Research Paper

Volume : 2 | Issue : 6 | June 2013 • ISSN No 2277 - 8179

Benefits of IPV6 in cloud Computing

Computer Science

KEYWORDS : IPv6, IPv4, cloud computing, routing, security, NAT, IPSec etc.

Sridevi Assistant Professor, Dept of Computer Science, Karnatak University, Dharwad-580003

ABSTRACT

This paper gives the IPv6 new features and advantages, which fit into the cloud computing paradigm and provide means to better develop new techniques from which the modern data centers can profit. The development and implementation of IPv6 has been underway for some years and consequently, its improvements over IPv4 are skillfully outlined.

1. Introduction

The Internet is mainly based on one protocol; the Internet Protocol. Version 4 of the Internet Protocol is developed in the 1970's and is the protocol that is common at the moment for Internet traffic. After examining a number of proposals, the IPv6 is settled in January 1995 and since then also known as the "next generation Internet Protocol". Although widespread implementation over the world is necessary within a couple of years mainly because the address space of the IPv4 is almost running out of addresses. "The added value of the IP is the efficient provision of end-to-end connections of arbitrary duration between any points on the globe. Once information is converted into IP packets these can run over any access and link technology connecting the IP routers. This is the definition of a truly open technology." IPv6 (Internet Protocol version 6) is the latest revision of the internet protocol(IP), the primary communications protocol upon which the entire Internet is built. It is intended to replace the older IPv4 which is still employed for the vast majority of Internet traffic as of 2012. IPv6 was developed by the Internet Engineering Task Force(IETF) to deal with the long-anticipated problem of IPv4 running out of addresses.

2. Cloud Computing

Cloud computing is used more and more often in the online environment and it can, at times, be a confusing term. Technically, it involves any kind of resources, software or hardware, which are created and sold as services, by third parties. The term "cloud" comes from the fact that in different diagrams, the internet was always depicted as a cloud, through which all the smaller components, as nodes, hosts, smaller networks, would communicate with each other. That implies that cloud computing always involves the use and the need of an online component. The "computing" part refers to services that are sold over the "cloud". Hardware infrastructure can be sold to customers, who in turn can customize it as they want, without being worried about managing and troubleshooting the data centre itself. Software is also an important part of the cloud computing idea. When talking about software in the cloud, there are two different approaches that imply different levels of interaction with the underlying infrastructure; one with the possibility of creating own applications and the other granting access to the ones that are predefined. Popularity of cloud computing is growing very fast. More and more companies chose to outsource their IT needs to different companies around the world. The consequence is that, in the near future, cloud computing can grow beyond its capabilities and crush under its own success. IPv6 deployment has been slow up until now and may be it will be in the future too, but "The introduction of IPv6 is envisaged as a solution, not only because of its huge address space, but also because it provides a platform for innovation in IP-based services and application.

3. Benefits of IPV6 in Cloud Computing

3.1. Security benefits:

Insecurity is one of the critical issues that generate reluctance to potential customers to make use of cloud computing. The fact that storing the sensitive data into the cloud might create potential losses for business due to low level of security should force cloud computing providers to deploy all the necessary methods to provide high security. Due to the limitation of IPv4, some of the techniques created to prolong the life of IPv4 can prove to be, in some situations, a barrier towards proper safe data transmissions. IPv6 has the potential to create a safer environment in which data can be exchanged easily with no down side for security.

The mechanism developed to slow down the IPv4 address exhaustion, network address translation (NAT), can be considered one of the main obstacles that inhibit proper security in the cloud and stop the deployment of addiction protection measures. The protocols that assures secure IP communication, IPsec, through data authentication and encryption, is the main victim of NAT protocol.

3.1.1. NAT Avoidence

IPv6 came into existence with the idea of bringing new and advanced features that can solve some of the problems that IPv4 is facing with. IPv6 brings to cloud computing from the most basic and obvious change in the protocol: the huge pool of addresses: $2^{128.}$ The sheer number of addresses that are available not only solves the critical problem of running out of addresses but brings a few advantages regarding other aspects of networking, for example, NAT avoidance.

The importance of properly understanding the basic functionality of NAT resides in its effects on the security aspects concerning IPsec. Through address translation, parts of the original packets have to be changed, which in turn makes the use of some features of IPsec impossible. Authentication and encryption are the two building blocks behind IP security.

Authentication provides data integrity and validation of the source, while encryption provides confidentiality and ensures no data manipulation. The authentication process implies creating a unique identification number, commonly a hash, based on some non mutable parameters, one of which is the source address in the IP header preceding the authentication header. The hash is added to the AH header; the receiver of the packet will apply the same algorithms on the same parameters and it will compare the resulted hash with the one received. In the case they do not match, the packet will be discarded.

3.1.2. IPSEC

IPsec is a protocol developed to serve IPv6. But, because of the slow deployment of the next IP, IPsec was adopted for IPv4 as well. As one would expect, IPsec cannot fully work with IPv4 and the existing networks, in which new "patches" were created to slow down the problem of address space. Therefore the issue of the IPv4 cloud-provider customer not having any idea where between the points along their connection proper encryption and authentication is made arises. Pragmatically, they do not even have to know. This is a big problem, because basically a user can access cloud services from anywhere, not only from the protected environment of intra-networks of the companies. It is mandatory, that proper security is offered to the regular user, as transparent as possible and as close as possible to the two end points of the internet connection. It is said that it is easier to hack one computer than one data centre. Proper security has to be offered equally to all entities that are present in the data centre of the cloud provider. It can be accomplished through IPv6

deployment in which support for IPsec is mandatory and can function at its fullest. IPsec a few mandatory concepts have to be noted. IPsec makes use of three important databases on which all the functionality is based: security policy database (SPD), security association database (SAD) and peer authentication database (PAD).

3.2. Network Management benefits
IPv6 provides multiple addresses per interface, link-local, global-unicast and unique local, a different addressing scheme than "on address per interface" that exists in IPv4. This offers different ways of host and network management. The stateless Configuration of IPv6 along with ND provides independent host management from a Centralized point.

3.2.1. IPv6 addressing and interface identifiers
One of the reasons for developing IPv6 was the address exhaustion from IPv4. Hence it was decided that the new IP addresses should be 128 bit long compared to the 32 bit IPv4 addresses. In this way it was assured that the number of possible addresses will be enough to last for the foreseeable future and be used by all the internet capable devices. However, the differences do not reduce only to the high number of available addresses but it extends to the meaning of the address in the context of network and to the way of generating an address. Interface identifiers are used to uniquely define a host and can be generated in many ways, from manual to automatic or stateless configuration. This method will be using the IEEE 802 address, also know was MAC (media access control address) to generate a global unique address.

The new concept of IPv6 is anycast. For better management of data access and communication in IPv4 there were three types of addresses created: unicast (one-to-one communication), broadcast (one-to-all communication) and multicast (one-to-many communication). However, a new addressing technique was introduced: anycast (one-to-one-of-many communication). More to the point, through unicast one host or source can access the data/server/host that is closest to its proximity. Anycast can be used to determine the closest geographical data centre of the cloud computing provider. For example, in case a user travels from a country to another or from a continent to another, through the usage of anycast addressing, the client can access their data from the closed data centre. In conjunction with VM migration or any other type of data distribution techniques, anycast address could provide the easiest and the simplest way for traffic, data access and data withdrawal. Furthermore, anycast addresses seem to be the best way to efficiently use bandwidth and processing power, by using the closest available resources..

3.2.2. Stateless approach
The high number of IPv6 addresses and the incredible elastic nature of a cloud computing data centre create the perfect environment for stateless configuration of host, or in other words for the auto configuration possibilities without any persistent data stored on the network. Data centers that host cloud computing services distinguish themselves through an arbitrary number of servers or VM that run at some point on the network infrastructure. This means that the addressing of such a data centers would take a lot of man power. Even if DHCP is involved, in some cases, the configurations and number of servers needed would increase the complexity even more. The statement: "The stateless approach is used when a site is not particularly concerned with the exact addresses hosts use, so long as they are unique and properly routable."

Data centers and their cloud services should focus on stateless configuration of their machines rather than on a centralized service. Regardless of the truistic nature of the statement "A complex entity will always generate more problems than a simpler one", it is the ground stone for the world of data centers and implicitly cloud computing. Auto configuration reduces the burden of administrator when considering addressing of hosts in a network. Furthermore, in cloud computing environments, this is a benediction, because it fits perfectly on the dynamic nature of the data centres, with hundreds, if not thousands of VMs and server going online and offline at an incredible rate. Compared with IPv4 auto configuration, IPv6 takes it a few steps further. The machine is able to configure on its own, with all the information needed for both link access as well as internet access. Some argue that a DHCP server will still be a good idea, in order to provide the randomness of IPs, thus screening the host for possible attacks.

3.2.3 Address validation
The development of cloud computing with its huge processing power and affordability means that attackers have now more powerful tools than ever to accomplish their goals; hence attacks coming from the cloud computing providers are increasing steadily. Address spoofing has always been one of the means for hackers to hide their traces, high-jack traffic and more. Thus, cloud providers face a great responsibility in trying to stop such users to exploit their infrastructure as a platform for denial of service (DoS) or distributed DoS.

Address spoofing problem has been addressed many times and solutions have been proposed. Although there are methods in use today for filtering incoming packets and checking their source address as a mean of validation, these mainly apply at a macro level, without a method of checking the validity of the packets at a more grained level. Such examples are ingress filtering and unicast reverse path forwarding. Moreover, these do not provide any protection against spoofing attacks from within the network, attacks that are more likely to occur in a cloud data centre. DoS attacks can cause massive drainage of computing power, which, translated in "cloud" terms, might mean a heavy loss in availability and money.

IPv6 and all the protocols behind it that provide extra functionalities bring viable solutions to the problem. By deploying full support for IPv6, cloud providers can easily prevent spoofing attacks.IPv6 implementation can prove to be optimum for verifying the authenticity of a customer/client without deploying any key exchange infrastructure. With IPv4, attackers can use ARP as a way to high jack traffic and redirected to an unwanted host. As with IP addressing spoofing, ARP can be subject to the same kind of attacks. However, IPv6 does not use ARP protocol, but instead the neighbor discovery (ND) protocol takes all its tasks. ND can be as well subject to attacks, but, unlike ARP, ND can be protected and can be used against spoofing attacks. This is a huge benefit compared to what IPv4 has to offer, because this mechanism can be only applied to IPv6 networks and it is furthermore independent from IPsec.

3.3. Performance benefits
Performances along with resource availability are two characteristics that define the quality of one cloud service; they are the corner stone that can destroy or help develop an online service provider. As a consequence, these two features must have priority in their importance. IPv6 can improve both of these, adding value to the service that the provider is offering. Anycast can improve resource availability and latency as well as provide location aware rerouting. Broadcasting, as it will be presented, is of extreme sensitivity when situated in the context of data centres. Fortunately, IPv6 has the means through its design and collateral protocols (ND, ICMPv6) to offer pertinent solutions that do not imply a change in the cloud computing paradigm.

3.3.1. Load balancing
IPv6 Anycast proves to be a feasible solution for improving the load balancing and failover mechanisms. The advantage of anycast scheme is that it offers the possibility of failover mechanisms without the need for any heavy reconfiguration in the eventuality of data centres going offline. With IPv6 anycast, optimum solutions can be more easily achieved in case of decreased complexity and availability in cloud computing data centres. Anycast is a stateless mechanism. As a result, anycast cannot assure that the datagrams of the same data flow will always be delivered to the same location. This means that in some case, TCP session cannot be sustained or kept alive. This means that, by itself, anycast addressing scheme can be used for UDP transmissions. DNS services, as a protocol that uses mainly UDP,

can be created to be aware of anycast addressing. This created a support for geo-aware DNS, which can provide low latency and optimum resource allocation to customers. The modular nature of IPv6 can provide improvements for anycast as well. This signifies that based on certain needs, methods can be created to provide the services required for cloud computing providers. In the article "IPv6 Anycast Routing aware of a Service Flow", a solution is presented based on functionalities of neighbor discovery protocol; the state of a certain traffic flow can be sustained and redirected to the same server, every time an anycast service is used

3.3.2. Broadcast efficiency

Broadcast is a legacy method presented in Ethernet communications which is characterized by the flooding of the network with layer 2 datagrams. A broadcast domain is represented by a LAN segment through which broadcast datagrams can be propagated to all host residing on the particular LAN. ARP and DHCP base their services on this method of host access. In small scale networks in which all broadcast domains have a small or moderate number of hosts, flooding the network with traffic in order to find the needed destination might not be problematic. However, in data centres broadcasting traffic might prove to be wasteful and dynamic enough.

3.4. Mobility benefits

Mobile internet services are becoming very affordable for the common customer. This indicates that cloud computing services will be more and more accessed from mobile devices that roam between different networks. They will present the focal point of the mobile internet: "The killer application for cloud computing is mobile computing: equally, the killer application for mobile computing is the cloud. Without cloud computing services, mobile devices offer limited capabilities." Moreover, as future companies and businesses move to the cloud, the cloud will take the role of "home data centre". As a result, both mobile internet and cloud services providers should be interested in deploying the most efficient solution for providing mobility.

4. Conclusions

As cloud computing is increasing in popularity among common user, businesses and even governmental agencies, the importance of better performance, security and reliability is greater than ever before. Data stored and accessed from the cloud has to be properly secured and available at any time, such that client's confidence in such services could break the insecurities that are nowadays wide spread towards security, bad handling of sensitive data, etc. IPv6 is the next protocol that has some obvious, first hand advantages over its predecessor. It was created from the idea of a new protocol that can handle a huge number of hosts, in complicated network topologies. It was created as being a protocol that is self depended, through auto configuration. All the inefficient mechanisms, such as ARP and broadcast have been removed and replaced with others ones. While the obvious advantages, like the huge address pool, provide improvement and benefits to the data centres, other advantages are a direct consequence of these first hand improvements.

REFERENCE

[1] P.Ganore, Virtualisation- A little history, ESDS, 11 November 2011[Online]. Available: http://www.esds.co.in/blog/ virtualisation-a-little history/ | [2] K.Marko, Server Virtualisation Panacea or Over-hyped Technology?, Tech and Trends, Vol.29,no.6, p.24,9 February 2007. | [3] H.Shah, A.Ghanwani and N.Bitar, ARP Broadcast Reduction for Large Data Centers, Proposed standard Internet Draft, IETF,2011,P.9. | [4] D.Simmons, IPv6 Protocol overhead, Caffeinated Bitstream, Available : http://cafbit.com/entry/ipv6-protocol-overhead. | [5] R.K.Murugesan, S.Ramadas and R.Budiarto, Improving the performance of IPv6 packet Transmission over LAN, IEEE Symposium on Industrial Electronics Applications,vol.1, pp.182-187, October 2009. | [6] G.Groat, M.Dunlop, R.Marchany and J.Tront, IPv6: Nowhere to Run, Nowhere to Hide, International Conference on System Sciences(HICSS),pp.1-10, January 2011. | [7] S.Qader and M.V.Siddiqi, Cryptographically Generated Addresses(CGAs): A survey and analysis of performance for use in mobile environment, IJCSNS, International Journal of Computer Science and Network Security, vol.11,no.2,pp.24-31,2011. | [8] Vodafone, Cloud computing and enterprise mobility, Vodafone, 24 January 2011. [Online]. Available :http://enterprise.vodafone.com/insight-news/2011-01-24-cloudcomputing-and- enterprise-mobility.jsp. | [9] J.Chen and X.Chen, Mobile IPv4/IPv6 virtual machine migration transition framework for cloud computing, Journal of Convergence Information Technology, vol.7,no.3,pp.226-232,2012.