Professional paper / Stručni rad
Manuscript received: 2017-11-15
Revised: 2017-12-07
Accepted: 2017-12-11
Pages: 123 - 126

Alternative to using VRRP for Mutual Next-Hop Redundancy

Tomislav Trohar
University College Algebra
Zagreb, Croatia
trohar.tomislav@racunarstvo.hr

Silvio Papić
University College Algebra
Zagreb, Croatia
silvio.papic@racunarstvo.hr

Abstract: In a situation where customers end locations and its central infrastructure servers are connected over service provider MPLS (Multi Protocol Label Switching) network infrastructure, each customer site, including the central one is one MPLS connection. To ensure redundancy for the central location where the customer servers are located, most companies use two MPLS connections so that if one fails other will take over the traffic. For various reasons, some companies have not implemented a dynamic routing protocol, and all of their routing decisions are based on static routes, which is not a good solution. Such companies for purposes of routing redundancy choose to use FHRP (First Hop Redundancy Protocols) protocols in combination with interface tracking in both directions to ensure failover when needed. This combination is used to ensure redundant two-way communication that is resistant to one link or one device failure. In this paper, we describe the method of implementing VRRP (Virtual Router Redundancy Protocol) protocol in combination with interface tracking mechanism to ensure the availability of key elements of customer networks and present shortcomings of this model on the availability of customer infrastructure. Also, we will compare this solution with the conventional solution using a dynamic routing protocol.

Keywords: VRRP, interface tracking, next-hop redundancy, MPLS, routing

INTRODUCTION

Although this type of solution is not the best practice we saw that some of our clients are using this approach to connect to service provider network. This is probably due to insufficient knowledge about how to achieve redundancy using other means when connecting to service provider MPLS network. Described situation is regarding one of the banks in Croatia which uses multiple service providers MPLS infrastructure to connect their POS network to the core network where credit card transactions are terminated.

BRIEFLY ON VRRP

VRRP is one of the FHRP that is used in campus networks to achieve gateway redundancy. It is industry standard described in RFC 5798. When using VRRP two routers are configured to work together in one VRRP group sharing one virtual IP address and virtual MAC address. VRRP group corresponds to one IP subnet. This virtual IP address is used by all of the computers in the subnet as the default gateway. Using higher priority on one of the routers we can affect the election of the primary gateway (Master) so that we control which device will be used as the gateway when everything works fine. In the case of failure of the Master the other device (Backup) will after the timers expire assume the role of the Master. We can also track certain important interfaces so that if this interface fails Master will decrement its priority (100 by default) and enable backup device to become the Master. Using short VRRP timers in combination with interface tracking we can achieve very short failover times so that network communication is minimally disrupted [1]. This process is shown in the picture below.

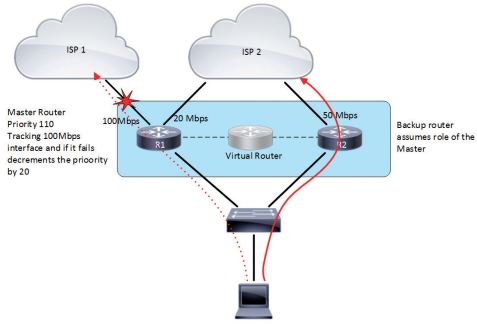

Figure 1 VRRP working principle

HOW IT WORKS IN CURRENT SCENARIO

On two main locations that are back up to each other banks infrastructure is connected to the ISPs MPLS network over two L3 switches. The two switches are connected to

each other over more than 10 kilometers using link aggregation. On each site service providers and banks, equipment is connected to these L3 switches to achieve VRRP connection between two sites. As far as the routing is concerned everything is done using static routing and using virtual routers IP address as the next hop address. One side is configured to be primary site using higher VRRP priority. On the switch, there are multiple VLANs, and every VLAN is used for one ISP to enable VRRP connection, a customer does the same thing in the corresponding VLAN with every service provider. Behind banks routers, there is a server farm that also uses VRRP and virtual IP address as the gateway. The principle is shown in the picture below.

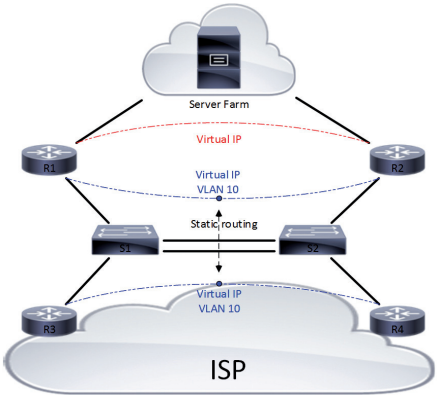

Figure 2 Current situation

In a case of a failure of any of the routers everything will work just fine because the remaining router will assume the role of the gateway or the next hop for static routing. Connectivity is retaind because switches still works. Failover time is in the range od few hundred miliseconds wich is adequate for this situation. To make this solution work routers also track different interfaces in order for VRRP to make the right failover decisions. And remember this is only one VLAN, and every ISP has it's own VLAN for VRRP. It is evident that this solution is very complex and impracticle to maintain. Sometimes it happens that after failed device came back on-line VRRP did not do what it soposed to do and the problem of communication persist untill manual intervention. One other problem is when one of the switches fails all routers transit to master state which causes routing problems. In short, FHRP should be used as it is intended which is for gateway redundancy in Campus Network design [2]. The same applies to other FHRP protocols [3].

PROPOSED SOLUTION

Much simpler and robust solution would be using one of the faster routing protocols between customer and ISP routers. Manipulating metric values we can achieve that traffic flows along one primary path, and in a case of failure, it can fallback to the alternative path or maybe BFD [4] (Bidirectional Forwarding Detection) mechanism. VRRP can still be used

on the customer server farm side with subsecond timers for gateway failover scenario. Service providers are already running MPLS L3 VPN backbone so for them, this would be a much more simple solution. Convergence times can be very short to accommodate customer needs, but the stability of the entire solution and the failover process is something that is much more important. Fast failover for this scenario is not the primary issue because credit card transactions are done manually by the salesperson anyway. In the case of failover only small part of card transactions are affected, and for a very short period of time. Proposed solution with one possible failure scenario is shown in the picture below.

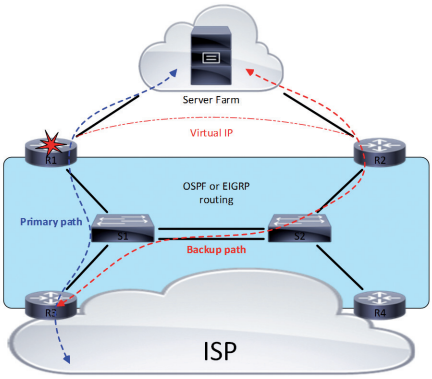

Figure 3 Solution using routing protocols

CONCLUSION

Although it is possible to use different methods to solve this problem it is very important to think about how any of chosen solutions will impact actual network redundancy, failover times, and how manageable the solution will be. In the case of using First Hop Redundancy Protocols in this type of situation, it is evident that it is very complex, and has unintended consequences when a failure actually happens. Generally, we should stick to simple and robust solutions, especially if failover times are not the primary issue.

REFERENCES

[1] Kocharians, N. and Paluch, P. (2015) CCIE Routing and Switching v5.0 Volume 1 Fifth Edition

[2] (2017-12-05) https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

[3] (2017-12-05) https://blog.serverfault.com/2010/07/18/828122846/

[4] (2017-12-05) https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.html