Journal of Computer Applications (JCA)
ISSN: 0974-1925, Volume IV, Issue 2, 2011

Traffic Control And Network Security In OSPF Without Filtering

Mr. Nikhil Hemant Bhagat [a,*], Ms. Rati Vilas Deshmukh [b,1]

Abstract— **The paper addresses the interoperability & network security issues, between Open Shortest Path First (OSPF) with filtering & OSPF without filtering. Furthermore, it shows how the OSPF without filtering concept serve to be more useful in controlling traffic without the device being disconnected from the network. The new non–filtering concepts of stubby, totally stubby, not so stubby, totally not so stubby areas in OSPF are therefore designed to gain maximum control over handling the routes thus ensuring the security. The applicability of this proposed algorithm is demonstrated through diagrams for different network architectures and traffic conditions. Description of such concepts and the interoperability issues between them with the suggestions how to make use of them are presented. Practical implementation of the presented issues and concepts was done and was found to be very effective in establishing Network Security.**

Index Terms — **Access lists, stubby, totally stubby, NSSA, Totally NSSA, Link State Advertisement**

I. INTRODUCTION

OSPF (Open shortest path first) is an open standard protocol that provides area wise networks to be created. [1] It works in a single autonomous system. After forming the topology, OSPF uses this topology to route the packets [2]. Each path is assigned a cost based on the throughput, round-trip time, and reliability of the link [3] . The sum of the costs across a particular path between hosts determines the overall cost of the path. Using the shortest path first algorithm the packets are routed along the path. OSPF routes packets along each path alternately, if multiple equal-cost paths exist between a source and destination address [4]. To control the traffic, filtering can be done [5]. This however is very tedious to configure as it lacks security. To gain more security and to get desired routes on a particular router or in a specific area, the concept of stub can be applied [6].

In this paper, we have had discussed the filtering using access lists & we had shown how the stub concept can be used to control traffic & add secured networks with desired routes in a particular area. This paper is organized as follows: Section 2 describes the filtering using access lists. The problems of access lists are stated in section 3. Section 4 & 5 describes LSA's and OSPF areas. Traffic control & network security without filtering is described in section 6 and conclusions are drawn in the final section.

Mr. Nikhil Hemant Bhagat [a,*], B.E. (EXTC) Student, Department of Electronics and Telecommunication, Lokmanya Tilak College of Engineering, Mumbai University, Maharashtra, India
(Email: nikhilhbhagat@gmail.com)
Ms. Rati Vilas Deshmukh [b,1], B.E. (EXTC) Student, Department of Electronics and Telecommunication, Lokmanya Tilak College of Engineering, Mumbai University, Maharashtra, India
(Email: ratid27@gmail.com)

II. FILTERING USING ACCESS LISTS

The access list is a group of statements which defines a pattern that would be found in an IP packet [7]. As each packet comes through an interface with an associated access list, the list is scanned from top to bottom in the exact order that it was entered for a pattern that matches the incoming packet. A permit or deny rule associated with the pattern determines that fate of the packet. The pattern statement also can include a TCP or UDP port number. There are many reasons to configure access lists, which are to provide security for your network, to provide traffic flow control, to filter packets that flow in or out of router interfaces and to restrict network use by certain users or devices[8].

III. PROBLEMS WITH FILTERING

The main issue with the access lists is that access list provide the facility of deny which completely stops the communication with that device on which the command is applied. Consider two routers R1 & R2 connected via serial link having 200 routes on router R1, where R1 is the Bank and the R2 is the investors' router respectively. But as they re in the same network, investors would be able to see the Bank accounts, which is threat to government's fund. So now the main goal is to restrict R2, from accessing the R1 routes. Under such circumstances, we are unable to apply the access list because it will completely disconnect the investors from the bank.

In order to achieve network security by not allowing the routes from R1, be seen on router R2 without disconnecting R1 from the network, the concept of filtering is not appropriate. Thus, the network security is obtained in OSPF without filtering by the use of concept called as "stub" which was found to be very efficient. The concept of stub can be well understood by understanding LSAs.

IV. LINK STATE ADVERTISEMENT

For the Internet Protocol, LSA is a basic communication means of the OSPF routing protocol [9]. Communication of router's local routing topology to all other local routers in the same OSPF area is done by LSA. Some LSAs are not flooded out on all interfaces, but only those that belong to the appropriate area. Thus the detailed information can be kept localized, while summary information is flooded to the rest of the network.

• Type 1 (Router LSA) - Every router generates router-link advertisements for each area to which it belongs. Router-link advertisements describe the states of the router's links to the area and are flooded only within a particular area [9].

• Type 2 (Network LSA) – Designated Routers generate network link advertisements for multi access networks, which describe the set of routers attached to a particular multi access network. Network link advertisements are flooded in the area that contains the network. The link-state ID of the type 2 LSA is the DR's IP interface address.

• Types 3 and 4 (Summary LSA) – ABRs generate summary link advertisements. Summary link advertisements describe the following inter area routes:
• Type 3 describes routes to the area's networks (and may include aggregate routes also).
• Type 4 describes routes to ASBRs .The link-state ID is the destination network number for
type 3 LSAs and the router ID of the described ASBR for type 4 LSAs.
These LSAs are flooded throughout the backbone area to the other ABRs. Type 3 LSAs are not flooded into totally stubby areas or totally stubby NSSAs. Type 4 LSAs are not flooded into any type of stub area.
• Type 5 (autonomous system external LSA) - ASBRs generate autonomous system external link advertisements. External link advertisements describe routes to destinations external to the autonomous system and are flooded everywhere except to any type of stub areas. The link-state ID of the type 5 LSA is the external network number.
• Type 6 (Multicast OSPF LSA) - These LSAs are used in multicast OSPF applications.
• Type 7 (LSAs for NSSAs) - These LSAs are used in NSSAs.
• Type 8 (External attributes LSA for BGP) - These LSAs are used to internetwork OSPF and BGP.

V. OSPF AREAS

The possible area types of OSPF are [10]: • Standard area-This default area type accepts all updates, and external routes.
• Backbone area- The backbone area is labeled area 0, and all other areas connect to this area to exchange the route information.
• Stub area- This area type does not accept information about routes external to the autonomous system, such as routes from non-OSPF sources. If routers need to route to networks outside the autonomous system, they use a default route, indicated as 0.0.0.0. Stub areas cannot contain ASBRs. An area can be made stub if it has same incoming and outgoing route physical connection.
• Totally stubby area [10] — This Cisco proprietary area type does not accept external autonomous system routes from other areas internal to the autonomous system. If a router needs to send a packet to a network external to the area, it sends the packet using a default route. Totally stubby areas cannot contain ASBRs.
• NSSA (Not so stubby area) — This area type defines a special LSA type 7. NSSA offers benefits that are similar to those of a stub area. They do not accept information about routes external to the autonomous system, but instead use a default route for external networks. However, NSSAs allow ASBRs, which is against the rules in a stub area.
• Totally NSSA - Cisco routers also allow an area to be configured as a totally NSSA which

Table1. Types of areas that can be defined to restrict particular LSA's

Area	Restrictions
Normal	None
Stub	No Type 5 AS-external LSA allowed.
Totally Stub	No Type 3, 4 or 5 LSAs allowed except the default summary route.
NSSA	No Type 5 AS-external LSAs allowed, but Type 7 LSAs that convert to Type 5 at the NSSA ABR can traverse.
Totally NSSA	No Type 3, 4 or 5 LSAs except the default summary route, but Type 7 LSAs that convert to Type 5 at the NSSA ABR are allowed.

allows ASBRs, but does not accept external routes from other areas. A default route is used to get to networks outside of the area.

VI. HOW THE TRAFFIC IS CONTROLLED & NETWORK SECURITY IS INCURRED?

To avoid use of excessive commands in filters i.e. in access lists, use of stub concept serve the purpose. It ensures security by displaying the default route instead of all routes. Moreover it has an additional advantage. It reduces the total number of routes arriving on that router thus reducing the load on that router and making it work efficiently. Consider there are 500 routes coming from Rip and 200 routes coming from R1. Now what to do if the R3 routes capacity is 300 routes? Thus to makes possible R3 is made stub as stub restricts LSA 4, 5. By doing this all 200 routes from R1 is accepted but the R4 routes are converted to default route 0.0.0.0 so the routes that approach are 201.

To aptly illustrate the network security rendered by total stubby area, consider R1 router as the bank, R4 is the regional office and R2 as the ABR as shown in the Figure1.

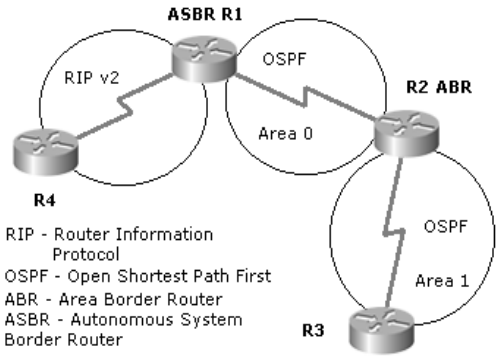

Figure1. Topology having RIP and OSPF protocols enabled in the redistributed network.

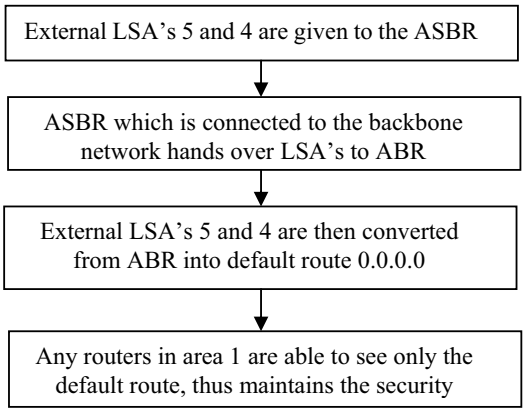

Figure2. Conversion in default route of external routes when area is made totally stubby.

R1 is running both the protocols on its interfaces. Rip is redistributed with OSPF for the routes to traverse. Now as R3 is the investor, he shouldn't be able to see the routes of the bank & its regional office as it would be a threat to accounts. But as they are in the same redistributed network the R3 will be able to see all the routes. To ensure this, area 1 is made totally stubby area. As it restricts LSA 3, 4, 5, R3 will get the default routes 0.0.0.0 from R4 and R1 and R3 would not understand which networks exists behind the default route. Figure 2 illustrates how the conversion in default route takes place if the area is totally stubby

In the live scenario, only one router is not used many routers are connected to the backbone area using virtual links. Now consider R3 has one more router connected i.e. R5 running EIGRP protocol having autonomous system 1 as shown in the figure2.

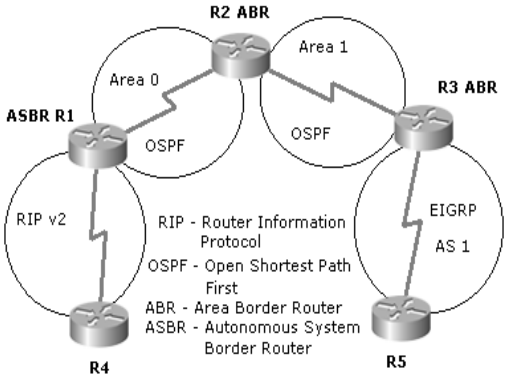

Figure3. Topology having RIPV2, OSPF & EIGRP protocols enabled in the redistributed network.

This is now redistributed with OSPF and the network is formed. Here if R5 is also the router connected to the investors & if they want to make transactions with the bank, it is impossible to make R4 stub as it is now ASBR. So R4 area 2 is made Totally NSSA which converts external type LSA's 3 ,4,5 into one default route 0.0.0.0 causing OIA and OE1/E2 to disappear. Then it converts the same area LSA 5 into type 7 and LSA 7 into type 5 again when it passes through ABR to the backbone area router. Thus security is again prevailed in spite of increase in number of routers.

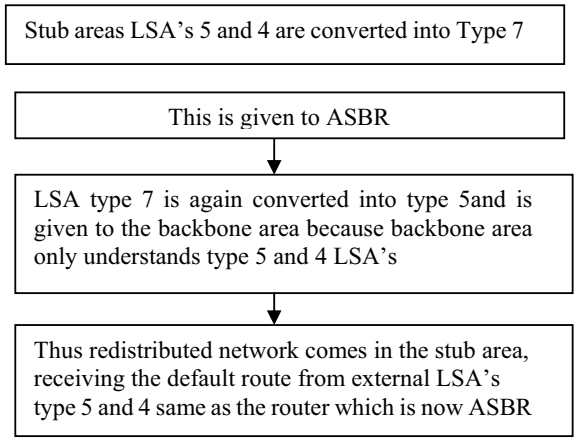

Figure4. Conversion of LSA's types when area is made totally not so stubby.

This configuration is done on the NSSA ASBR shown in the figure3. Figure 4 illustrates the conversion of the LSA types when the area is totally not so stubby.. Thus security is again prevailed in spite of increase in number of routers.

VII. CONCLUSION

The paper studies the fault recovery performance of the OSPF without filtering over filtering in terms of network security. The analysis highlights insightful features of Link state advertisements, concept of stubby, totally stubby, not so stubby area & totally not so stubby area and explains how to control the traffic and generate network security by laying restrictions on specific LSA's. Furthermore, the concept explains how the default route is generated without blocking completely any of the networks, which made us useful to apply in various areas, one of them is net banking.

VIII. ANALYTICAL ASSESSMENT

We have made practical implementation of these OSPF non filtering concepts in Network labs (CISCO) at Thane centre, and we further investigated the working of them, which was found to be very efficient in terms of traffic control and Network security.

REFERENCES

[1] Todd Lammle, *Cisco certified Network Associate study guide,* USA: Wiley publishing, 2007.

[2] Wendell Odom, *CCNP Route Official certification guide,* Pearson Education, 2010.

[3] OSPF fundamentals Article, *http://users.lmi.net/canepa/subdir/ospf_fundamentals.html, December 18,* 2005.

[4] Article Networking 101: Part 2 Understand the Rest of OSPF Protocol, *http://omnitraining.net/networking-101/93-networking-101-understanding-ospf-part-2*

[5] Issam, journal OSPF Filtering, *http://ciscoworlds.com/main/index.php?option=com_content&view=article&id=64:ospf-filtering&catid=41:latest-articles&Itemid=66*, june 17, 2011

[6] OSPF: Stub, totally stubby, not-so-stubby areas, The Network Journal,

http://cyruslab.wordpress.com/2010/10/09 /ospf-stub-totally-stubby-not-so-stubby-areas/ October9,2010.

[7] Access list, Article, *http://networking.ringofsaturn.com/Cisco/accesslists.php,* May 28, 2007.

[8] Samuel J Brown, Access Control Lists (ACLs) For Network security, *http://ezinearticles.com/?Access Control-Lists-(ACLs)-For-Network-Security& id=3095138,* October 15, 2009.

[9] Emmanuel Baccelli1, Juan Antonio Cordero2 and Philippe Jacquet3Équipe Hipercom, Inria Saclay, France, OSPF over multi-hop ad hoc wireless communications, Vol.2, No.5, September 2010.

[10] Cyruslab in OSPF, Route, OSPF: Special area types, *http://cyruslab.wordpress.com/2011/01/16/ospf-special -area-types/,* January 16, 2011.

BIOGRAPHY

Mr.Nikhil Hemant Bhagat is currently pursuing his Final year of B.E. Electronics and Telecomm. Engineering from Lokmanya Tilak College of Engg., Mumbai University, INDIA 2011-2012. He is the Head of the Department of Student Affairs committee of IEEE. He has also completed Network + technician and PC technician certifications from NIIT in the year 2010. He became Microsoft Certified in Dec. 2010 and was regarded as Microsoft Office Specialist 2007. He underwent practical experience in Mobile Communications from Mahanagar Telephone Nigam Ltd. (Govt. of India), Mumbai in June-July 2011. He went deep into Computer Networks by acquiring Cisco certifications like Cisco Certified Network Associate (CCNA Routing & Switching) in Aug. 2011 and Cisco Certified Network Professional (CCNP Routing & Switching) in Sept. 2011. He further assimilated couple of certifications like Windows XP Professional and IT Technology Professional 2010 from Ranksheet.com. He is currently targeting Cisco Certified Internet Expert (CCIE Routing and Switching) certification. His area of interests are Computer Networks, Neural Networks and Network Security.

Ms. Rati Vilas Deshmukh is the final year student of the (B.E) Bachelor of Engineering in the field of Electronics and Telecommunication in the Lokmanya Tilak college of Engineering affiliated to the University of Mumbai INDIA. She is one of the member of the IEEE. She had also taken the professional training and experience in the mobile Networking and Communication at the Mahanagar Telephone Nigam Limited INDIA and she had also successfully completed the converged communication course being held by Government of India in Mumbai Maharashtra in 2011. Her area of interest for further studies and research work lies in the Computer Networks, Neural Networks, Mobile and Wireless Communication.