International Journal of Mathematical Archive-3(5), 2012, 2109-2113
Available online through www.ijma.info ISSN 2229 – 5046

NEW LAYERS FUNCTION IN MULTIHOMING ARCHITECTURE

[1]Kewal Krishan Sharma* & [2]Dr. Rakesh Dube

[1]Scholar, Mewar University, Vasundhra, Ghaziabad, UP, India
[2]Department of Mathematics, Faculty of Science, Jazan University, Jazan, KSA

(Received on: 22-04-12; Revised & Accepted on: 14-05-12)

ABSTRACT

Layer of Networking is vital function in establishment of the connections and data communication. Various protocols are used to create Multihoming environment. BGP, SCTP and overlay routing are used in single or mixtures of these to achieving the multihoming. BGP take care only the outside network. While SCTP control the streaming of the network. Multihoming [3] is yet achieved with help of mixtures of various technologies. No pure dedicated protocol has been design yet to keep in mind the requirement of Multihoming and especially with current scenario of a network having packets of heavy loads like IP TV [11], Digital phone calls and remote live operations and normal Internet demand. Some steps to handle such problems should be initiated to create a pathway for future before it gets too late. IPv6 [4] is now ready to take place in real world which is going to revolutionize the world with it great power in mixture of Multihoming.

Keywords: *Multihoming, Bandwidth, Malicious Programs, Dysfunctional Routes, IPTV.*

INTRODUCTION

The Internet expansion has created a world where each computer and computing device is connected to web. It is like a person step out from his home or office or shop he has to step on path, the road, he can go anywhere through the network of roads and highways. The same way each home has connected with internet. We are going to transform our internet network to a NETWORK where every device is connected and to use such services:

- Internet
- TV Broadcasting(IPTV)[11]
- Telephonic Streaming
- Remote Machining operation and Controlling

So Multihoming [5] will be the only way to survive the heavy demand of such services, and future is through only multihoming. The currently used protocols are:

UDP (User Datagram Protocol) is connectionless, which means that it cannot provide error control and flow control. But create vary low overhead to network and essential to start a new connection and to look around in the network when a device start connect in network.

TCP (Transport Control Protocol) is connection oriented protocol, guaranteed correct data delivery. These are vital properties of a transport to support the real-time transfer of signaling information. TCP even thought it is connection oriented, has other drawbacks that decrease its suitability. It is byte stream oriented, always delivers data in strict order, does not allow control of protocol parameters and does not support “multi-homing” at all.

SCTP (Stream Control Transmission Protocol) [12] [13] is important protocol and operates like TCP and UDP. It is flow control and window-based. It provides reliable transmission, detecting when data is discarded, reordered, duplicated or corrupted and retransmitting damaged data as necessary. SCTP is rate adaptive similar to TCP, and will scale back data transfer to the prevailing load conditions in the network. It is designed to behave co-operatively with TCP sessions attempting to use the same bandwidth. The concept of multi-homing is an important feature of SCTP. To provide network layer redundancy, SCTP includes the “multi-homing” capability.

The (**BGP**) Border Gateway Protocol [2] is the protocol backing the core routing decisions on the Internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS) [1]. It is

Corresponding author: *[1]Kewal Krishan Sharma**
[1]Scholar, Mewar University, Vasundhra, Ghaziabad, UP, India

described as a path vector protocol. BGP does not use traditional Interior Gateway Protocol (**IGP**) metrics, but makes routing decisions based on path, network policies and/or rule sets. It is more appropriately termed a reachability protocol rather than routing protocol. BGP was created to replace the Exterior Gateway Protocol (**EGP**) protocol to allow fully decentralized routing in order to transition from the core ARPAnet model to a decentralized system that included the NSFNET backbone and its associated regional networks. This allowed the Internet to become a truly decentralized system.

Clean Network **CN** is network in which only those packets are exist and traveling which are essential and meaningful. Filthy network **FN** is a network in which all packets are exists which are broadcast, malicious activity packets and non essential. Such activity consumes the capacity of network for non productive work.

PROBLEM & DISCUSSION

Since beginning in network development it was prime concern of how to connect independent nodes and create a domain which understands each. Then variation comes across in form of different protocols.

- The stream-oriented nature of TCP is often an inconvenience. Applications must add their own record marking to know messages, and must make explicit use of the push facility to ensure that a complete message is transferred in a reasonable time. The limited scope of TCP sockets complicates the task of providing highly-available data transfer capability using multi-homed hosts. TCP is relatively vulnerable to denial-of-service attacks, such as SYN attacks
- Delivery of packets by independent streams removes unnecessary head-of-line blocking, as we see in the case of TCP delivery.
- In SCTP path selection and monitoring select a primary data transmission path and test the connectivity of the transmission path. Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data packets.

We have seen that all available protocols are having limitation since they are developed with purely mindset of data communication. They rout the packets to achieve performance with less congested world.

The main problem is that all designed protocols are focus on delivery and throughput of the network. None of them concerned about other major issues comes like dysfunctional routs, broadcast attacks, flooding and various attacks. Although this is not the work of network channel to see what is going on. But since day by day often the uncontrolled and unsupervised Internet is facing congestion problem it become very necessary to handle such situation and avoid the situation before this become a nightmare.

During the experiment in lab and data collected from various UTM and Firewall Makers, we found that the % wise application uses the network resources is:

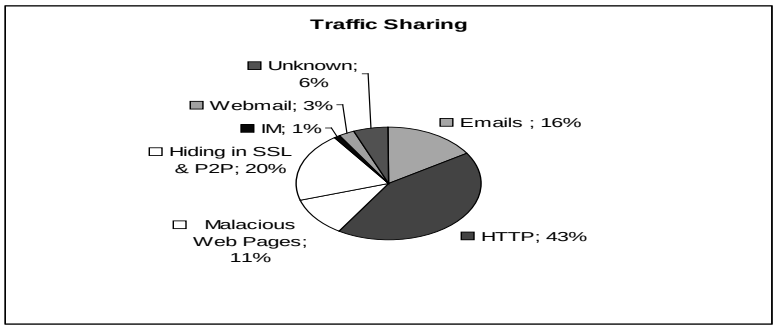

Fig. 1

Here we see "Malicious Web Pages" and "Hiding in SSL and P2P" consist 31% of clear utilization wastage.

PROPOSAL

We propose a model that can cater above discussed issues. The structure diagram follows.

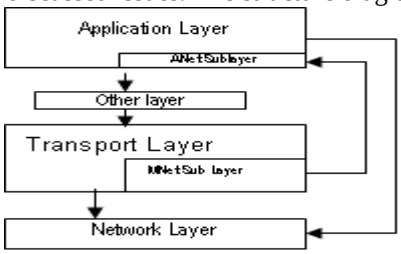

Fig. 2

There should be module in transport layer, we call it MNet sublayer. This sub layer is only design to capture a packet at random interval and forward to application layer for deep inspection. A sub layer at Application layer also needed to handle the captured packet at transport layer, we called it ANet sublayer. The application layer will analyse the packet and take appropriate action. The application layer will parallel study the packet since the performance of the lower layer should not be affected. If upper layer find the abnormally or mysterious activity in the packet it should create action packet for forwarding to source and destination and as well as the intermediate network. The proposed model should be based as on as follows-

- It should use BGP protocol to rout the packet through various routers and will work outside for routing the packet.
- Inside the user premises the SCTP major structure should be adapted with a communication model that can establish communication to BGP.

The ANet sublayer is capable of communicate with ANet sublayer of another node as shown in Fig3.

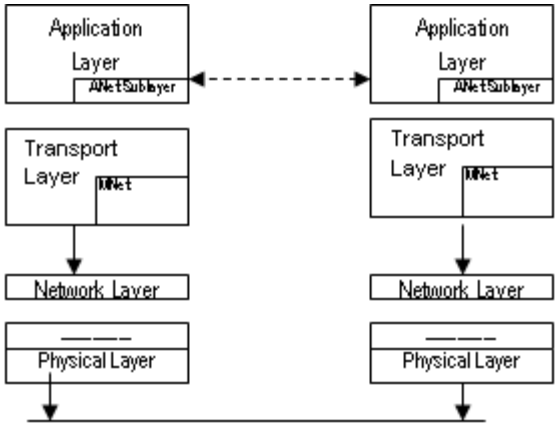

Fig.3

Mnet sublayer in general allows all packets to flow without any check to maintain the speed of packet forwarding. At a given trigger time it get a packet from ongoing traffic and pass to ANet sublayer of application layer. Being application this layer is ample time to analyse the packet and takes a decision what to do according to law define. The small algorithm to handle the packet analysis is below as and can be modified further as required.

Algorithm

If the packet is broadcast packet
Ask ANet for next packet from MNet
Check next for broadcast packet
If found broadcast Packet
Take predefine action P1, P2, P3….Pn
Else if
Check for malicious activity
Take action from M1, M2…..Mn
Else if
If found jumbo packet
Take action from J1, J2…..Jn
Else if
(REM:-This mean good traffic is there)
Increase MNet packet check time at MNet
End if

We see if the on going traffic is good quality than the random check time can be increase with a good delay. This will allow the less overhead on performance of the network. If congestion occurs the more packets can be checked to insure the less malicious activities.

There may be a number of predefine packet actions, which can be selected from the application sub layer. If we create more in-depth algorithm we can control more and produce clean traffic.

The above model will cater seriously following concern:
a. Dysfunctional routs
b. Virus Attack
c. Broadcast Control
d. Monitoring Multi Streams

a. Dysfunctional routes should be detected and dropped from the routing tables of router and gateways. When a packet leaves the source, then in-between routers rout the packets. They use CAM [11] memory with SRAM to keep next hop information and routing information such as MAC or IP address and next hop, in form of routing [8] tables. They rout each packet according to the information. If a rout becomes dysfunctional the information remains in such routers and gateway for some time. Such routs are bottlenecks if they grow in numbers and that rout becomes slow. The speed of a rout (which consist a number of routing point, routing table growth [7], [10]) is effected by the speed of slowest routing point. Clearing such dirty routing table entry is essential.

ANet layer is capable to tell the dysfunctional routs and will pass back information to those routers which are lying in between source and destination by broadcasting special packet which have special meaning to router and gateways. This will happen as follows, when special packet reaches to router or gateway.

1. Take corrective action in its routing table and.
2. Forward a packet to another router for their correction.

b. Virus Attack is creating lot of traffic with the enhanced throughput capacity of network which is working maliciously, can degraded the performance of whole network. The broadcast also create mayhem with multihoming capacity. A controlling mechanism is very important.

c. Generating a good throughput is basically equal to have a good bandwidth, which can be achieved through the proper implementation of Multihoming. But this is not good enough without handling the unnecessary traffic of broadcast.

This should be minimizing in LAN/WAN otherwise the benefits of performance of network become nightmare to network extended from source to destination. The in-between routers become unnecessary flooded and state of congestion occurs. Monitoring multi stream is very much needed to avoid the unnecessary load of streaming. For example a lot of DNS requested send frequently by the system is indication of mysterious activities. Such system can generate unnecessary load to all over the internet for which congestion is felt by the whole network.

d. Let see an example of multi streaming

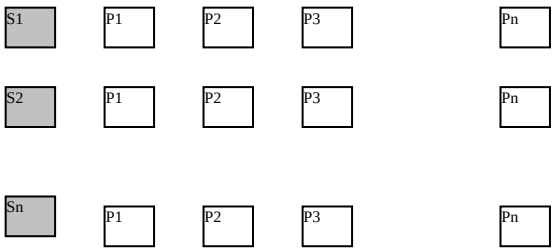

Fig. 4 (**S** are stream, **P** are packets)

Suppose we have n no. stream is running in computer and they are going through multihoming domain. There should be some monitor to keep watch on performance of streams which can not be done at the lower layer level. These should be done on application level as various down loaders software do. They keep watch on various streaming connections. But unfortunately they have no control on lower level of layering systems since there is no mechanism there to communicate with such programs. If some mechanism gets implanted in new design a far better result will be produce.

Suppose a video is transmitted with three streams. Various packets are sent through S1, S2 and S3 stream. Stream S2 is performing slowly in comparison to S1 and S3. At combing the packet received, S1 and S3 packets are used since they are synchronized with the video running and the packet received by S2 is have no use due to out of time. Such packets discarded at application layer. That means the long channel used between two remote machines remain occupied for those packets which finally not be used at receiver. The poorly constructed software wasted the shared channel capacity. This should be not left to merely to end user application software. Some kind mechanism is required at network layers level also to avoid such wastage.

As we all know there are ***pro's and con's***. So the same above proposed protocol has some issues. The vary fist one is the overhead, which will increased. But that is nothing as compare to the congestion and link down problem.

The second one is the compatibility with the existent network infrastructure, which can be minimize with the help of updating firmware with rewritten or upgraded firmware which is a possible in today network equipments easily. Although this is based on BGP and SCTC there may not be much problem.

CONCLUSION

The multihoming has given a new strength to world of web. It has made Internet dependable and fast. In clean network CN this creates the routes less congested and resources used on the web of internet, such as router, gateways and data center, less overburdened [9]. But in filthy network Multihoming creates overburden. In a network this also guarantees that all the time information will be available over the network, except the failure of destination and source itself. **Future scope** of the matter discussed is very wide. There are numerous thing can be done in this field. Even we propose that the layering system should be rewritten completely according to demand of current requirements such as Google has developed the new android OS keeping in mind the internet. While all other OS have written just to manage the computing resource only. The new system should take care of multihoming and multipath requirements and controlling of ill solicited traffic.

The major part is that duplicating information like broadcast and malicious traffic must not travel on network.

REFERENCES

[1] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", IETF RFC 1930, March 1996

[2] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)", IETF RFC 1771, March 1995

[3] J. Abley., "IPv4 Multihoming Practices and Limitations" (work in progress), IETF Internet-Draft, January 2005

[4] G. Huston, "An Update on Multihoming in IPv6 – Report on IETFActivity", Proceedings of RIPE49, September 2004

[5] J. Abley., "IPv4 Multihoming Practices and Limitations" (work in progress), IETF Internet-Draft, January 2005

[6] B. Carpenter, "Internet Transparency", IETF RFC 2775, February 2000

[7] G. Huston, "Analyzing the Internet's BGP Routing Table", The Internet Protocol Journal, vol. 4 no. 1, March 2001

[8] T. Bu, L. Gao and D. Towsley, "On Routing Table Growth", Proceedings of Global Internet Symposium, 2002

[9] G. Huston, "Commentary on Inter-Domain Routing in the Internet", IETF RFC 3221, December 2001

[10] G. Huston, "Analyzing the Internet's BGP Routing Table

[11] Electronics for you, Vol.41 No. 9, Sep 2009

[12] http://www.sctp.org/

[13] Concurrent Multipath Transfer Using SCTP Multihoming, Janardhan R. Iyengar, Keyur C. Shah, Paul D. Amer

Source of support: Nil, Conflict of interest: None Declared

