Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015

ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-15

First Hop Redundancy Protocols in IPv6 network assessment using Cisco internetworking devices

Maciej ROSTANSKI, Adam RATAJ

***Abstract*—The article presents first hop redundancy concept and the means for its realization in IPv6 network. The research regarding the performance comparison and challenges and issues regarding different solutions is revealed and conclusions are shown. The implementation based on Cisco internetworking devices was chosen, including HSRP and GLBP protocols, as well as built-in IPv6 method for router discovery - NDP protocol.**

***Keywords*—IPv6, Computer Networks, Availability, FHRP, NDP**

I. Introduction

IPv6 is a new version of IP protocol, which was defined in the series of RFC documents at the end of previous century. Although developments and improvements are conducted for many years already, a new standard still did not get such distribution as IPv4.

Migration to IPv6 protocol with its vast address space is a step forward into those and many other possibilities for innovative services. This is a major IPv6 adoption driver for innovative enterprises, and many of small and medium organizations are considering migration. Although the dynamics of IPv6 protocol deployment is not as high as expected, experts assume it is going to grow for a couple of next years [1]. IPv6 protocol, being a successor to the most popular network layer protocol, is already recognised, especially for the addressing space [2] mentioned before, and is thoroughly described in RFCs and in numerous literature, such as [3], [4] or [5].

The addressing space is not the only notable thing - there are many IPv6 advantages over IPv4 protocol, which, among many benefits, include multiaddressing (which basically means, the node may have many IPv6 addresses, related to its function and connectivity), simplified network configuration, directed data flows, utilizing multicast rather than broadcast transmission, simplified packet header, meaning more efficient packet processing, true end-to-end connectivity, restored by eliminating the need for Network Address Translation, and authentication and privacy capabilities, built into protocol itself. [6].

Maciej Rostanski
University of Dabrowa Gornicza
Poland

Adam Rataj
Tieto Chech, s.r.o.
Czech Republic

As the literature often suggests (such as [6] or [7]), the IPv6 solutions, especially for autoconfiguration, is not immune to problems or security issues and concerns. It is the common IT problem - any technique introduced to ease the management, operation or usability, may probably enable some security problems. The risk and security management staff needs to address those problems, harden the configuration, introduce additional procedures, etc. For the operation of IPv6, constant discussion over potential vulnerabilities and configuration difficulties is necessary, since the IPv6 is the basis of the future network. This paper serves such purpose.

A. *Paper aim and scope*

This article is about a number of methods that an end-host can use to determine its first-hop router towards a particular IP destination. These include running (or snooping) a dynamic routing protocol, running an NDP-based (Network Discovery Protocol) router discovery procedure, or using more than one statically configured default routes. However, running a dynamic routing protocol on every end-host may be infeasible for a number of reasons, including administrative overhead, processing overhead, security issues, or lack of a protocol implementation for some platforms. The use of a statically configured default route is quite popular. This however creates a single point of failure. Loss of the default router results in a catastrophic event, isolating all end-hosts that are unable to detect any alternate path that may be available. IPv6 hosts on a LAN will usually learn about one or more default routers by receiving Router Advertisements sent using the IPv6 Neighbor Discovery (ND) protocol [8]. Quoting [9] directly, "Using the default parameters in ND, it will take a host about 38 seconds to learn that a router is unreachable before it will switch to another default router. This delay would be very noticeable to users and cause some transport protocol implementations to time out. While the ND unreachability detection could be made quicker by changing the parameters to be more aggressive (...), this would have the downside of significantly increasing the overhead of ND traffic, especially when there are many hosts all trying to determine the reachability of one of more routers".

The first-hop redundancy protocols are designed to eliminate the single point of failure inherent in the static default-routed environment. They should provide dynamic failover means by deploying many routers in a group (creating single virtual router) so any of such virtual router's IP addresses on a LAN can then be used as the default first hop. The advantage gained from using such protocols is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015

ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-15

The paper is organized as follows - the computer network high availability necessity is explained and investigated, then the first-hop redundancy protocols are selected and characterized. The comparison is presented and the testing results are shown and discussed. The article is then concluded.

II. The computer network resiliency

In computer networks, the most common availability (A) is defined as a percentage of successful operating time in measured time period. Equation (1) shows the formula:

$$A = (\textit{time of operation} / \textit{overall time}) \quad (1)$$

There is a common classification of computer systems availability, based on 'nines' in availability percentage, for example "three nines" mean 99,9 percent availability.

The network availability loss may lead to disastrous consequences and may pose a threat to business continuity of the enterprise. Therefore, the resilience of the enterprise network is one of the most important characteristics. The most common causes of the availability loss are, according to [10]:

- hardware failure (50%)
- software failure (30%)
- Configuration-related errors (11%)
- Hardware-related human errors (9%)

The important conclusion is that the 80% of failures are caused by hardware or software failures, which can be summarized as the equipment failures. But what are the approaches to equipment resiliency improvement?

The proposition given here is, the network equipment is as resilient as it is highly available (failures and downtimes are predicted and processed) and scalable (its performance may be easily improved). Thus, three distinct resiliency components may be defined: scalability, high availability and fault-tolerance.

A. *Scalability*

Scalability is an architectural characteristic, which can be defined as a capability to cope and perform under an increased or expanding workload. A system that scales well will be able to maintain or even increase its level of performance or efficiency when tested by larger operational demands. In terms of networking this would mean the possibility of increasing available bandwidth capacity by adding more first-hop routers, and in effect, paths to the exterior network.

B. *High availability*

In general, the highly available (HA) and fault tolerant (FT) systems are designed with two different design principles in mind. Given the specific availability (A) formula (2), HA aims to minimize downtime and IT service disruption; so the common goal in HA is to increase Mean Time Between Failure (MTBF) and decrease Mean Time to Repair (MTTR).

$$A = MTBF / (MTBF+MTTR) \quad (2)$$

HA applications are designed to have a high level of service uptime. HA solutions may feature many elements, e.g.: system management, live replacement (hot-swap), component redundancy and failover mechanisms. Common strategy is to avoid single points of failure in the system. This can be difficult, because demands on such systems include not only ensuring the availability of important data, but also efficient resource sharing of the relatively expensive components. The typical HA solution would involve active-passive failover in case of router or link failure.

C. *Fault Tolerance*

Contrary to HA, which implies a service level in which both planned and unplanned outages do not exceed a small stated value, fault-tolerant (FT) systems tend to implement as much component redundancy and mirroring techniques as possible, in order to eliminate system failures completely (this is of course from client's perspective, in fact introducing redundant components will make component failures occur faster) [11].

III. First-hop redundancy as a resiliency improvement

The end device utilizes its LAN gateway to communicate with other devices in campus network, in the enterprise network, or even the cloud and the Internet. Therefore, the key device in network services operation is the gateway, which should be as available is possible.

In order to provide the redundancy of the gateway, the most implemented solution is to deploy another gateway, such as in the model of the Distribution Layer in SAFE Architecture by Cisco [12].

The connection to many gateways requires additional mechanisms allowing for correct network operation. This is the purpose of so-called First Hop Redundancy Protocols (FHRP), as explained in the Introduction part. The FHRP for IPv6 network examples could be:

- NDP (Neighbor Discovery Protocol),
- HSRP (Hot Standby Router Protocol),
- VRRP (Virtual Router Redundancy Protocol),
- GLBP (Gateway Load Balancing Protocol)

Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015

ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-15

A. *First-hop redundancy protocols characterization*

NDP is an integral IPv6 part [8]. It allows for router discovery, meaning that through the ICMPv6 operation of Router Solicitation and Router Advertisement messages, IPv6 devices are able to automatically locate gateways on their local link [13]. It can be secured using SeND [14] mechanisms such as Cryptographically Generated Addresses [15].

HSRP [16] was one of the first routing redundancy protocols. It was created by Cisco Systems and is based on sharing a network-layer and link-layer addresses by a group of physical routers. Network nodes use only this virtual address and physically are served by only one router, called active router. There is one standby router, ready to take on the role of an active router in case of failure, other routers in a group are totally passive.

An active HSRP router utilizes NDP - in Router Advertisements there is a virtual HSRP router address. HSRP supports authentication, preemption, interface or object tracking. However, the disadvantage is lack of true load balancing - only one router is active.

GLBP enables load balancing, because more than one router is forwarding packets. GLBP utilizes one virtual address and group, however, there is an Active Virtual Gateway in the group, that serves NS messages and assigns other routers (called Active Virtual Forwarders) to different nodes in the local network. GLBP is capable of using round-robin, weighted or host-dependent load balancing algorithms. Like HSRP, GLBP supports authentication, preemption, interface or object tracking.

B. *Selected first-hop redundancy protocols functionality comparison*

For this paper purposes, the first-hop redundancy protocols compatible with Cisco internetworking devices were chosen because of the implementation, configuration and testing possibilities on the same networking equipment (2801 Cisco router). The comparison is presented in table 1.

TABLE I. SELECTED IPV6 FIRST-HOP REDUNDANCY METHODS CHARACTERISTICS COMPARISON

	Redundancy method		
	NDP	***HSRP***	***GLBP***
Authentication	X	X	X
Preemption		X	X
Interface tracking		X	X
Object tracking		X	X
Load balancing			X
Additional info	Built-in IPv6 algorithm	Very similar to VRRP	Cisco proprietary

Source: Own work

IV. First-hop redundancy methods assessment

The end device utilizes its LAN gateway to communicate with other devices in campus network, in the enterprise network, or even the cloud and the Internet. Therefore, the key device in network services operation is the gateway, which should be as available is possible.

A. *Testing environment and procedures*

Testbed network has been constructed using a typical networking equipment:

- Cisco 2801 router (IOS 15.1(4)M1 software),
- Cisco WS-C3560-24TS switch (IOS 12.2(44)SE2 software),
- Dell Latitude E6430 laptop (Windows 7 Enterprise ServicePack1, 64-bit),
- Fujitsu Siemens V5505 laptop (Xubuntu 13.10),
- Dell OptiPlex 760 desktop (Xubuntu 13.10).

For testing purposes, two applications were used:

- Wireshark sniffing software (v 1.10.2),
- Fping - echo requests (ping) generator (v 3.00).

The topology and testing methodology is presented on fig. 1. During ping process, the switch interface leading to the active router was being shut down (and the next router was supposed to take on active role). The gateway's unavailability time is defined as a time between the first unreplied ICMP packet and the first to be replied again. On fig. 1 there is an example shown (times T5 and T7).

For packet sniffing and monitoring, SPAN port (Switched Port Analyzer) was configured on a switch. In this case, the traffic of router interfaces was monitored on workstations - W1 workstation was monitoring R1 router, and W2 station - R2 router. Tests were carried out for Windows and Linux hosts.

B. *C. Gateway unreachability testing*

The tests were conducted multiple times in order to determine whether unavailability times vary over time or are similar regardless to any other conditions. The tests were conducted:

- Using default parameters (hello times, etc),
- With parameters configured for minimize the unavailability, even if it means frequent RA/Hello messages.

The results are presented on fig. 2 and fig. 3, respectively. For Linux system, it is problematic to use NDP for router failover at default - using Network Manager, the static router entry is created and no failover was possible.

Proc. of the Third Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2015

ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-15

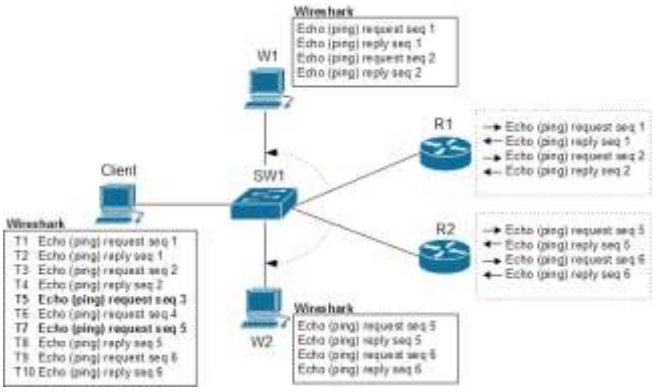

Figure 1. Testing methodology overview. Source: own work

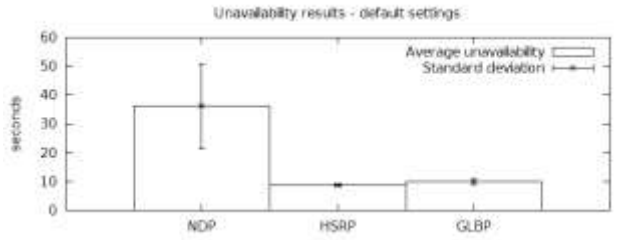

Figure 2. Unavailability testing results for FHRPs - default settings. Source: own work

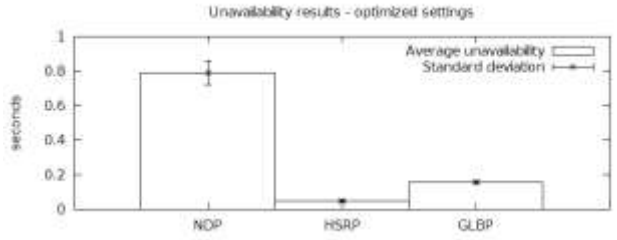

Figure 3. Unavailability testing results for FHRPs - optimized settings. Source: own work

The shortest times of unavailability are of course the result of much greater frequency of Router Advertisement (with NDP) or Hello (for HSRP and GLBP) packets being transferred on link between routers. The traffic increase during optimization process is shown on Table 2.

v. Conclusions

In this article, first hop redundancy concept and the means for its realization in IPv6 network were presented, as well as some thoughts and general classification on availability. This is an interesting topic, because besides the first-hop redundancy methods implementations based on Cisco

TABLE II. ROUTER PROTOCOL-SPECIFIC PACKETS PER SECOND FOR INCREASED AVAILABILITY

	Redundancy method		
	NDP	***HSRP***	***GLBP***
Packets per second	28	134	40

Source: Own work

internetworking devices that were chosen, (including HSRP and GLBP protocols) there is a built-in IPv6 method for router discovery - NDP protocol. The research regarding the performance comparison and challenges and issues regarding different solutions was revealed, showing that:

- It is necessary to optimize certain parameters, affecting the time for failover process, resulting in shorter unavailability times,
- Nearly 100 times faster failover is possible to achieve, but it results in much more congested link.

Unlike 'classical' first-hop routing protocols, NDP relies heavily on client's operating system behavior and its IPv6 implementation. The most important observation at this point was that Linux system autoconfigured first gateway as a static route, which rendered any failover impossible.

Given the fact, that the first-hop redundancy protocols offer additional functionalities, it is clear that while NDP may be applied in smaller environments as a gateway redundancy and availability technique, more demanding networks should employ typical protocols, such as HSRP or GLBP.

References

[1] G Curtis S., Niedzielewski D.: Internet of Things: miliardy urzadzen, czujnikow i licznikow podlaczonych do sieci. Networld (polish ed.) 01/2013, Miller Druk, Warszawa 2013

[2] Domanski A., Wybrane zagadnienia protokolu IPv6, in: Rostanski M. (Ed.) Systemy przetwarzania danych, Academy of Business in Dabrowa Gornicza, Dabrowa Gornicza 2012, ISBN: 978-83-62897-04-9

[3] Van Beijnum I.: Running IPv6, Apress New York, 2006, ISBN: 1-59059-527-0

[4] Odom W.: CCNP Route 642-902 Official Certification Guide 4th ed., Cisco Press, Indianapolis, 2011

[5] Deering S., Hinden R.: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, IETF 1998

[6] Rostanski M., Mushynskyy T.: Security Issues of IPv6 Network Autoconfiguration, in: Saeed K., Chaki R., Cortesi A., Wierzchon S. (Eds.): Computer Information Systems and Industrial Management. 12th IFIP TC8 International Conference, CISIM 2013, Edition: LNCS 8104, DOI:10.1007/978-3-642-40925-7 ISBN: 978-3-642-40924-0, pp.218-228

[7] Nikander P., Kempf J., Nordmark E.: IPv6 Neighbor Discovery (ND) Trust Models and Threats, RFC 3756, IETF, May 2004

[8] Narten T. et al: Neighbor Discovery for IP version 6 (IPv6), RFC 4861. IETF, September 2007

[9] Nadas S. et al: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6, RFC 5798, IETF, March 2010

[10] Badr H., Schrader J.: Secrets to Achieving High Availability, BRKNMS Orlando 2013, p.7, http://d2zmdbbm9feqrf.cloudfront.net/2013/usa/pdf/BRKNMS-2518.pdf

ISBN: 978-1-63248-061-3 doi: 10.15224/ 978-1-63248-061-3-15

[11] Buchwald, P., The Example of IT System with Fault Tolerance in a Small Business Organization, in: Tkacz, E., Kapczynski, A., Rostanski, M.: Internet - Technical Development and Applications 2, Springer 2012, pp. 179-187

[12] Froom R., Sivasubramanian B., Frahim E.: Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide.: Foundation learning for SWITCH 642-813, Cisco Press 2010, Chapter 5

[13] Graziani R.: IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, Cisco Press 2013, Figure 4-16

[14] Arkko J. et al: SEcure Neighbor Discovery (SEND), IETF, March 2005

[15] Aura T.: Cryptographically Generated Addresses (CGA), RFC 3971, IETF, March 2005

[16] Li T., Cole B., Morton P., Li D.: Cisco Hot Standby Router Protocol (HSRP), RFC 2281, IETF, March 1998

[17] Kempf et al.: Securing IPv6 Neighbor Discovery Using Address Based Keys (ABKs), https://tools.ietf.org/html/draft-kempf-secure-nd-01

About Author (s):

Maciej Rostanski

The first-hop redundancy protocols are designed to eliminate the single point of failure. The advantage gained from using such protocols is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.