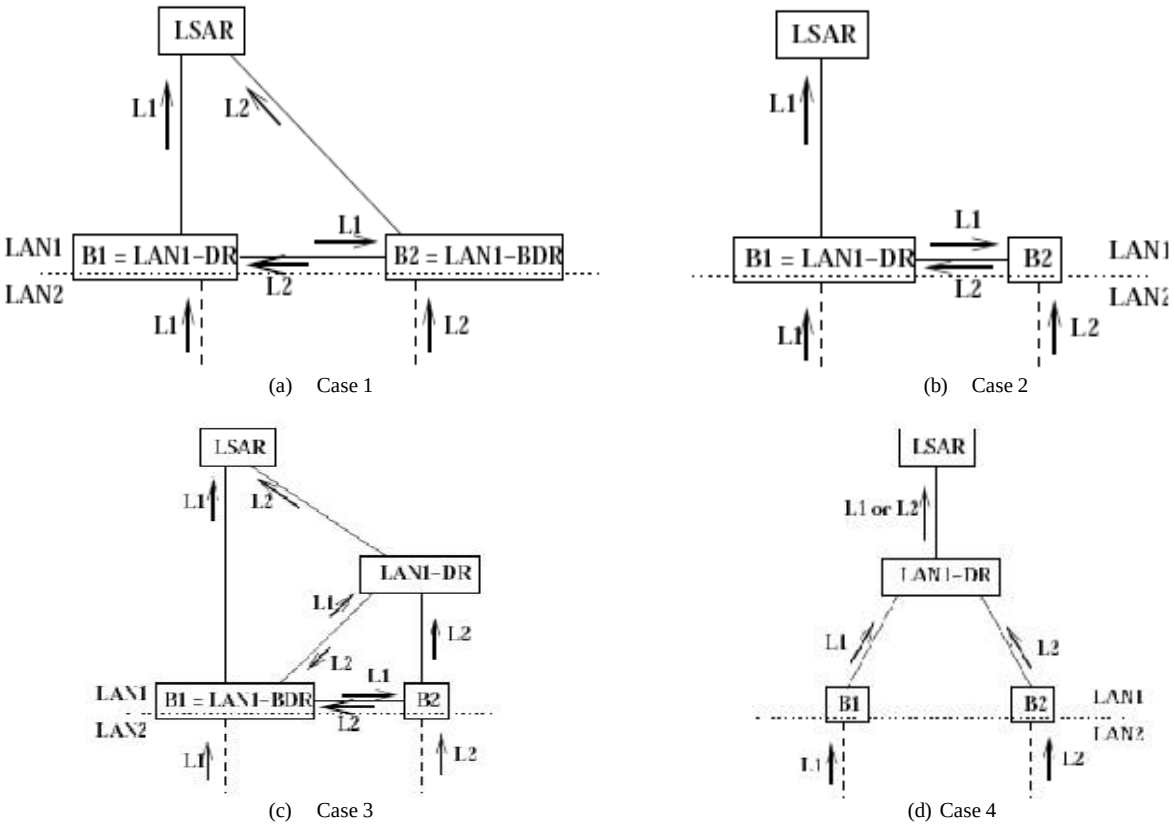


Fig. 5: Control-plane diagram for LAN 1 under different roles played by the *B-pair* routers. This figure also shows how different copies of LSA L can arrive at the LSAR via the *B-pair* router L1 and L2 are copies of LSA L.

.This can be accomplished by making the both routers priority as zero and so they are ineligible to get selected for DR and BDR. The forcing of case 4 is based on two factors. First, the DR and BDR have important role to be played on a LAN, and also need bear more OSPF processing load compare to load of regular routers on LAN. Thus, it is necessary for operator to ensure the suitable routers to become DR and BDR. The second factor is subtle. Reducing the duplicates of LSA requires the number of alternate path also to be reduced that occurs while reliable flooding. This may increase the propagation time of LSA, which also increases the convergence time. Using the above case 4, LSAs which get originated on the LAN 2 must use extra hop before LAN1 routers can receive. This indicates that if case 4 is forced than propagation time of LSA can increase. Overall flow is depicted in the Fig. 5.

IV.CONCLUSION

In this paper, OSPF behaviour is described in operational network. A general method is used to predict the refresh LSA traffic rates. It was found that topological change of LSA is due to external changes. As network will import customer reach ability information into domain, there is chances that customers may get added, or may be dropped or change in the connectivity. Duplicate-LSA traffic was also observed, a simple change in configures helps to reduce duplicate traffic, without affecting the physical structure of network.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 8, August 2018

REFERENCES

[1] Christian Huitema, "Routing in the Internet", Prentice Hall, 2000.
[2] Anindya Basu and Jon G. Riecke, "Stability Issues in OSPF Routing", Proc. ACM SIGCOMM, August 2001.
[3] Aman Shaikh, Mukul Goyal, Albert Greenberg, Raju Rajan, and K.K. Ramakrishnan, "An OPSF Topology Server: Design and Evaluation", IEEE, Vol. 20, No. 4, 2002.
[4] Aman Shaikh and Albert Greenberg, "Experience in Black-box OSPF Measurement", Proc. ACM SIGCOMM Internet Measurement Workshop (IMW), 2001.
[5] Craig Labovitz, Abha Ahuja, and Farnam Jahanian, "Experimental Study of Internet Stability and Wide-Area Network Failures", International Symposium on Fault-Tolerant Computing, 1999.
[6] Craig Labovitz, Rob Malan, and Farnam Jahanian, "Internet Routing Stability", IEEE, Vol. 6, No. 5, pp. 515–558, 1998.
[7] Craig Labovitz, Rob Malan, and Farnam Jahanian, "Origins of Pathological Internet Routing Instability, IEEE, 1999.
[8] John T. Moy, "OSPF : Anatomy of an Internet Routing Protocol", Addison-Wesley, 1998.
[9] John T. Moy, "OSPF Version 2," Request for Comments 2328, 1998.
[10] Anja Feldmann and Jennifer Rexford, "IP Network Configuration for Intra-domain Traffic Engineering," IEEE, 2001.
[11] Sally Floyd and Van Jacobson, "The Synchronization of Periodic Routing Messages," IEEE, Vol. 2, No. 2, pp. 122–136, 1994.