IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Optimisation of Network Access in Data Center

Dr.M.Suresh Kumar[1], S.Rohini[2]

Associate Professor, Dept. of I.T.,Sri Sairam Engineering College, Chennai, India[1]

PG Student, Dept. of I.T., Sri Sairam Engineering College, Chennai, India[2]

ABSTRACT: Data centres have become an integral part of all business today. Data centers have largely evolved as cloud resource from traditional local network resource, centerally hosted and accessed from different locations. The vital need to access these cloud data center resources is a reliable, robust and high available network connectivity with a fatter bandwidth. The businesses today have become multilocation, therefore the data center has to available to all the locations all the time 24x7x365. The entire data center thus depends on many system parameters, such as uninterruptible power supply, application stability, continuous interconnection of devices that are in the system and so on. This paper is focused on providing high availability network access to the datacentre by implementing device and link redundancy with seamless switching between multiple service providers, providing service provide redundancy as well. It also forms multipath transmission without any downtime of an system. It also describe the use of HSRP, VRRP, GLBP routing protocol feature employed to ensure smooth traffic routing of the critical system to an IP network in case of the main network device failure.

KEYWORDS: data center, hsrp, glbp, vrrp.

I.INTRODUCTION

The data center sometimes reincorporates technology or methodologies that used to work but were phased out in favor of newer options. Then, when higher performing or simplified versions of the old technology are eventually developed, the cycle starts over again. A good example of this is the end user's endpoint device. There was a time where the computing power and logic for end user applications was contained in the data center. A terminal device gave users a display, controls, and a session back to the data center via the network. Somewhere along the way, as the personal computer matured, IT organizations found that employees could be more productive and IT could be more effective by deploying PCs for each user and running client-server applications where the computing happened at the desktop and only accessed resources in the data center when necessary.

It is a facility that centralizes an organization's IT operations and equipment, as well as where it BG are vital to the continuity of daily operations. Consequentially, the security and reliability of data centers and their information is a top priority for organizations.

Although data center designs are unique, they can generally be classified as internet-facing or enterprise (or "internal") data centers. Internet-facing data centers usually support relatively few applications, are typically browser-based, and have many users, typically unknown. In contrast, enterprise data centers service fewer users, but host more applications that vary from off-the-shelf to custom applications.

Facility – the location and "white space," or usable space, that is available for IT equipment. Providing round-the-clock access to information makes data centers some of the most energy-consuming facilities in the world. A high emphasis is placed on design to optimize white space and environmental control to keep equipment within manufacturer-specified temperature/humidity range.

Support infrastructure – equipment contributing to securely sustaining the highest level of availability possible. The Uptime Institute defined four tiers data centers can fall under, with availability ranging from 99.671% to 99.995%. Some components for supporting infrastructure include:

Uninterruptible Power Sources (UPS) – battery banks, generators and redundant power sources.

Environmental Control – computer room air conditioners (CRAC), heating, ventilation, and air conditioning (HVAC) systems, and exhaust systems.

Physical Security Systems – biometrics and video surveillance systems.

IT equipment – actual equipment for IT operations and storage of the organization's data. This includes servers, storage hardware, cables and racks, as well as a variety of information security elements, such as firewalls.

Operations staff – to monitor operations and maintain IT and infrastructural equipment around the clock.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Data centers have evolved significantly in recent years, adopting technologies such as virtualization to optimize resource utilization and increase IT flexibility. As enterprise IT needs continue to evolve toward on-demand services, many organizations are moving toward cloud-based services and infrastructure. A focus has also been placed on initiatives to reduce the enormous energy consumption of data centers by incorporating more efficient technologies and practices in data center management. Data centers built to these standards have been coined "green data centers."

II.RELATED WORK

The data center sometimes reincorporates technology or methodologies that used to work but were phased out in favor of newer options. Then, when higher performing or simplified versions of the old technology are eventually developed, the cycle starts over again. A good example of this is the end user's endpoint device. There was a time where the computing power and logic for end user applications was contained in the data center. A terminal device gave users a display, controls, and a session back to the data center via the network. Somewhere along the way, as the personal computer matured, IT organizations found that employees could be more productive and IT could be more effective by deploying PCs for each user and running client-server applications where the computing happened at the desktop and only accessed resources in the data center when necessary.

It is a facility that centralizes an organization's IT operations and equipment, as well as where it BG are vital to the continuity of daily operations. Consequentially, the security and reliability of data centers and their information is a top priority for organizations.

Although data center designs are unique, they can generally be classified as internet-facing or enterprise (or "internal") data centers. Internet-facing data centers usually support relatively few applications, are typically browser-based, and have many users, typically unknown. In contrast, enterprise data centers service fewer users, but host more applications that vary from off-the-shelf to custom applications.

Facility – the location and "white space," or usable space, that is available for IT equipment. Providing round-the-clock access to information makes data centers some of the most energy-consuming facilities in the world. A high emphasis is placed on design to optimize white space and environmental control to keep equipment within manufacturer-specified temperature/humidity range.

Support infrastructure – equipment contributing to securely sustaining the highest level of availability possible. The Uptime Institute defined four tiers data centers can fall under, with availability ranging from 99.671% to 99.995%. Some components for supporting infrastructure include:

Uninterruptible Power Sources (UPS) – battery banks, generators and redundant power sources.

Environmental Control – computer room air conditioners (CRAC), heating, ventilation, and air conditioning (HVAC) systems, and exhaust systems.

Physical Security Systems – biometrics and video surveillance systems.

IT equipment – actual equipment for IT operations and storage of the organization's data. This includes servers, storage hardware, cables and racks, as well as a variety of information security elements, such as firewalls.

Operations staff – to monitor operations and maintain IT and infrastructural equipment around the clock.

Data centers have evolved significantly in recent years, adopting technologies such as virtualization to optimize resource utilization and increase IT flexibility. As enterprise IT needs continue to evolve toward on-demand services, many organizations are moving toward cloud-based services and infrastructure. A focus has also been placed on initiatives to reduce the enormous energy consumption of data centers by incorporating more efficient technologies and practices in data center management. Data centers built to these standards have been coined "green data centers."

III.EXISTING SYSTEM

Let us consider a business concern which is running business online. To access the internet, they get a leased line from one of the internet service provider and connect their LAN through a router using this link. Whenever there is a failure in the link, they lose their network and it affects their network performance (efficiency). So, they get another link and use it as standby. The following are the limitations of existing system, concern have to manually divert the traffic to the backup whenever the active link fails. It takes a lot of time and within the period they lose the network time and it ultimately reflects negatively in the performance of the network.

Limitation of Existing System:

The concern has to manually divert the traffic to the backup whenever active link fails. It takes a lot of time and within the period they lose the network time and it ultimately reflects negatively in the network.

Does not provide the load balancing facility.

To enable the preemption it is to be configured manually every time.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

IV.PROPOSED WORK

4.2.1 Hot Standby Router Protocol (HSRP)

HSRP protocol has used a priority scheme to decide which configuration of the HSRP protocol router becomes the default active router. If priority setting of a router is higher than other routers, the router becomes the active router and fault priority is 100. If the router with the priority is sameness, higher IP address of the router becomes the active router. HSRP priority has broadcast among its protocol router setting, and its protocol chosen the active router. If the predetermined period time(Hold Time defaults) is 10 seconds ,active router can't send hello message, or information of active router can't be detected by HSRP. It will think that active router has fault, then the HSRP will choose the highest priority standby router change active router, at the same time, HSRP priority in the configuration of the HSRP router chooses a router as a new standby router. HSRP protocol has been configured in a set of routers, and there are a virtual router for the host computer in the LAN, Default gateway of network workstations will point to the virtual address, and active router elected is responsible for transmitting the virtual address in the packet of the workstation. The working principle of HSRP protocol and VRRP protocol are similar, but VRRP includes a protectivemechanism of VRRP packet which is not append by another remote network. Setting TTL = 255 and checking it stops much defect, and the TTL value is 1 by application of HSRP.

4.2.2 Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) is an open standard protocol used to provide redundancy in a network. VRRP is a network layer protocol. It uses the concept of Master and back up router i.e when the master router goes down, one of the backup routers will take up the responsibilities of themaster router, that is the backup router will be responsible for forwarding the traffic until the master router comes again.

VRRP is very useful in a mixed-vendor environment. We can configure VRRP in router to work with routers from other vendor in providing gateway redundancy. When we do, it is important to use the same timer values in all VRRP routers. Otherwise, they will not talk to each other and set themselves as the master, causing conflict in the network.

The timer that we refer here is the advertisement packet interval. By default, VRRP master sends a packet advertisement to its backup, indicating that it is still alive. Default interval on CISCO router is 1 second.

When using Cisco router as the **master**, we can modify the interval by adding command **vrrp <*group_number*> timers advertise <*interval*>** to specify interval in seconds, or use command **vrrp <*group_number*> timers advertise msec <*interval*>** to specify interval in milliseconds.

4.3.3 Gateway Load Balancing Protocol (GLBP)

The Actual Virtual Gateway (AVG) provides virtual Mac addresses to all the other routers operating GLBP of the same group. The remaining routers are Actual Virtual Forwarder (AVF). When an ARP request comes from subnet device to know the Mac address of the virtual IP address, one of the virtual Mac addresses is provided by the AVG. AVG will provide the virtual Mac address by using Round Robin algorithm or other algorithms that have been applied. In this way, all devices running GLBP are used to forward traffic.

GLBP virtual Mac address Assignment : When a subnet device (host) wants to send traffic, it requests a Mac address for the virtual IP (gateway) by sending an ARP request. In response to the ARP request, AVG will provide one of the virtual Mac address (provided to AVF by AVG).

Virtual Gateway Redundancy : To detect a gateway failure, GLBP members communicate with each other through *hello* messages, sent in every 3-seconds to the multicast address 224.0.0.102. If AVG fails, then the AVF having highest priority will become the AVG i.e responsible for providing the Mac address of AVFs.

Virtual forwarder Redundancy : Just like in HSRP, if one of the AVF fails then the other AVF in the same GLBP group will take the responsibility of forwarding the packets. There can be maximum 4 routers in a GLBP group.

Active Virtual Forwarder (AVF)

A router within a GLBP group is elected as Active Virtual Forwarder (AVF) This AVF is responsible for forwarding packets sent to the mac address returned by the AVG router. Multiple active virtual forwarders can exist for each GLBP group.

So, when a client needs to send a packet to the known default gateway (AVG) with a configured IP address, it requests for the MAC address by sending an ARP (address resolution protocol) request on the subnet.

The AVG will respond to these ARP requests with the virtual MAC address of each "active" virtual forwarders, based on a configured load-sharing algorithm.

4.2.4 ARCHITECTURE:

The overall architecture of the entire implementation of process in real time, in this server which is in remote location can be accessed by the centrally hosted data center unit with multiple ISP, connected to form network access without

any down time. The 3 routers which are interconnected with each other acts as a master ip of other two. User can data from multiple domains at a same time ,incase of delay in data transmission of data .The protocols which are been used to configure can backup when the device failure occurs in the system. The entire system thus transmits data and also provides by implementing device and link redundancy with seamless switching between multiple service providers, providing service provide redundancy as well. It also describe the use security and vpn tunnel establishment between the multiple server location.

4.2.5 DEVICE REQUIREMENTS:

Device	Quantity	Model
Pc	1	Generic
Router	3	Cisco1921
Switch	1	Cisco
Server	1	cisco
Cable-Serial DTE	2	Serial DTE
Cable-Straight-through and cross-over CAT 5e	2	Straight through and cross-over CAT 5e
Isp	2	Commercial usage

4.2.6 SECURITY

Security has always been an important issue of any network architecture. The issue is exacerbated in the context of virtualized data centers due to complex interactions between tenants and infrastructure providers, and among tenants themselves. Although the virtualization of both servers and data center networks can address some of the security challenges such as limiting information leakage, the existence of side channels and performance interference attacks, today's virtualization technologies are still far from being mature.

For example, an attack against a VM may lead to an attack against a hypervisor of a physical server hosting the VM, subsequent attacks against other VMs hosted on that server, and eventually, all virtual networks sharing that server . This raises the issue of designing secure virtualization architectures immune to these security vulnerabilities. In addition to mitigating security vulnerabilities.

V.EXPERIMENTAL RESULT

Testing and configuration of routers has been done using and will ping between the devices to ensure the connectivity and performance measures has been calculated by each packet transmission. Thus the end to end device has been connected without any downfall of network transmission. the routers are been configured with inbound and outbound parameters for security purpose.

VI.CONCLUSION AND FUTURE WORK

Data centers have become a more cost-effective infrastructure for data storage and hosting large-scale network applications. However, traditional data center network architectures are ill-suited for future multi-tenant data center environments.

In this paper, when designing these architectures. We also identified some of the key research directions in data center network virtualization and discussed potential approaches for pursuing them Designing smart-edge networks, providing strict performance guarantees, devising effective business and pric-ing models, ensuring security and programmability, supporting multi-tiered and multi-sited data center infrastructures, implementing flexible provisioning and management interfaces between multiple host, and developing efficient tools for managing virtualized data centersare important directions for future research.

REFERENCES

[1]. Cisco System. Hot Standby Router Protocol Features and Functionality [EB//OL] (May 25, 2006),

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

[2]. Chua E. M. et al., 2018, "Comparative Study on Networking Simulation Tools using Correlation Analysis", IEEE, International Symposium on Educational Technology, pp 123127.
[3]. Robbins D. S., 2018, "Using Protocol Redundancy to Enhance OSPF Network System Survivability", IEEE.
[4]. Ayoub O. et al., 2018, "Energy-Efficient Video-on-Demand Content Caching and Distribution in Metro Area Networks", IEEE transactions on Green Communications and Networking.
[5]. Savas S. S. et al., 2018, "RASCAR: Recovery-Aware Switch-Controller Assignment and Routing in SDN", IEEE transactions on Network and Service Management.
[6]. Liu Y. et al., 2018, "Design and Analysis of Probing Route to Defense Sink-hole Attacks for Internet of Things Security", IEEE transactions on Network Science and Engineering.
[7]. Mohamed A. et al., 2018," Joint Energy and SINR Coverage in Spatially Clustered RF-powered IoT Network", IEEE transactions on Green Communications and Networking.
[8]. Rambach et al., 2013, "A Multilayer Cost Model for Metro/Core Networks", J. OPT. COMMUN. NETW./VOL. 5, NO. 3, pp 210-225.
[9]. Murakami M. et al., 2014, "Highly Reliable and LargeCapacityPacketTransportNetworks: Technologies, Perspectives, and Standardization", Journal of Lightwave Technology, VOL. 32
[10] W. Dally and B. Towles, Principles and Practices of Interconnection Networks. Morgan Kaufmann Publishers Inc., 2004.
[11] C. Leiserson, "Fat-Trees: Universal Networks for Hardware-Efficient Supercomputing," IEEE Trans. Comput., vol. 34, no. 10, pp. 892–901, 1985.
[12] M. Al-Fares, A. Loukissas, and A. Vahdat, "A Scalable, Commodity Data Center Network Architecture," in Proc. ACM SIGCOMM, August 2008.
[13] C. Guo, G. Lu, D. Li, H. Wu, X. Zhang, Y. Shi, C. Tian, Y. Zhang, and S. Lu, "BCube: A High Performance, Server-centric Network Architecture for Modular Data Centers," in Proc. ACM SIGCOMM, August 2009. [14] L. Popa, S. Ratnasamy, G. Iannaccone, A. Krishnamurthy, and I. Stoica, "A Cost Comparison of Datacenter Network Architectures," in Proc. ACM CoNext, November 2010.
[15] C. Guo, G. Lu, H. Wang, S. Yang, C. Kong, P. Sun, W. Wu, and Y. Zhang, "SecondNet: A Data Center Network Virtualization Architecture with Bandwidth Guarantees," in Proc. ACM CoNEXT, December 2010.
[16] H. Ballani, P. Costa, T. Karagiannis, and A. Rowstron, "Towards Predictable Datacenter Networks," in Proc. ACM SIGCOMM, August 2011.
[17] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson, "Measuring ISP Topologies with

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details