A COMPREHENSIVE SOLUTION TO CLOUD TRAFFIC TRIBULATIONS

Mathur Mohit
Asst. Professor, Department of IT &CS
Jagan Institute of Management Studies (Affiliated to GGSIP University, New Delhi), Rohini, Delhi, India.
mohitmathur19@yahoo.co.in

ABSTRACT

Cloud computing is generally believed to the most gifted technological revolution in computing and it will soon become an industry standard. It is believed that cloud will replace the traditional office setup. However a big question mark exists over the network performance when the cloud traffic explodes. We call it "explosion" as in future we know that various cloud services replacing desktop computing will be accessed via cloud and the traffic increases exponentially. This journal aims at addressing some of these doubts better called "dangers" about the network performance, when cloud becomes a standard globally and providing a comprehensive solution to those problems. Our study concentrates on, that despite of offering better round-trip times and throughputs, cloud appears to consistently lose large amounts of the data that it is required to send to the clients. In this journal, we give a concise survey on the research efforts in this area. Our survey findings show that the networking research community has converged to the common understanding that a measurement infrastructure is insufficient for the optimal operation and future growth of the cloud. Despite many proposals on building an network measurement infrastructure from the research community, we believe that it will not be in the near future for such an infrastructure to be fully deployed and operational, due to both the scale and the complexity of the network. We also suggest a set of technologies to identify and manage cloud traffic using IP header DS field, QoS protocols, MPLS/IP Header Compression, Use of high speed edge routers and cloud traffic flow measurement. In the solution DS Field of IP header will be used to recognize the cloud traffic separately, QOS protocols provide the cloud traffic, the type of QOS it requires by allocating resources and marking cloud traffic identification. Further the MPLS/IP Header Compression is performed so that the traffic can pass through the existing network efficiently and speedily. The solution also suggests deployment of high speed edge routers to improve network conditions and finally it suggest to measure the traffic flow using meters for better cloud network management. Our solutions assume that cloud is being assessed via basic public network.

KEYWORDS

Cloud computing, traffic, Round trip time, Throughput, IP, DS field, MPLS, RSVP, Sampling, and Compression.

1. INTRODUCTION

Akin to how very few people today prefer to build a house on their own, but rather prefer to rent one, in the next generation of computing, people may prefer to opt for renting a scalable and reliable provider for their computing needs. This will actually minimize risks while induction a new application, rather than build an entire new enterprise for the purpose of launching products. Cloud computing is such one of the hottest topics in information technology today. This is the outsourcing of data center functionality and resources to a third party via a network connection. Companies use IT for highly distributed activities including transaction processing, Web retail and customer support, data analysis and mining and regulatory reporting. If these applications are hosted via cloud computing, it will be necessary

to link cloud resources to a company's own data center resources for data access, and it will also be necessary to provide user access to the applications in the cloud.

Though there is much talk about the rewards of using the cloud, there is no existing measurement study to validate the claims. Also no clear comparisons have been made between the performance of a cloud computing service and that of an established web hosting service. With relation to Cloud Computing, we can classify measurement studies into two broad categories: computation-based measurements and network-based measurements. The computation-based measurements include Storage, Process cycles, and language engine performance. These measurements can only be made at the server level and hence are taken by the service providers themselves or by authorized third parties. The network based measurement is a quantities and qualitative metrics that may include throughput, round trip time, data loss and other QoS (Quality of Service). The main attention of our work is on network-based measurements of the Cloud Computing service.

1.1 The Network Based Measurement

The three important metrics that we shall be analyzing for the cloud network measurement are Network Throughput, Roundtrip time (RTT), and Data Loss, using the measurement tool. A brief description of each of these metrics is provided below:

i) Network Throughput: The average rate of successful data transfer through a network connection is known as network throughput. It is important to differentiate this term from network bandwidth, which is the capacity for a given system to transfer data over a connection. Though providers base their billing on bandwidth and not throughput, throughput is more important from a client's perspective as it decides the data rate they receives for there request.

ii) Round-trip Time (RTT): RTT is defined as the time elapsed from the propagation of a message to a remote place and to its arrival back at the source. The choice of this metric is obvious it provides the exact amount of time that a client accessing a web application would experience as delay in receiving the output of her query from the time of her input.

iii) Packet/Data loss: Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination. This metric is important as it places a quantitative test on the data that a client actually received from the server. Loss can be measured either as loss rate – which detects the amount of data in bytes or as packets lost per unit of time - or simply as loss - the amount of data in bytes that were lost during transfer. It is important to note that none of these metrics can alone provide a general picture of the performance of the cloud computing service.

2 Current State of Cloud Computing Services

The problem Definition: There are a number of cloud computing services in the market today, each offering a variety of services ranging from powerful tools like Google App Engine offers to the complete server solution that Amazon EC2 offers. According to the Network Performance Frustration Research Report by Dimension Data, IT users lose a monthly average of 35 minutes on network log-in delay and 25 minutes on e-mail processing activities such as downloading of mail from a server. File transfers take up an average 23 minutes per month. According to the report, shorter delays were associated with applications such as VoIP (voice over Internet Protocol) and video, but such applications have low tolerance for delays that any time lapse might render them unusable. The survey also found that 30 percent of end users including decision makers--reported frequent computer crashes and slow running applications. On the other hand, about 30 percent of IT departments have well-defined processes for handling

network performance issues. In addition, fewer than 40 percent of IT departments have complete capability to monitor network performance, and even smaller groups have access to a "rough view" of network traffic. Lack of visibility could result in either unnecessary over-investment, or conversely too little investment, and may lead to unnecessary costs and performance implications

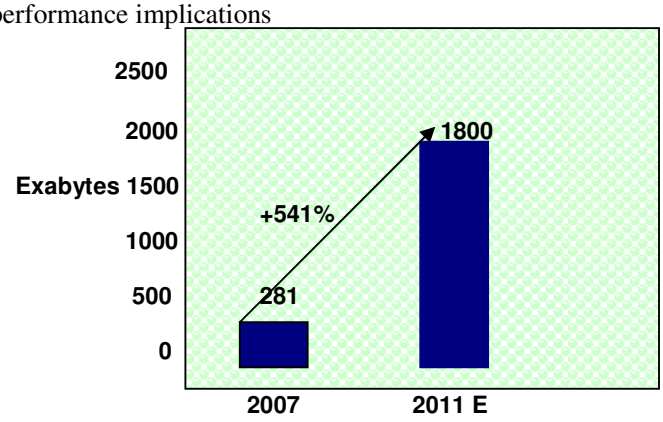

Fig1: Worldwide growth of digital Information

Studies indicate that cloud engines perform exceedingly poorly under heavy loads, opposite to claims made by the cloud companies. What actually is the scenario in most cloud is, at zero load, App Engine will not dedicate much server resource to an application, letting a single server monitor the application. When this server is subjected to an extremely heavy load, the single App Engine server appears to make connection and service every request that arrives to an application at least partially, regardless of the number and size. In the meantime, it appears to be calling for assistance from the other servers in the cluster in order to distribute the load efficiently. This would probably result in a delay in servicing a request for the client. With a more robust client like a browser, a slightly longer delay is permissible. According to a study, The Internet traffic that includes cloud services of 2015 will be at least 50 times larger than it was in 2006.Thus the network growth at these levels will require a dramatic expansion of bandwidth, storage, and traffic management capabilities in core, edge, metro, and access networks.

2.1 Networking Vendors are forced to Change Their Equipments: The Efforts Going On …..

When a company builds a web site in the real world, they assemble servers, routers, switches, load balancers and firewalls, wire them up, configure them and go live. But when that application moves into a cloud environment, things change. In a cloud model, the customer isn't dealing with physical equipment. Many operational clouds still require their customers to accumulate their own machines, however virtual. To build an application, the operator still needs to do what they do in the real world — assemble servers, routers and switches to make a data center — only this time; they're configuring virtual servers instead of real ones. All this means a big transition for the makers of traditional networking equipment. The company's like Cisco, Juniper Networks and many more are adding some new piece of telecommunication equipments. Cisco will give its customers like cable and mobile phone companies and Internet service providers six times the capacity of products from competitors. The change is desperately needed because the rapid explosion of data and movies distributed on the Web will mean a doubling of Internet traffic by 2010 and again by 2012. Edge routers will play a crucial role in determining whether that future consumer experience will be a pleasant one, or simply another excuse to keep your cable company's customer service division on speed-dial. Unlike

core routers, which send data packets within a network, edge routers are the traffic cops for data that travels between local area networks (LANs). They sit on the boundaries, of service areas and are that much closer to the actual users. They are expected to handle a lot of the diverse media now heading to homes and cell phones. In future, routers might function via load balancing over passive optics, with packets distributed randomly across the lines. A passive optical switch, which consumes no power itself, will regulate data flow, eliminating the need for arbiters (directional data packet buffers), and increase performance. Flow by flow load-balancing will enable the building of a mesh network, which will operate over a logical mesh of optical circuits, support all traffic patterns, will be resilient against failure, demonstrate simple routing and cost less to run. Presently, no network provider makes a profit from generating a public internet service, which has to be subsidised by Voice (especially mobile) and VPN activities. Ultimately this lack of profiteering will lead to the consolidation of the number of network providers, which will inevitably converge into one monopoly provider. Potentially optical dynamic circuit switches will be used. These are well suited to optics, are simple, have high capacities to unit volume and wattage, low cost, no queues and no delay variation.

3. Existing solutions and associated problems

3.1 VPN (Virtual Private Network)

The easiest application of cloud computing to support the enterprise network is one where access to the application is via the Internet/VPN, where the cloud computing host can be joined to the VPN, and where little synchronization of data is needed between the cloud host and the enterprise data center. In this case, there will be little traffic impact on the enterprise network, but the support of a cloud resource as a member of the VPN will cause security considerations that will have to be resolved both in a technical sense and through a contract with the cloud computing provider. However the cloud computing providers may incur significant network bandwidth charges as their business grows. These charges can result from traffic to and from customers and traffic between provider's sites. Moreover to implement private tunnels services providers can use there own WAN with multiple peering points with all major ISP's, however small cloud vendors lack the resources to implement it.

3.2 Use of Geographical distribution services:

With the increase of cloud traffic, some cloud support service providers give network and system administrators a DNS based alternative to costly hardware based global server load balancing systems. They direct their client's traffic to the geographically closest available servers. It gives an ability to route, load balance and control cloud traffic to the applications running on the dedicated servers that they provide. This solution may have to deal with all the problems related to geographical distribution like replication of data, fragmentation, updating etc. Moreover it is difficult and inefficient for a cloud vendor to keep servers globally.

4. Differential Services (DS), QoS protocols (MPLS, RSVP), Header Compression, and high speed Edge Routers- A proposed solution to traffic problems

We know that the telecommunication companies are making efforts to develop new high speed telecommunication devices like high speed routers and putting fiber optics path against traffic demands of cloud. But this will not be going to happen globally in near future since replacement of these technologies will cost high and cannot be employed globally in one day. Therefore with a little support of these paths and routers, we propose a solution to traffic problems just described above. The solution involves marking cloud traffic with the use of IP Header DS (Differential Services) to identify cloud vendors traffic and providing QoS protocols (RSVP, MPLS) to satisfy the traffic demands along with high speed Edge routers. Because these high speed routers/ routers identifying QoS protocols will be very few, they use tunneling

approach to forward packets to each other and identify cloud traffic using DS field. In this paper we suggest a solution that involves use of following technologies:

4.1 Use of IP header DS field to identify cloud traffic.
4.2 Use of QoS (Quality of Service) protocols such as RSVP to reserve resources, MPLS to label such packet for forwarding and providing required services
4.3. MPLS/IP Header Compression
4.4 Use of high capacity edge routers.
4.5 Cloud Traffic Flow Measurement to monitor cloud traffic

The overall procedure and use of these techniques to provide QoS and to monitor cloud network are as follows:
In the solution DS Field of IP header will be used to recognize the cloud traffic separately, QOS protocols provide the cloud traffic, the type of QOS it requires by allocating resources and marking cloud traffic identification. . In our paper we are suggesting to use RSVP and MPLS protocols to achieve QoS. RSVP is signalling protocols for setting up paths and reserving resources and MPLS is a forwarding scheme that labels the packet and then forward those packets based on the label .Further the MPLS/IP Header Compression is performed so that the traffic can pass through the existing network efficiently and speedily. The solution also suggests deployment of high speed edge routers to improve network conditions and finally it suggest to measure the traffic flow using meters for better cloud network management. Hence this Cloud system will provide communication capability that is service oriented, configurable, schedulable, predictable, and reliable.

4.1 Use of Differential Services

We suggest Differential service field of IP header to be used to classify and recognize cloud network traffic. Differential services categorize the packets at the edge of the network by setting the DS field of the packets according to their DS value. In the middle of the network packets are buffered and scheduled in accordance to their DS field. MPLS Label Switching Routers (LSR) provides fast packet forwarding compared to routers, with lower price and higher performance. They also offer traffic engineering, which results in better utilization of network resources such as link capacity as well as the ability to become accustomed to node and link failures. According to RFC 2474 six bits of the DS field are used as a code point (DSCP) to select the PHB a packet experiences at each node. A two-bit currently unused(Fig 2).

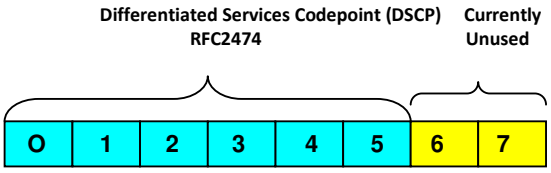

Fig2: Differentiated Services Field

Since we want to differentiate usual internet traffic and cloud traffic we can use one LSB's i.e last bit(8th Bit) which is unused by internet, to identify cloud traffic(Fig. 3). If the 8th bit is set it identifies packet as cloud packet, in this case the 6 MSB's contain 101110 which is suggested for Expedited forwarding in internet and having highest priority over all the traffic. Expedited Forwarding minimizes delay and jitters and provides the highest level of aggregate quality of service. But if 8th bit is not set it will be identified as internet traffic and the router can then check for the 6 MSB's to serve internet traffic as defined in IETF standard.

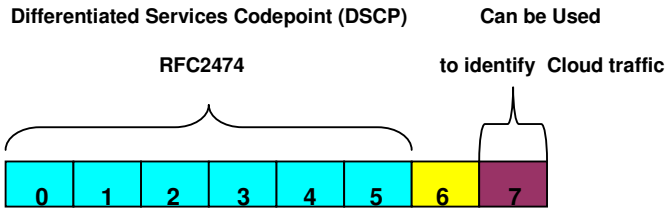

Fig3: Suggested classification for cloud traffic

4.2 Use of Qos Protocols

4.2.1 Use of MPLS

MPLS is an advanced forwarding scheme. It extends routing with respect to packet forwarding and path controlling. Each MPLS packet has a header. MPLS capable routers, termed Label Switching Router (LSR), examine the label and forward the packet. In MPLS domain IP packets are categorize and routed based on information carried in the IP header DS field of the packets. An MPLS header is then inserted for each packet. Within an MPLS proficient domain, an LSR will use the label as the index to look up the forwarding table of the LSR. The packet is processed as specified by the forwarding table entry. The incoming label is replaced by the outgoing label and the packet is switched to the next LSR. Before a packet leaves a MPLS domain, its MPLS header is removed. This whole process is showed in Fig. 4. The paths between the

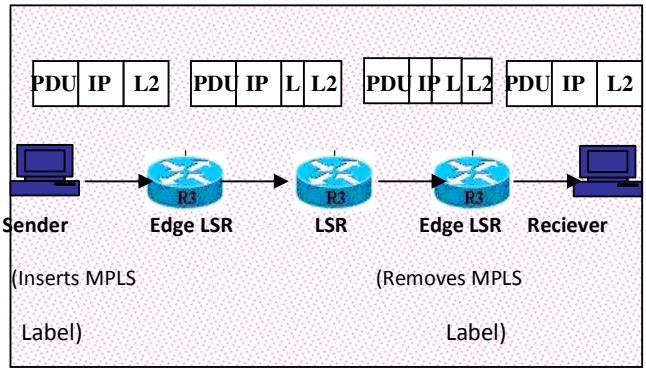

Fig4: MPLS

ingress LSRs and the egress LSRs are called Label Switched Paths (LSPs). MPLS uses some signaling protocol like RSVP to set up LSPs. In order to control the path of LSPs efficiently, each LSP can be assigned one or more attributes. These attributes will be considered in computing the path for the LSP. When we use Differentiated Service filed to identify cloud traffic, packets are classified at the edge of the network. The Differentiated Services-fields (DS-fields) of the packets are set accordingly. In the middle of the network, packets are buffered and scheduled in accordance to their DS-fields. With MPLS, QoS is provided in a slightly different way. Packets still have their DS-fields set at the edge of the network. In addition, the experimental fields in the MPLS headers are set at the ingress LSRs. In the middle of an LSP, packets are buffered and scheduled in accordance to the experimental fields. Whether MPLS is involved or not in providing QoS is transparent to end users. Sometimes it is advantageous to use different LSPs for different classes of traffic. The effect is that the physical network is divided into many virtual networks, one per class. These virtual networks may have different topology and resources. Cloud traffic can use more resources than best effort traffic. Cloud traffic will also have higher priority in getting the backup resources in the case of link or router failure. LSP's will be treated as a link in building the LSPs for VPN. Only the endpoints of

LSPs will be involved in the signaling process of building new LSPs for VPN. LSPs are therefore stacked.

4.2.2 Use of RSVP

RSVP is protocol for resource reservation in network nodes along traffic's path. To achieve it the sender sends a PATH Message to the receiver specifying the characteristics of the traffic. We are assuming that DS field is used to identify cloud traffic. RSVP enables routers to schedule and prioritize cloud packets to fulfill the QoS demands. Every middle router along the path forwards the PATH Message to the next hop determined by the routing protocol. Upon receiving a PATH Message, the receiver responds with a RESV Message to request resources for the flow. Every intermediate router along the path can reject or accept the request of the RESV Message. If the request is rejected, the router will send an error message to the receiver, and the signaling process will terminate. If the request is accepted, link bandwidth and buffer space are allocated for the flow and the related flow state information will be put in the router.

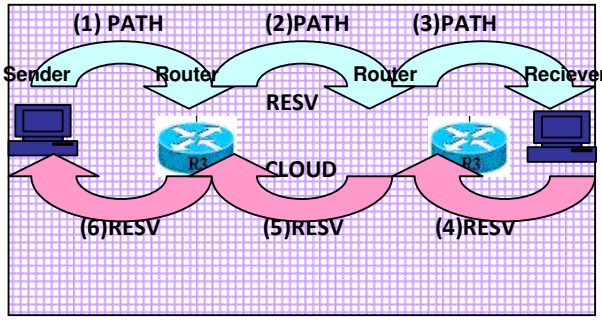

Fig 5: RSVP Signaling

4.3 MPLS/IP Header Compression

The idea of header compression (HC) is to exploit the possibility of considerably reducing the overhead through various compression mechanisms, such as with enhanced compressed RTP or robust header compression [ROHC], and also to increase scalability of HC. We consider using MPLS to route compressed packets over an MPLS Label Switched Path (LSP) without compression/decompression cycles at each router.

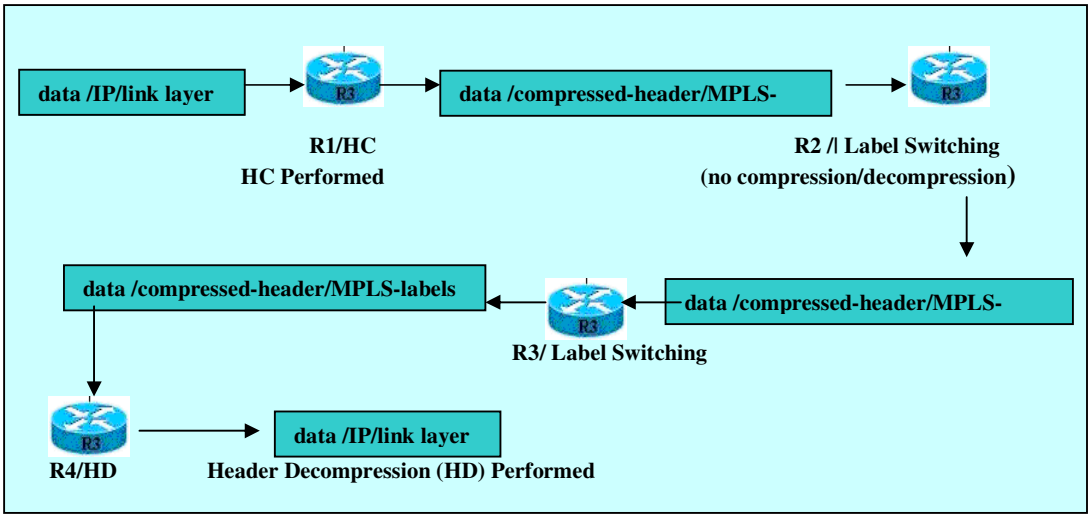

Figure 6: Example of HC over MPLS over Routers R1 → R4

Such an HC over MPLS capability can increase bandwidth efficiency as well as the processing scalability of the maximum number of concurrent flows that use HC at each router.
To implement HC over MPLS, the ingress router/gateway would have to apply the HC algorithm to the IP packet, the compressed packet routed on an MPLS LSP using MPLS labels, and the compressed header would be decompressed at the egress router/gateway where the HC session terminates. The Figure 6 illustrates an HC over MPLS session established on an LSP that crosses several routers, from R1/HC --> R2 --> R3 --> R4/HD, where R1/HC is the ingress router where HC is performed, and R4/HD is the egress router where header decompression (HD) is done. HC of the header is performed at R1/HC, and the compressed packets are routed using MPLS labels from R1/HC to R2, to R3, and finally to R4/HD, without further decompression/recompression cycles. The header is decompressed at R4/HD and can be forwarded to other routers, as needed.

HC over MPLS can significantly reduce the header overhead through HC mechanisms. The need for HC may be important on low-speed links where bandwidth is limited, but it could also be important on backbone facilities, especially where costs are high. The claim is often made that once fiber is in place, increasing the bandwidth capacity is inexpensive, nearly 'free'. This may be true in some cases; however, on some international cross-sections, especially, facility/transport costs are very high and saving bandwidth on such backbone links is valuable. Decreasing the backbone bandwidth is needed in some areas of the world where bandwidth is very expensive. It is also important in almost all locations to decrease the bandwidth consumption on low-speed links

The goals of HC over MPLS are as follows:
i. provide more efficient transport over MPLS networks,
ii. increase the scalability of HC to a large number of flows,
iii. not significantly increase packet delay, delay variation, or loss probability, and
iv. leverage existing work through use of standard protocols as much as possible.

Therefore the requirements for HC over MPLS are as follows:
a. MUST use existing protocols to compress IP headers, in order to provide for efficient transport, tolerance to packet loss, and resistance to loss of session context.
b. MUST allow HC over an MPLS LSP, and thereby avoid hop-by-hop compression/decompression cycles
c. MUST minimize incremental performance degradation due to increased delay, packet loss, and jitter.
d. MUST use standard protocols to signal context identification and control information (e.g., [RSVP], [RSVP-TE], [LDP]).
e. Packet reordering MUST NOT cause incorrectly decompressed packets to be forwarded from the decompressor.
It is necessary that the HC method be able to handle out-of-sequence packets. MPLS enables 4-byte labels to be appended to IP packets to allow switching from the ingress Label Switching Router (LSR) to the egress LSP on an LSP through an MPLS network.

4.4 Use of High Speed Edge Routers

Another requirement for traffic problem elimination is installing high-performance, carrier-class, intelligent routers at the edge of the network, through which operators can efficiently manage bandwidth while delivering cloud services over cable infrastructure. These routers provide reliability, stability, security, and service richness combined with MPLS capabilities. Cloud networks require carrier-class edge routers with high levels of cleverness so that all traffic flows can be efficiently classified and treated according to network policies. The key

feature of this position in the network is that the edge router is the first trusted device in the network and must therefore have the intelligence to implement traffic classification, management and policing. Edge routers focus on processing large numbers of cloud packets with simplified per packet logic. The routers at the edge of the network recognize and classify traffic flows and need to provide per-flow dealing according to network policies. After dealing with the flows, the router must proficiently forward the traffic to the appropriate destination. Traffic treatments include applying the suitable Quality of Service (QoS) controls as well as implementing Admission Control and other traditional router services. To be effective edge routers also need to offer support advanced-load balancing to guarantee the optimization of network infrastructure assets. The packets are processed by Edge routers in the following way: The most basic function of packet processing is the classification function, which performs packet differentiation and understanding based on the packets' header information. To achieve both high-speed packet processing and complex processing with flexibility, the packet engine is constructed from multiple programmable processing units (PU's) arranged in a pipeline-manner as shown in Figure. Each processing unit is specialized for table lookup operation and packet header processing. These processing units are controlled by micro-code processing units are controlled by micro-code which can be programmed to meet the customers requirements. Implementing multiple processing units may increase the circuit-size; but given the recent advances in LSI technology, this will not be a significant issue. The packet access registers in the processing units that the packets go through. These packet access registers form a cascaded packet transmission route. The incoming packets are forwarded in synchronization with clocks with no additional buffering delay time. The processing units can perform operations on the packets only when they are passing through their packet access registers. The processing is distributed among multiple processing units.

It provides 1) high-speed processing, 2) the packet classification function essential for QoS processing, and 3) the ability to flexibly define these functions. QoS performs 1) flow detection, which maps each packet into an associated QoS by classifying them according to the DS field information, and 2) QoS management, which measures and polices the flow quality (bandwidth, delay, jitter, etc.) and manages the packet sending order by scheduling.

After marking the packets according to their QoS requirements, the packet has to be transmitted within the network according to a routing scheme, which searches a table to find a routing. Then, the packet headers must be modified in accordance with the routing.

4.5 Cloud Traffic Flow Measurement

To improve performance, it may be desirable to use traffic information gathered through traffic flow measurement in lieu of network statistics obtained in other ways. Here we are describing some Common metrics for measuring traffic flows. By using the same metrics, traffic flow data can be exchanged and compared across multiple platforms. Such data is useful for:

- Check the behaviour of existing cloud traffic,
- Planning for cloud network development and expansion,
- Quantification of cloud network performance,
- Verifying the quality of cloud network service, and
- Attribution of cloud network usage to users

4.5.1 Meter and Traffic Flows

The basic element of the traffic measurement are network entities called traffic METERS. Meters observe packets as they pass by a single point on their way through the network and categorize them into certain groups. For each such group a meter will accrue certain attributes. We assume that routers or traffic monitors throughout a network have meters to measure traffic.

Traffic flow measurement includes the concept of TRAFFIC FLOW, which is like an artificial logical equivalent to a call or connection. A flow is a portion of traffic, surrounded by a start and stop time, that belongs to one of the metered traffic groups. Attribute values (source/destination addresses, packet counts, byte counts, etc.) associated with a flow are aggregate quantities reflecting events which take place in the DURATION between the start and stop times. The start time of a flow is fixed for a given flow; the stop time may increase with the age of the flow .Each packet is completely independent. A traffic meter has a set of 'rules' which specify the flows of interest as part of its configuration, in terms of the values of their attributes. It derives attribute values from each observed packet, and uses these to decide which flow they belong to. Classifying packets into 'flows' in this way provides an economical and practical way to measure network traffic and subdivide it into well-defined groups.

In practical terms, a flow is a stream of packets observed by the meter as they pass across a network between two end points, which have been summarized by a traffic meter for analysis purposes.

Along with FLOWS and METERS, the traffic flow measurement model includes MANAGERS, METER READERS and ANALYSIS APPLICATIONS. It may well be convenient to combine the functions of meter reader and manager within a single network entity.

MANAGER is an application which configures 'meter' entities and controls 'meter reader' entities. It sends configuration commands to the meters, and supervises the proper operation of each meter and meter reader.

METER is placed at measurement points determined by Network Operations personnel. Each meter selectively records network activity as directed by its configuration settings. It can also aggregate, transform and further process the recorded activity before the data is stored. The processed and stored results are called the 'usage data'. A meter could be implemented in various ways, including:

- A dedicated small host, connected to a broadcast LAN. A multiprocessing system with one or more network interfaces, with drivers enabling a traffic meter program to see packets, A packet-forwarding device such as a router or switch

METER READER transports usage data from meters so that it is available to analysis applications.

ANALYSIS APPLICATION processes the usage data so as to provide information and reports which are useful for network engineering and management purposes. For Example TRAFFIC FLOW MATRICES, showing the total flow rates for many of the possible paths within an internet.

Every traffic meter maintains a table of 'flow records' for flows seen by the meter. A flow record holds the values of the ATTRIBUTES of interest for its flow. These attributes might include:

- ADDRESSES for the flow's source and destination.
- First and last TIMES when packets were seen for this flow, i.e. the 'creation' and 'last activity' times for the flow.
- COUNTS for 'forward' (source to destination) and 'backward' (destination to source) components (e.g. packets and bytes) of the flow's traffic.
- OTHER attributes, e.g. the index of the flow's record in the flow table and the rule set number for the rules which the meter was running while the flow was observed.

A flow's METERED TRAFFIC GROUP is specified by the values of its ADDRESS attributes.

4.5.2 Flow Table

Every traffic meter maintains 'flow table', i.e. a table of TRAFFIC FLOW RECORDS for flows seen by the meter. A flow record contains attribute values for its flow, including:
- Addresses for the flow's source and destination.
- First and last times when packets were seen for this flow.
- Counts for 'forward' (source to destination) and 'backward' (destination to source) components of the flow's traffic.
- Other attributes, e.g. state of the flow record

The state of a flow record may be:
- INACTIVE: The flow record is not being used by the meter.
- CURRENT: The record is in use and describes a flow which belongs to the 'current flow set', i.e. the set of flows recently seen by the meter.
- IDLE: The record is in use and the flow which it describes is part of the current flow set. In addition, no packets belonging to this flow have been seen for a period specified by the meter's InactivityTime variable.

4.5.3 Packet Handling, Packet Matching

Each packet header received by the traffic meter program is processed as follows:
- Extract attribute values from the packet header and use them to create a MATCH KEY for the packet.
- Match the packet's key against the current rule set, as explained in detail below.

The rule set specifies whether the packet is to be counted or ignored. If it is to be counted the matching process produce a FLOW KEY for the flow to which the packet belongs. This flow key is used to find the flow's record in the flow table; if a record does not yet exist for this flow, a new flow record may be created. The data for the matching flow record can then be updated. Each packet's match key is passed to the meter's PATTERN MATCHING ENGINE (PME) for matching. The PME is a Virtual Machine which uses a set of instructions called RULES, i.e. a RULE SET is a program for the PME. A packet's match key contains source and destination interface identities, address values and masks. If measured flows were unidirectional, i.e. only counted packets travelling in one direction, the matching process would be simple. The PME would be called once to match the packet. Any flow key produced by a successful match would be used to find the flow's record in the flow table, and that flow's counters would be updated.

CONCLUSION

Cloud computing is a relatively new concept, and the current services are emerging. As a result, a very limited amount of literature is available in the area. Furthermore, no clear standards exist in this industry, and hence each service provider has its own definitions for resource usage. The upcoming near danger of traffic explosion is really a challenge for the cloud services. Though a lot of telecommunication companies get involved to solve the problem, yet a lot of efforts need to be done. Traffic shaping, load balancing, traffic monitoring, adding new high capacity routers, adding high bandwidth fiber optic networks and many more keywords like these need to be considered for the success of next generation computing- Cloud Computing. That’s a big challenge for the IT service vendors. Nobody should jump into cloud computing on a massive scale; it must be managed as a careful transition. A smart enterprise will trial out applications of cloud computing where network impact is minimal and gradually increase commitments to the cloud as experience develops. That way, network costs and computing savings can both be projected accurately.

ACKNOWLEDGEMENTS

First of all I would like to acknowledge Goddess Saraswati for making me capable of writing this research paper. This work would not be possible without support of my respected parents. Further, I would like to thank everyone at my workplace and anonymous reviewers for their useful comments and suggestions.

REFERENCES:

[1] Beard, H., 2008. Cloud Computing Best Practices for Managing and Measuring Processes for On-Demand Computing, Applications and Data Centers in the Cloud with S LA's. Amazon.com: Emereo.
[2] LaMonica, M., 2008. Amazon storage 'cloud' service goes dark, ruffles Web 2.0 feathers | Webware - CNET.
[3] Weiss, A., 2007. Computing in the clouds, netWorker, 11(4)
[4] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venu- gopal, Market Oriented Cloud Computing: Vision, Hype and Reality for delivering IT Services as Computing Utilities
10 Elucidation of upcoming traffic problems in Cloud Computing

[5] BRODKIN, J. Loss of customer data spurs closure of online storage service 'The Linkup'. Network World (August 2008).
[6] BECHTOLSHEIM, A. Cloud Computing and Cloud Networking talk at UC Berkeley, December 2008.
[7] MCCALPIN, J. Memory bandwidth and machine balance in current high performance computers. IEEE Technical Committee on Computer Architecture Newsletter (1995), 19–25.
[8] RANGAN, K. The Cloud Wars: $100+ billion at stake. Tech. rep., Merrill Lynch, May 2008.
[9] Network-based Measurements on Cloud Computing Services-Vinod Venkataraman Ankit Shah Department of Computer SciencesThe University of Texas at Austin, Austin, TX 78712-0233 Yin Zhang
[10]Davie, B. and Rekhter, Y., "MPLS Technology and Applications," Morgan Kaufmann, 2000
[11]Black, U., "MPLS and Label Switching Networks," Prentice Hall, 2001
[12]Armitage, G., "Quality of Service in IP Networks, Morgan Kaufmann, 2000
[13]E. Rosen, A. Viswanathan, and R. Callon: Multiprotocol Label Switching Architecture. Internet Drafts<draft-ietf-mpls–arch-06.txt>, August 1999.
[14]R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, and S. Jamin: Resource ReSerVation Protocol (RSVP) – Version 1 Functional Spec- ification. RFC2205, September 1997.
[15]T. Li and Y. Rekhter: A Provider Architecture for Differentiated Services and Traffic Engi- neering (PASTE). RFC2430, October 1998.
[16]K. Nichols, S. Blake, F. Baker, and D. Black: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC2474, December 1998. N. McKeown, M. Izzard, A. Mekkittikul, B.
[17] White Paper : Internet QoS: A Big Picture Xipeng Xiao and Lionel M. Ni Department of Computer Science 3115 Engineering Building Michigan State University East Lansing, MI 48824-1226
[18] White Paper : MPLS DiffServ: A Combined Approach by Asha Rahul Sawant, Jihad Qaddour Applied Computer Science,Illinois State University
[19] Uyless Black, MPLS and label Switching Networks, Prentice Hall, Upper Saddle River, 2002
[20] S. Blake, An Architecture for Differentiated Services, RFC 2475, December 1998
[21] Cisco Systems, Diffserv –The Scalable End-to-End QoS Model, http://www.cisco.com/warp/public/cc/pd/iosw/ioft /iofwft/prodlit/difse_wp.htm
[22]White Paper Quality of Service and MPLS Methodologies by ipinfusion Inc.
[23] CESNET technical report number 14/2004 Notes to Flow-Based Traffic Analysis System Design Tom Kosnar7.12. 2004
[24]White paper : Managing Incoming Traffic by Ashok Singh Sairam Supervisor: Prof. Gautam Barua Dept. of CSE, IIT Guwahati,,India.
[25] "Can we Afford a Cloud?" by Mohit Mathur, Nitin Saraswat published in ICACCT'08, APIIT Panipat, India
[26] "Assessment of Strong User Authentication Techniques in cloud based Computing" by Mohit Mathur, Nitin Saraswat published in IACC'09, Thapar University, Patiala,India.
[27] Internet Traffic Explosion by 2015 - Next Phase is Rich Media for Infrastructure 2.0 February 2,

2009 Posted by John Furrier in Technology
[28] Sampled Based Estimation of Network Traffic Flow Characteristics by Lili Yang George Michailidis Department of Statistics Department of Statistics University of Michigan University of Michigan Ann Arbor, MI 48109 Ann Arbor, MI 48109
[29] Yang, L and Michailidis, G. (2006), Estimating Network Traffic Characteristics based on Sampled Data, Technical Report, Department of Statistics, The University of Michigan.
[30] Mori, T., Uchida, M. and Kawahara, R. (2004), Identifying elephant flows through periodically sampled packets, Proceedings ACM SIGCOMM, 115-120.
[31] White Paper : Monitoring network traffic using sflow technology on ex series ethernet switches by Juniper Networks, 2010.
[32] Bandwidth Estimation for Best-Effort Internet Traffic by Jin Cao, William S. Cleveland and Don X. Sun.
[33] Cloud Computing Initiative using Modified Ant Colony Framework by Soumya Banerjee, Indrajit Mukherjee, and P.K. Mahanti., World Academy of Science, Engineering and Technology 56 2009.
[34] Duffield, N. (2004), Sampling for passive Internet measurement: A Review, Statistical Science, 19, 472-498

Authors

Mohit Mathur is Asst. Professor, Dept. of Computer Science at Jagan Institute of Management Studies, Delhi. He has done his Graduation of Delhi University and MCA from Dept. of Electronics, MIT, INDIA. His area of Interest is Network / Network security. He is pursuing his Research work on Cloud Computing. He has already written many research papers in the same area representing different aspects of cloud like security, traffic, scalability etc