ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
www.computerscijournal.org

ISSN: 0974-6471
December 2011,
Vol. 4, No. (2):
Pgs. 399-404

HSRP (Hot Stand by Routing Protocol) Reliability Issues Over the Internet Service Provider's Network

ABHISHEK KUMAR SINGH and ABHAY KOTHARI

[1]Department of Computer Application, Shivdan Singh Institute of Technology and Management Aligarh (India).
[2]Principal, Indore Institute of Science & Technology-II Indore (India).
*Corresponding author: E-mail: abhinuvanu@gmail.com

(Received: November 04, 2011; Accepted: November 10, 2011)

ABSTRACT

With the appearance and expansion of Internet subscribers all over the world, ISPs services are becoming more popular. The rapid increase of connection-demand and highly traffic network is the main reason behind the need to scale reliable network. To offer better solutions, a new theoretical and practical approach should be considered that can cover the reliable network.

Key words: Internet Service Provider (ISP), Hot Standby Routing Protocol (HSRP), Virtual Local Area Network in Virtual Local Area Network (VLAN in VLAN (QinQ)).

INTRODUCTION

Today users want higher bandwidth Internet connection without the extra burden in terms of expenses and advanced modems. The Internet service providers (ISPs) have had a great impact for delivering high bandwidth Internet connections to the subscribers. The ISP is a way for users to connect to the Internet services. The ISP enters into business arrangements for connectivity with other service providers to make sure that the customer's data is able to move smoothly among the various parts of the Internet. The average rates of customers are connected to the ISP network through dial-up modem or broadband connection. For convenient services to the Internet subscribers, ISP maintains connections with the efficient use of network devices and bandwidths.

ISP provides the capable communication to connecting the remotely offices.

Problem Definition

Redundancy and load balancing are crucial issues facing anyone implementing high-throughput connections to the Internet. The demand for the Internet application services is increasing. It is vital that a better communication framework is implemented, which resolves present problems and also give the reliable solution to the ISPs network.

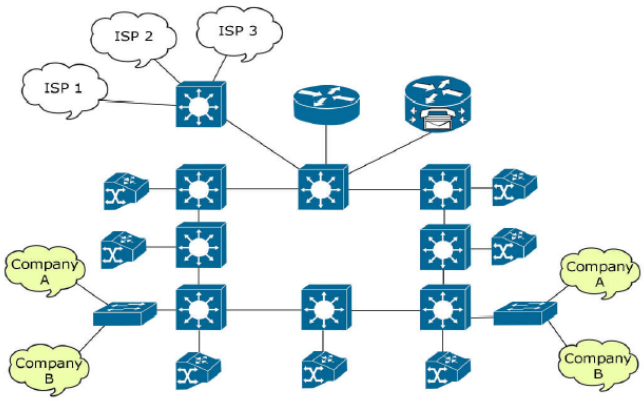

Fig. 1: Running ISP network infrastructure

In the above figure ISP network, problem is based on reliability currently this problem has been covered by Rapid spanning tree protocol (RSTP); but still it does not provide the load balancing solution. Furthermore, RSTP does not provide the fast re-convergence when network topology has changed occur. Thus any real time packet loss during route re convergence cannot be recovered and this loss more or less depends upon the selection of protocol in the available network topology.

Load balancing is the technique to spread the network traffic for the optimal network resource utilization. This uses a single link increase the reliability of network instead of using multiple devices and links for load balancing. For example, if one link fails then an alternative path will take over the network traffic quickly in order to provide the fastest and most reliable packet forwarding. If the network does not provide any redundancy link, the entire network may fail due to a single link failure. Redundancy is defined as a duplication of components or devices that allows continued functionality despite the failure of an individual component. In the suggested network, redundancy and load balancing increases the reliability and reduce the downtime that is caused by a single point of failure.

Redundancy and Load Balancing

Most of companies require network infrastructure without interruption of the services. *Redundant link* is one of technique to achieve the backup link, if master link fails. Redundancy is good approach to solve the fault tolerance issues in the network. One of the keys to make redundancy work for fault tolerance problems is the mechanism for switching to the backup. The network redundancy should be the primary consideration for automated fault recovery. It is clearly an important way of improving reliability in a network, particularly reliability against failures.

There are two approaches which can be used to support the load balancing such as software based load balancing and hardware based load balancing. In the hardware load-balancing, devices use numerous factors to make a decision relating to how to route the traffic. The device will examine the traffic or by pass the traffic to other devices to process and optimize the load across the traffic.

Redundancy and Load balancing provides optimized resources and reliability. Some protocols are loop free like spanning tree protocol (STP), rapid spanning tree protocol (RSTP) and these do not provide the load balancing. There are different protocols which provide the redundancy and load-balancing in the network. There are hot standby routing protocols (HSRP), virtual redundancy routing protocols (VRRP) and gateway load balancing protocols (GLBP), which provide the best features.

We review the different protocols and compare them later on, to decide which protocol is efficient for providing redundancy, load-balancing and minimizing the failover time.

Spanning Tree Protocol (STP)

Spanning tree protocol (STP) is a link management protocol. It provides a loop free network. If there are alternate links to a destination on a switch then only one link is responsible for forwarding the traffic. The spanning tree algorithm runs on a switch to activate or block redundant links. The spanning tree algorithm determines any redundant path. If it is there, it chooses which path will be utilized to forward frames and which path to be blocked.

The blocked link cannot forward traffic. However, the interface in blocking mode continues to listen, for changes in network topology. If a link or interface fails, the spanning tree process begins again. The STP typically takes between 30 to 60 seconds to "converge". Convergence occurs when switches and bridges define a stable tree and traffic can pass freely around the network. For many networks, convergence time of 30 to 60 seconds is simply too high. Thus, it is required to enhance the STP, to achieve faster convergence times for redundant link.

Rapid Spanning Tree Protocol (RSTP)

Rapid spanning tree protocol (RSTP) is the enhancement of the spanning tree protocol (STP) 802.1D. RSTP helps with convergence issues that plague legacy STP. RSTP has additional features similar to Uplink Fast and Back bone Fast that offer better recovery. RSTP requires a full-duplex point to- point connection between adjacent switches to achieve fast convergence. RSTP speeds the recalculation of the spanning tree when the layer 2 network topology changes. The STP takes 30 to 50 seconds to re-converge the network, but the RSTP protocol reduces it. RSTP is designed to provide faster recovery convergence time from topology changes. RSTP adds a new port designation for the recovery of the failover network. This alternate port acts as a backup port to the root port, if active link fails.

Converge Time

Only three states are lying in the RSTP: discarding, learning and forwarding. RSTP skip the listening state and blocking state. RSTP reduces the re-convergence network failure time by skipping the time-consuming listening and learning stages. RSTP is backward compatible with the STP. In the case of STP BPDU receives, the STP standard should work in conjunction with the switch port. The result increases the recovery time of the network because the switch works with STP states (five states). Therefore, in the RSTP the re-converge time is shorter because of forward delay only, which is equal to 15 seconds. This convergence time is also very high for a large network.

HSRP (Hot Standby Routing Protocol)

Hot standby routing protocol (HSRP) provides a mechanism to support non disrupting failover network. It allows the devices to use a single virtual default gateway to transmit the traffic. HSRP allows one router to resume the function of a second router if the first router fails [3]. HSRP is useful for critical networks that need a failover router for network reach ability. HSRP uses a priority scheme to determine the default active router. If the router is configured with a higher priority, it acts as an active router. By sharing an IP address and a MAC (Layer 2) address, multiple routers can act as a single "virtual" router and this virtual router can be configured as the default gateway. Frames are sent to the virtual router's address and processed with virtual router group, because the HSRP works in the group and forwards to the destination address.

HSRP Group

In HSRP, a set of routers work in concert to present the illusion of a single virtual router to the hosts on the LAN. The set is known as an HSRP group or a standby group. In the HSRP each router is assigned a specific role within the group because an HSRP group consists of the following: Active Router, Standby router, Virtual router, other router. In the HSRP standby group, the set of routers are jointly emulating a virtual router.

It is possible to share some traffic with the standby router. HSRP offers different features including groups and priority. It is possible to achieve the load balancing by applying the HSRP features such as priority on each different VLAN or by the standby groups on different routers. HSRP provides redundancy very efficiently. It optimizes the traffic and reduces the re-convergence time in the network.

Gateway Load Balancing Protocol(GLBP)

Gateway load balancing protocol (GLBP) is a successor of HSRP. It is similar to HSRP; however GLBP is able to use multiple physical gateways at the same time. GLBP allows the automatic selection, simultaneous use of multiple gateways, and automatic failover between those gateways. Multiple routers share the load of frames that, from a client perspective, are sent to a single default gateway address. With GLBP, resources can be fully utilized without any burden.

GLBP has one active virtual gateway (AVG) router as a master router and other routers are actual virtual forwarding (AVF). The GLBP uses full resources without the CPU overhead on one router. GLBP allows automatic selection for AVG and AVF by using the priority. If the priority is same, the MAC addresses are used for the selection of the AVG and AVF routers. GLBP also uses multiple gateways and automatic failover for gateways.

As if we compare the re-converge time it is same as the HSRP, it holds 10 seconds for network re-converge, then the higher priority AVF act as AVG. GLBP provide one extra feature that is load balancing. However, the problem with GLBP is that it supports only specific Cisco catalyst switches.

Ether channel

Ether channel provides the higher bandwidth with lower cost overheads. Ether channel allows the two, four or eight physical Ethernet links between the two devices to create one logical Ethernet link for providing high-speed and fault-tolerance links.

The Ether channel allows these features and has the following advantages:

- It allows a very high bandwidth logical link
- It configures only on the logical interface
- It provides the Load balancing among the physical links involved.

Comparisons among RSTP, HSRP and GLBP

A network with high availability provides alternative means by which all infrastructure paths and key servers can be accessed at all times. RSTP, HSRP and GLBP have software features that can be configured to provide redundancy to the network host. These protocols provide immediate or link specific failover and a recovery mechanism. Here a major issue arises, as to which protocol is best to provide the high availability with load sharing.

If we compare these protocols (RSTP, HSRP and GLBP), it can be agreed that HSRP offers intrinsic features for providing redundancy and load sharing.

Take a look at HSRP, GLBP and RSTP main characteristics. Some states are the same but some HSRP states are advantageous over RSTP and GLBP.

Hello Message

With the redundant link, a set of router works by sharing an IP address and a MAC (layer 2) address. Two or more routers act as a single router [4]. For identifying the presence of redundant link or device the 'hello' message is used. The hello message generates bridge protocol data units (BPDU) every three seconds for a keep alive mechanism. The bridges send and receive keep alive messages in HSRP between bridges using the multicast address 224.0.0.2.

Failover Time

The aim of RSTP, HSRP and GLBP is to maintain redundant connections which are reactivated only when topology changes occur. However, they differ in the time it takes them to re-converge after a topology change. The convergence of the RSTP is three consecutive hello messages. The default hello's time is three seconds . In order to achieve the fast re-convergence time, the behavior of the RSTP had to be changed. The HSRP provides the facility to adjust the HSRP hello timers. This timer adjustment tunes the performance of HSRP. HSRP hello and hold timers can be adjusted to millisecond values. With HSRP and GLBP, the hello's value can set from the range of one to 255.

Port State

RSTP provide rapid convergence when a link failure or during reestablishing.

RSTP has three basic operations of a switch port: discarding, learning and forwarding [2]. In all port states, BPDU frames are processed.

The discarding and learning states are seen in both stable active topology and during the synchronization and change stages. The forwarding state is seen in stable active topology only, because the data frames forwarding occurs only after a proposal and agreement of process. Only three states are performed action in RSTP for stable network[2]. The router exists in one of the states for the stable network. All HSRP routers in the group perform transitions through all states. For example, if there are three routers in the group, all routers perform all states and become active and standby router.

The keep alive time is same in RSTP and HSRP but the states are different. HSRP performs well and provides better performance.

Optimization features

HSRP and GLBP offers optimizing options to make it possible to allow the network optimizations. RSTP does not provide these kinds of optimization features and the HSRP and GLBP tracking options. The tracking options monitor interface condition such as line-protocol and IP routing. The other feature is priority value. The priority value in a standby group in HSRP is allowing influencing the active and standby router selection. The Preemption option provides the facility to active router become active after re-establishing the link (if active router fails). The RSTP does not provide optimization features.

Port Role

The Port role is the way to handle the data frames and define the ultimate purpose of a switch port. Port roles are able to transition independently. The additional port allows the RSTP to define a standby switch port before a failure or topology change. The designated port forwards the data frames. If it designated port is failure then alternative port moves to the forwarding state.

Router Roles

HSRP has one active and standby router and more than one router perform as a listen state[4]. However if we compare with GLBP, the protocol has one active virtual gateway (AVG) router with the highest priority among all routers. For the backup or standby, up to four active virtual forwarding (AVG) routers are in GLBP[5]. HSRP and GLBP have major advantages for the optimization of load sharing. If we compare with the port roles in RSTP, the HSRP has active and standby routers. This HSRP features offers sufficient solution to enable redundancy and load balancing.

Load Balancing

In order to share the network traffic, load balancing is required. One of the drawbacks of the RSTP is load balancing; RSTP does not provide the load balancing. In other hand, HSRP facilitates the load balance in order to optimize the network traffic. To facilitate load sharing, a single router may be a member of multiple HSRP groups in the network. Multiple HSRP standby groups can enable load sharing. There can be up to 255 HSRP standby groups on any LAN[7]. The GLBP is a host dependent; each client will always have the same virtual MAC.

CONCLUSION

Although, the comparison shows that the HSRP has efficient features for providing the redundancy and load-balancing. The GLBP is supported only by specific Cisco's devices that are not enough for network solution.

Consequently, the HSRP is the efficient protocol for providing the redundancy and the load balancing as well as for scalable network because HSRP supports the IPv6. The IPv6 provides a more robust router discovery through its neighbor discovery protocol (NDP).

Hot standby router protocol (HSRP) is implemented to provide the reliable network hosts and optimize the network traffic. The network stability and efficiently fault tolerant networking also provide by the HSRP. For the scalability of ISP network, HSRP also support the IPv6 addresses.

REFERENCES

1. Experiencing network problems- Cisco Systems,http://www.cisco.com/en/US/products/ps9967/products_qanda_item09186a0080a 3698f.shtml, last updated: 12th Dec, 2008, last accessed web site 2nd Feb, 2009
2. http://www.cisco.com
3. http://www.apps.ietf.org/rfc/rfc 4318.html
4. RFC 2281, HSRP for optimization, T. Li, B. Cole, P. Morton, D. Li, March, 1998.
5. CCNA study guide, By Richard Deal, 4th edition, page no 983, accessed Date: 05th April, 2009.
6. Cisco network academy, published 1992 – 2008, http://www.cisco.com/en/US/docs/Internetworking/design/guide/nd20e.html, last accessed web site 29th Jan (2011).
7. RFC 2460: S. Deering, Cisco, R. Hinden Nokia, December 1998, last checked website 19th Dec, 2008
8. RFC 4779 IPv6 over DSL Broadband network, Asadullah, January 2007.
9. The essential guide to telecommunications book, by A. Z. Dodd, third edition, last accessed 25th May, 2009.
10. RFC 2460: S. Deering, Cisco, R. Hinden Nokia, December 1998, last checked website 19th Dec, 2008.