Journal of Contemporary Issues in Business and Government Vol. 27, No. 04, 2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.04.047

Improving Failover time in Dual VIOS Network Virtualized Environment

[1]S.Annie Christila
[1]Associate Professor
Department of Computer Science, St. Francis de Sales College, Bangalore, Karnataka, India

ABSTRACT

Failover is a very important feature of network. Generally customers will be using dual path network environment. Whenever there is failure in one path, the path can be used and still the network communication can continue. If there is no failover setup network communication will be disturbed when there is failure in the path. Problem could on the switch / routers in that path. On virtualized environmentNetwork Interface Card(NIC) will be attached to VIOS(Virutal IO servers) and logical partitions will be sharing this NIC through virtualization technique using the bridge layer SEA (Shared Ethernet Adapter). SEA will be bridging the traffic between physical adapter and virtual adapters. Each of the LPAR(Logical Partition) will have virtual ethernet adapter (VEA) and will be communicating through SEA and physical adapter. In this paper, method to achieve faster failover when there is a failure identified in one path is being proposed in this draft.

Keywords: VIOS(Virtual IO Server), SEA(Shared Ethernet Adapter), NIC (Network Interface Card), LPAR (Logical PARtition), VEA (Virtual Ethernet adapter)

1. INTRODUCTION

Generally networks are configured with dual path. This is to ensure when one path goes down the traffic can go on other path. Problems could be with switches or any other intermediate devices. Users can achieve this by configuring dual VIOS in their environment. Both VIOS will be connected with separate switch and they will be connected to other intermediate devices to connect to network. When dual VIOS is configured user need to assign the priority. The VIOS which has high priority will be the primary VIOS and the other one will be secondary VIOS. All the LPARs will establish communication to outside using the primary VIOS. When LPAR initiates traffic outside for host A, then SEA on the primary VIOS will be forwarding it to the physical layer. When primary VIOS receives response from host A it will learn about host A and update the forwarding table in the SEA. SEA will be learning about the hosts to which LPARs are communicating through the responses and update the forward table. As this is dual VIOS environment the same information will be updated to SEA on the secondary VIOS periodically. This will ensure both VIOS maintains the information about hosts. In a scenario where the switch connected to primary VIOS gone bad or the primary VIOS itself gone bad, the secondary VIOS will be up to take care of the communication. However the data will still be routed to primary VIOS. In this paper will be discussing about the method how fast fail can be achieved.

2. PROBLEM STATEMENT

On virtualized environment, users will be configuring failover setup using dual VIOS. Both the VIOS will be connected to different switch and intermediate devices to connect to network. At any given time LPARs will be communicating to outside using single VIOS(It

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.04.047

could be either primary or backup). Shared Ethernet adapter on the VIOS through LPAR is communicating will be having forwarding table in which destination IP and MAC address will be stored. This information will be periodically updated to SEA on the other VIOS. Whenever any problem happens to the switch or the VIOS the communication will be lost. Even though the other VIOS will take over it will take 1 minute to resume the communication. This is due to forwarding table gets maintained on all the switches.

3. EXISTING METHOD

When TCP connection gets establishedLPAR will be sending TCP SYN packet. On receiving this packet, VIOS will be sending ARP request for the destination IP address. Upon receiving the ARP response the forwarding table will be updated in the VIOS. This operation will keep happen whenever any of the LPAR tries to communicate to any new host outside. As this is dual VIOS environment(failover environment), SEAs (Shared Ethernet adapter) on both VIOS will be communicating through virtual link. The primary SEA will be sending the forwarding table to the secondary SEA. The information will get exchanged periodically so that when secondary VIOS need to take over it can take over. The learning process and updating the forwarding table on both VIOS done periodically. Whenever there is problem with VIOS or with the switch connected to primary VIOS, communication from LPAR will not reach outside, similarly communication from outside will not reach LPAR. To avoid this both VIOS will be exchanging heartbeats periodically. If secondary VIOS doesn't get response for 3 consecutive heartbeats, it will be become primary VIOS and starts network traffic forwarding operation. However it takes1 minute to restore the traffic as forwarding tables in the switches need to be in synch.

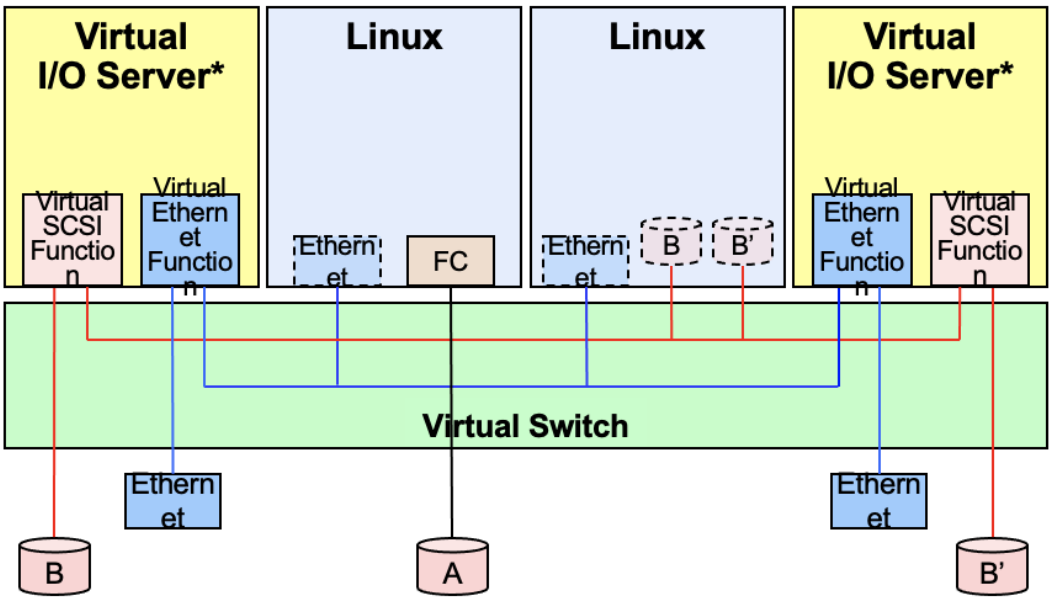

Figure 1. Failover Configuration - Dual VIOS setup

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.04.047

4. PROPOSED METHOD

In this paper, an algorithm to achieve fast failover is proposed. On VIOS at SEA layer information (Source IP, Source MAC, Destination IP, Destination MAC) about each IP configured on all of the LPARS will be maintained. This information will be sent to SEA on the secondary VIOS once in every 5 seconds.
This process helps to maintain forwarding table information at both sides in sync.
Failover is identified using heartbeat mechanism. Secondary VIOS will be sending heartbeats once every one second. If there is no heartbeat response for 3 consecutive heartbeat request, secondary VIOS will become primary and starts data forwarding operation. Also it will go through the current forwarding table and start sending RARP packet to the switch. As a result switch will learn about the MAC address and corresponding new ports associated with it. This process will ensure switches learn quickly about the new ports associated with MAC addresses and uses them for forwarding the data packets. We can also use Grat ARP instead of RARP.

We are sending the information only to the interfaces switches are connected (not on the virtual interfaces), no one else outside will be owning that MAC/IP address. Hence there won't be any response from outside.

ICMP message used for heartbeat communication between both SEAs (Primary and Backup). Periodic update on the forwarding table will happen. Data will have SourceIP, Source MAC, Destination IP and Destination MAC. Only the incremental update is sent to the other side.

RARP(Reverse Address Resolution Protocol) is used to update the switch about the port information related to specific MAC address.

Algorithm

1) During bringup phase both VIOS(SEA) will exchange heartbeats.
2) One of the VIOS will be acting as primary VIOS and the other one will be secondary VIOS. Primary VIOS will be responsible for data forwarding
3) SEA on primary VIOS sends out ARP request to the switch when any LPAR wants to establish the communication outside.
4) Periodically exchange the forwarding table information (Source MAC, Source IP, Destination MAC, Destination IP).
5) Keep exchanging the heartbeat information between both VIOS
6) When there is no response for the heartbeat requests, secondary VIOS will become primary VIOS.
7) Secondary VIOS will go through the forward table and for each entry, frame the RARP packet and send it to switch.
8) Switch upon receiving the RARP packet it will learn the port from which the packet is received.
9) As switch is having the correct information about the port and MAC address inward and outward traffic will reach the right VIOS.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.04.047

Bits	Bytes	Field
0—7	1	Hardware Address Space
8—15	2	
16—23	3	Protocol Address Space
24—31	4	
32—39	5	Hardware Address Length
40—47	6	Protocol Address Length
48—55	7	Opcode
56—63	8	
64—71	9	Source Hardware Address
72—79	10	
80—87	11	
88—95	12	
96—103	13	
104—111	14	
112—119	15	Source Protocol Address
120—127	16	
128—135	17	
136—143	18	
144—151	19	Target Hardware Address
152—159	20	
160—167	21	
168—175	22	
176—183	23	
184—191	24	
192—199	25	Target Protocol Address
200—207	26	
208—215	27	
216—223	28	

Figure 2. RARP Protocol format

5. CONCLUSION

The objective of the proposed method is to improve thefailover time when primary VIOS or the switch connected to primary VIOS is down by sending RARP packets from secondary VIOS to the switch for all the MAC addresses and IP addresses the LPARs are owning. As no host from outside are owning the MAC address or IP address there won't be any response from outside. However the switches will learn about new port corresponding to the MAC addresses. Failover will be immediate with very less network down time.

REFERENCES

1. **RFC 903RARP Protocol -** https://tools.ietf.org/html/rfc903
2. Hai Lin, Lucio Correia, Mel Cordero, Rodrigo Xavier, Scott Vetter, and Vamshikrishna Thatikonda - IBM PowerVM Virtualization
3. Gary R. Wright(Author), W. Richard Stevens - TCP/IP Illustrated, Vol. 2: The Implementation
4. Kumar Reddy, "Network Virtualization".P
5. Network Adapter Specification LSO feature – Intel