International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(4), pp.077-085
DOI: http://dx.doi.org/10.21172/1.84.11
e-ISSN:2278-621X

NETWORK LAYER WORK BASED ON CLOUD

P.Suresh[1]

ABSTRACT: The cloud computing is growing rapidly for it offers on-demand computing power and capacity. The power of cloud enables dynamic scalability of applications facing various business requirements. However, challenges arise when considering the large amount of existing applications. Network architectures define the standards and techniques for designing and building communication systems for computers and other devices. In the past, vendors developed their own architectures and required that other vendors conform to this architecture if they wanted to develop compatible hardware and software. There are proprietary network architectures such as IBM's SNA (Systems Network Architecture) and there are open architectures like the OSI (Open Systems Interconnection) model defined by the International Organization for Standardization. The previous strategy, where the computer network is designed with the hardware as the main concern and software is afterthought, no longer works. Network software is now highly structured To reduce the design complexity, most of the networks are organized as a series of layers or levels, each one build upon one below it. n an n-layer architecture, layer n on one machine carries on conversation with the layer n on other machine. The rules and conventions used in this conversation are collectively known as the layer-n protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed. Violating the protocol will make communication more difficult, if not impossible. THIS PAPER responsible for addressing messages and data so they are sent to the correct destination, and for translating logical addresses and names (like a machine name FLAME) into physical addresses. This layer is also responsible for finding a path through the network to the destination computer.

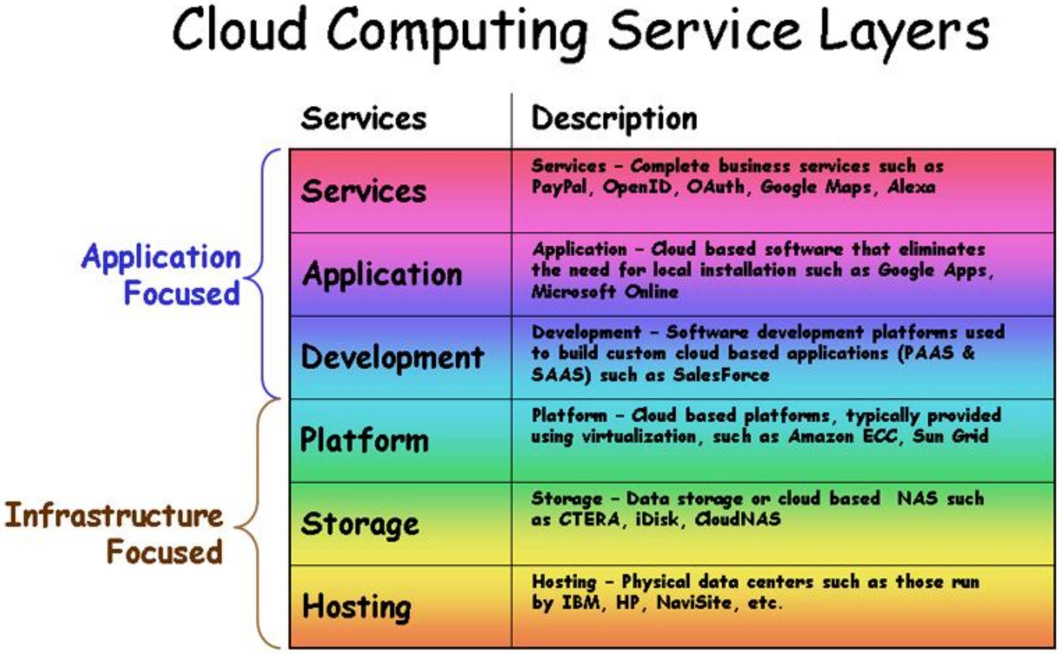
KEYTERMS: cloud, ip address, network, seven layer, protocol.

I. INTRODUCTION

In the cloud storage Environment, users can remotely save their content and used software application alreadyavailable in cloud server when they needed, user also able to shared his her data or information to other user cloud useruse resources of cloud without the burden of local data storage and maintenance. However, the fact that users nolonger have physical possession of the outsourced data makes the data integrity protection in cloud computing aformidable task, especially for users with constrained computing resources. To securely introduce an effective TPA, theauditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional onlineburden to user. This introductory section of cloud is some keyword of cloud computing .Nowadays cloud computingis a hot topic all over the world, through which customers can access information, software, resources without a arranging a basic requirement with the help of web browser or internet . Hence, it eliminates the need for maintainingexpensive computing facilities. On the other hand a brief introduction about the cloud computing .A Cloud computing is an attractive and cost efficient continuation of server based computing [Ref -1] and application service providermodel brief information about the cloud model explainNextParagraph .We see cloud computing as a highly availablecomputing environment where secure services and data are delivered on-demand pattern. There are so manydefinitions of Cloud computing .As per the National Institute of Standards and Technology (N IST) [Ref-2], says acloud computing is “A model for enabling convenient, on-demand network

[1] *Department Of Computer Science H.H The Rajah’s College (Autonomous) India*

access to a shared pool of configurablecomputing resources. In this category we include Resources like Servers, Networks, Storage, and some Services thatcan be rapidly provisioned and released with minimal management effort or service provider interaction”.



Services	Description
Services	Services – Complete business services such as PayPal, OpenID, OAuth, Google Maps, Alexa
Application	Application – Cloud based software that eliminates the need for local installation such as Google Apps, Microsoft Online
Development	Development – Software development platforms used to build custom cloud based applications (PAAS & SAAS) such as SalesForce
Platform	Platform – Cloud based platforms, typically provided using virtualization, such as Amazon ECC, Sun Grid
Storage	Storage – Data storage or cloud based NAS such as CTERA, iDisk, CloudNAS
Hosting	Hosting – Physical data centers such as those run by IBM, HP, NaviSite, etc.

FIG:1

NETWORK LAYER

Network Layer – supervises host-to-host packet delivery – hosts could be separated by several physical networks. data-link layer provides node-to-node delivery, transport layer provides process-to-process delivery.

MAJOR (BASIC) NETWORK LAYER DUTIES

addressing: identify each device uniquely to allow global communication. routing: determine optimal route for sending a packet from one host to another. packetizing: encapsulate packets received from upper-layer protocols. fragmenting: decapsulate packets from one and encapsulate them for another network. The basic purpose of the network layer is to provide an end-to-end communication capability in contrast to machine-to-machine communication provided by the data link layer. This end-to-end is performed using two basic approaches known as connection-oriented or connectionless network-layer services.

FOUR ISSUES:

1. Interface between the host and the network (the network layer is typically the boundary between the host and subnet)
2. Routing
3. Congestion and deadlock
4. Internetworking (A path may traverse different network technologies (e.g., Ethernet, point-to-point links, etc.)

NETWORK LAYER INTERFACE

There are two basic approaches used for sending packets, which is a group of bits that includes data plus source and destination addresses, from node to node called virtual circuit and datagram methods. These are also referred to as connection-oriented and connectionless network-layer services. In virtual circuit approach, a route, which consists of logical connection, is first established between two users. During this establishment phase, the two users not only agree to set up a connection between them but also decide upon the quality of service to be associated with the connection. The well-known virtual-circuit protocol is the ISO and CCITT X.25 specification. The datagram is a self-contained message unit, which contains sufficient information for routing from the source node to the destination node without dependence on previous message interchanges between them. In contrast to the virtual-circuit method, where a fixed path is explicitly set up before message transmission, sequentially transmitted messages can follow completely different paths. The datagram method is analogous to the postal system and the virtual-circuit method is analogous to the telephone system.

OVERVIEW OF OTHER NETWORK LAYER ISSUES:

The network layer is responsible for routing packets from the source to destination. The routing algorithm is the piece of software that decides where a packet goes next (e.g., which output line, or which node on a broadcast channel).For connectionless networks, the routing decision is made for each datagram. For connection-oriented networks, the decision is made once, at circuit setup time. Version 2 CSE IIT, Kharagpur

ROUTING ISSUES:

The routing algorithm must deal with the following issues: Correctness and simplicity: networks are never taken down; individual parts (e.g., links, routers) may fail, but the whole network should not. Stability: if a link or router fails, how much time elapses before the remaining routers recognize the topology change? (Some never do.)Fairness and optimality: an inherently intractable problem. Definition of optimality usually doesn't consider fairness. Do we want to maximize channel usage? Minimize average delay? When we look at routing in detail, we'll consider both adaptive--those that take current traffic and topology into consideration--and non-adaptive algorithms.

CONGESTION

The network layer also must deal with congestion:

When more packets enter an area than can be processed, delays increase and performance decreases. If the situation continues, the subnet may have no alternative but to discard packets.If the delay increases, the sender may (incorrectly) retransmit, making a bad situation even worse. Overall, performance degrades because the network is using (wasting) resources processing packets that eventually get discarded.

INTERNETWORKING

Finally, when we consider internetworking -- connecting different network technologies together -- one finds the same problems, only worse: Packets may travel through many different networks. Each network may have a different frame format. Some networks may be connectionless, other connection oriented.

ROUTING

Routing is concerned with the question: Which line should router J use when forwarding a packet to router K? There are two types of algorithms: Adaptive algorithms use such dynamic information as current topology, load, delay, etc. to select routes. In non-adaptive algorithms, routes never change once initial routes have been selected. Also called static routing. Obviously, adaptive algorithms are more interesting, as non-adaptive algorithms don't even make an attempt to handle failed links. network layer example figure2.**Some protocols are using network layer.**

- DDP, Datagram Delivery Protocol.
- DVMRP, Distance Vector Multicast Routing Protocol.
- ICMP, Internet Control Message Protocol.
- IGMP, Internet Group Management Protocol.
- IPsec, Internet Protocol Security.
- IPv4/IPv6, Internet Protocol.
- IPX, Internetwork Packet Exchange.
- PIM-DM, Protocol Independent Multicast Dense Mode
- .RIP, Routing Information Protocol

- RSMLT Routed-SMLT

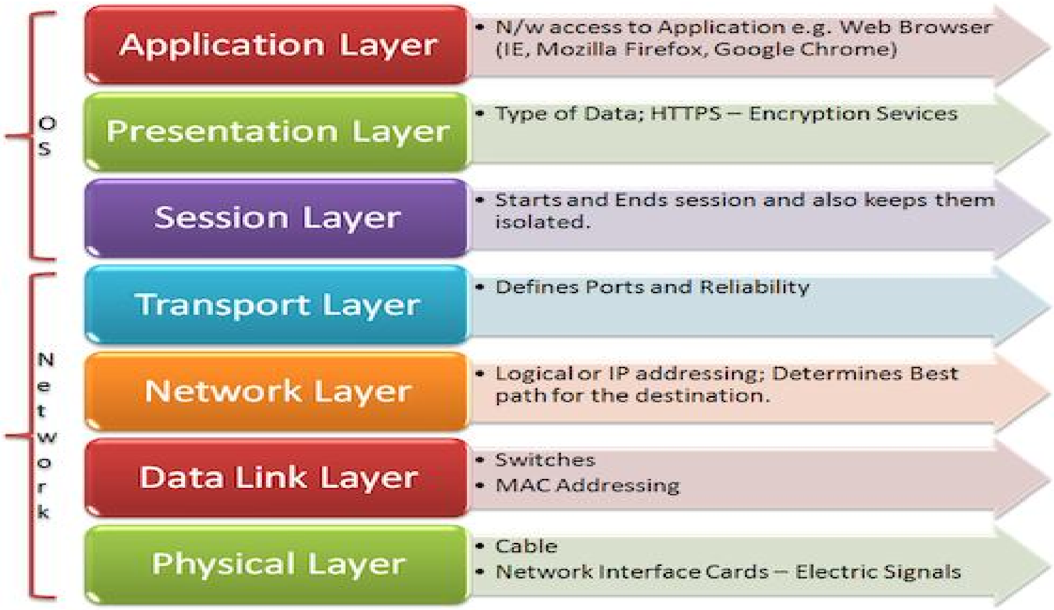
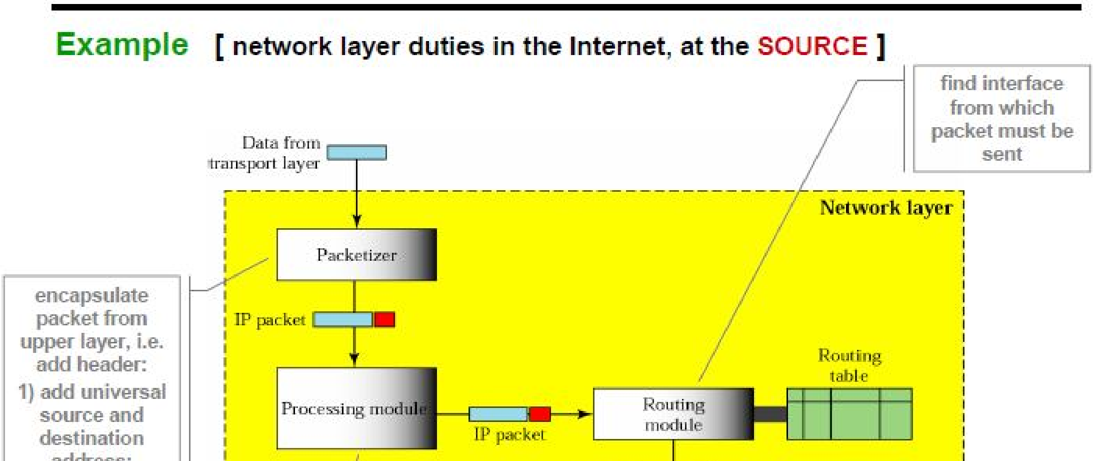

O
S
N
e
t
w
o
r
k
Application Layer
• N/w access to Application e.g. Web Browser (IE, Mozilla Firefox, Google Chrome)
Presentation Layer
• Type of Data; HTTPS – Encryption Sevices
Session Layer
• Starts and Ends session and also keeps them isolated.
Transport Layer
• Defines Ports and Reliability
Network Layer
• Logical or IP addressing; Determines Best path for the destination.
Data Link Layer
• Switches
• MAC Addressing
Physical Layer
• Cable
• Network Interface Cards – Electric Signals

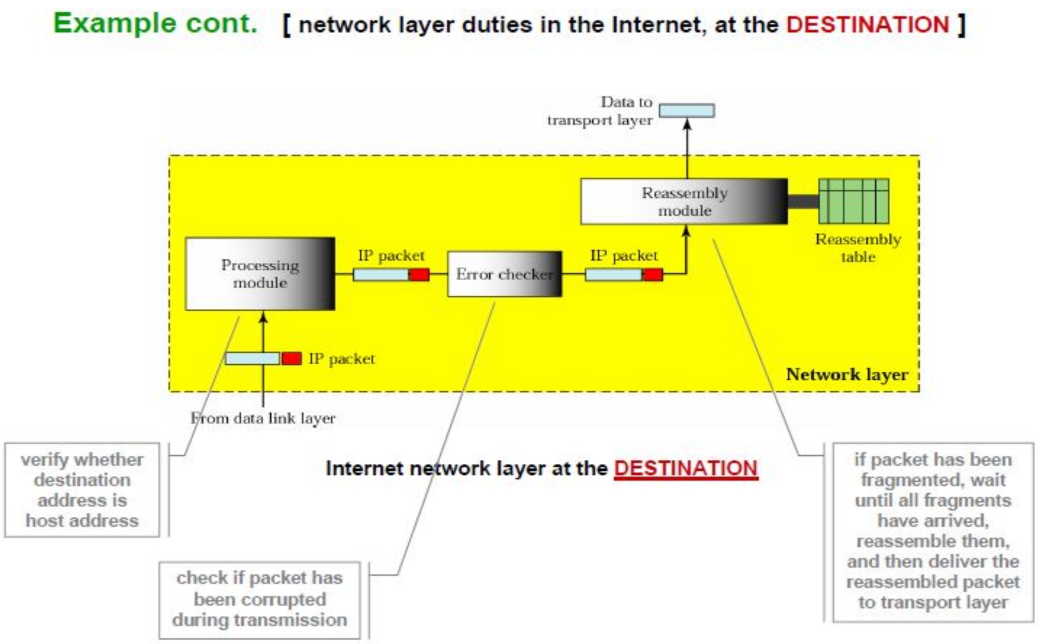
FIG: 2

II. LITRATURE SURVEY

OSI is a standard description or a reference model for defining how messages should be transmitted between any two points in a telecommunication network. Kayri et al., [4] proposed that, possible troubles on the related layer vary and possible troubles on each layer are categorized for functional network administration and they are standardized in an eligible way. Scheidell et al., [5] proposed a theory which seeks to help the reader understand how the traditional OSI model applies to security, realize that three additional layers exert a powerful influence over security programs and decisions, and leverage tips for navigating OSI Layers 8,9 and 10 to become more effective security professionals. The network layer is a medium used by packets to get to their final destination over multiple data. As said earlier in the previous chapter above, virtually all the layers have challenges of security. The lowest third layer of the OSI model is known to face challenges of information privacy problems and Denial of Service attacks. Internet protocol (IP) is the well-known protocol for the network layer. There are many security risks associated with the IP in the network layer. The part of the security risk affecting network layers are network layer packet sniffing, route spoofing, IP Address spoofing. Route policy controls - This mitigation gives a network administrator total control over the routing behavior of particular system. This control also improves network stability. Authentication— Packet sniffing can be mitigated by various methods, and the using of strong one-time passwords is one mitigating method It could also be controlled by deploying switch infrastructure to counter the use of packet sniffers.

PROPOSED WORK


Example [network layer duties in the Internet, at the SOURCE]
find interface from which packet must be sent
Data from transport layer
Network layer
Packetizer
encapsulate packet from upper layer, i.e. add header:
1) add universal source and destination address:
IP packet
Processing module
IP packet
Routing module
Routing table



Example cont. [network layer duties in the Internet, at the DESTINATION]

Internet network layer at the DESTINATION

verify whether destination address is host address

check if packet has been corrupted during transmission

if packet has been fragmented, wait until all fragments have arrived, reassemble them, and then deliver the reassembled packet to transport layer

FIG: 4

The p ost to the destination across intermediate routers. Cloud application all data transport at the network layer is handled by the Internet Protocol (IP). IP receives support from other protocols, such as the Internet Control and Messaging Protocol (ICMP) and the Internet Group Management Protocol 0.10(IGMP) which perform error reporting and other functions. Also, IP relies on routing protocols, such as the Routing Information Protocol (RIP) or Open Shortest Path First (OSFP), or Border Gateway Protocol (BGP), which determine the content of the routing table a IP routers.

EXPERIMENTAL RESULT

In Figure (5) we show the assignment of all protocols discussed in this book to the layers of the TCP/IP protocol suite. Figure (5) is not complete and shows only a subset of the protocol used in the TCP/IP protocol suite. An arrow in the figure indicates how protocols request services from each other. For example, HTTP requests the services of TCP, which, in turn, requests the services of IP, and so on. Figure (5) shows protocols that we have not mentioned so far. SNMP, the Simple Network Management Protocol, is used for remote monitoring and administration of equipment in an IP network. With exception of the ping program, all applications shown in the figure use the services of TCP or UDP, or, as in the case of DNS, both .RIP, OSPF and PIM are routing protocols which determine the content of the routing tables at IP routers. Interestingly, RIP sends routing messages with UDP, a transport layer protocol. CMP is a helper protocol to IP, which performs error reporting and other functions. IGMP is used for group communications. The ARP protocol, which translates IP addresses to MAC addresses, so that IP can send frames over a local area network communicates directly with the data link layer. Figure (5) clearly illustrates the central role of IP in the TCP/IP protocol suite. IP carries all application data, and can neither be bypassed nor replaced.

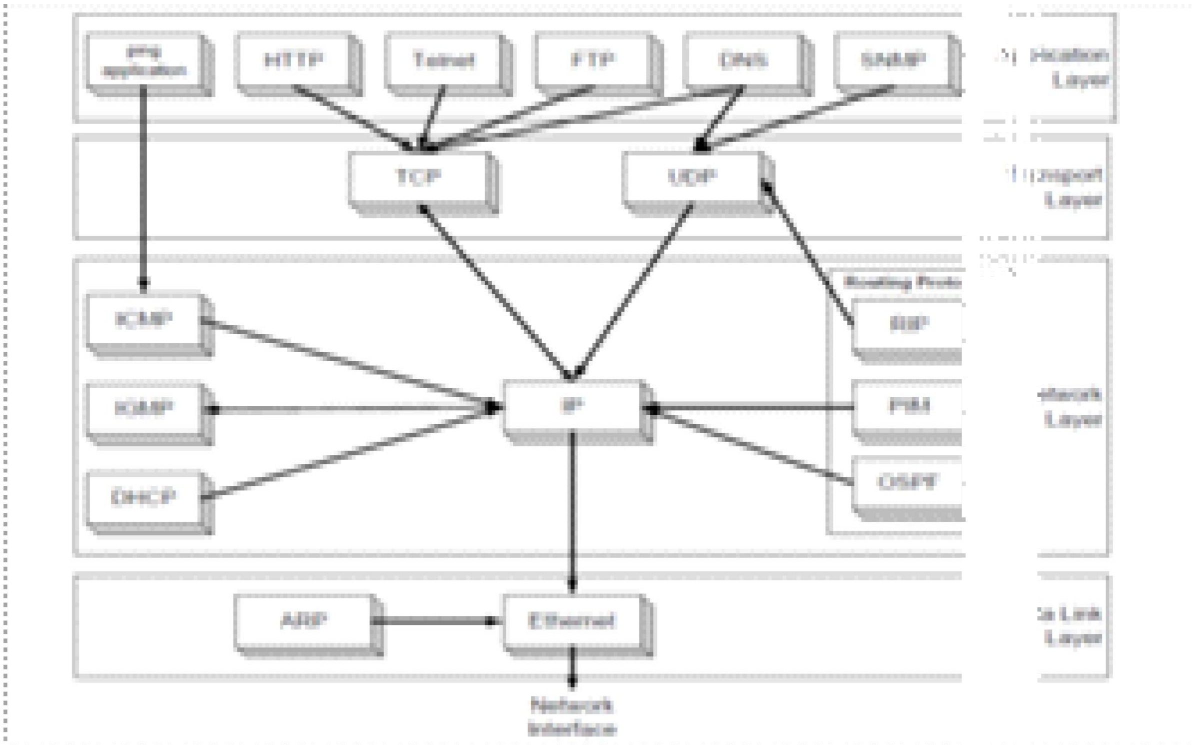


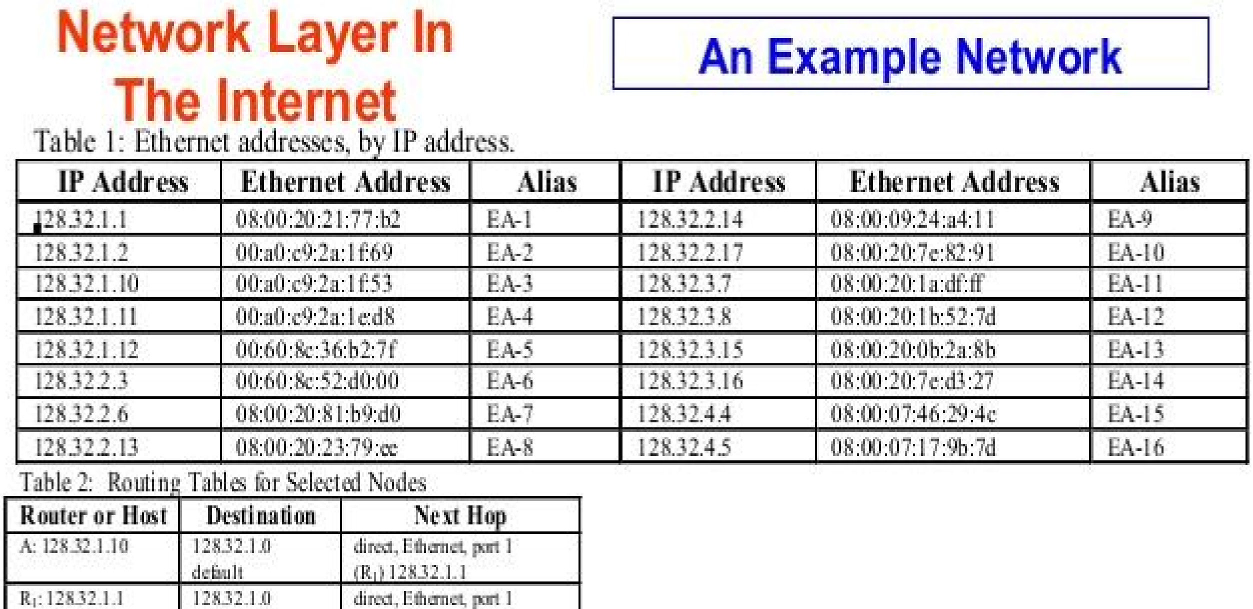
FIG:5

All protocols are using in this layer to convert some values arrange on table. This layer on sending side encapsulates segments into datagrams on receiving side, delivers segments to transport layer network layer protocols in every host, router.in this figure (6).

ANALOGY:

routing: process of planning trip from source to destination .
forwarding: process of correct left turns, right turns, exits, etc.
forwarding: move packets from router’s input to appropriate router output
routing: determine route taken by packets from source to destination.

Interplay between routing and forwarding



Network Layer In The Internet

An Example Network

Table 1: Ethernet addresses, by IP address.

IP Address	Ethernet Address	Alias	IP Address	Ethernet Address	Alias
128.32.1.1	08:00:20:21:77:b2	EA-1	128.32.2.14	08:00:09:24:a4:11	EA-9
128.32.1.2	00:a0:c9:2a:1f:69	EA-2	128.32.2.17	08:00:20:7e:82:91	EA-10
128.32.1.10	00:a0:c9:2a:1f:53	EA-3	128.32.3.7	08:00:20:1a:df:ff	EA-11
128.32.1.11	00:a0:c9:2a:1e:d8	EA-4	128.32.3.8	08:00:20:1b:52:7d	EA-12
128.32.1.12	00:60:8c:36:b2:7f	EA-5	128.32.3.15	08:00:20:0b:2a:8b	EA-13
128.32.2.3	00:60:8c:52:d0:00	EA-6	128.32.3.16	08:00:20:7e:d3:27	EA-14
128.32.2.6	08:00:20:81:b9:d0	EA-7	128.32.4.4	08:00:07:46:29:4c	EA-15
128.32.2.13	08:00:20:23:79:ee	EA-8	128.32.4.5	08:00:07:17:9b:7d	EA-16

Table 2: Routing Tables for Selected Nodes

Router or Host	Destination	Next Hop
A: 128.32.1.10	128.32.1.0 default	direct, Ethernet, port 1 (R_1) 128.32.1.1
R_1: 128.32.1.1	128.32.1.0	direct, Ethernet, port 1

CONCLUSION:

In this figure (7) router to host, to packet information on arrangement tables. One or more then ip address to connected on source and destination.

CONCLUSION AND FUTURE WORK:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In this paper we have tried to explain what exactly an OSI reference model is, why it is used and contribution of various researchers in this reference. Network layer basically an architecture which only gives us an idea how packets transfer over the network during any communication on cloud. Future implementation in network layer multi cloud will be used to enhancement in security and many other areas.

REFERENCES:

[1] 91-us-31- cloud computing white paper thin clients in the cloud(2009).

[2] The NIST definition of cloud computing retrieved march 15, 2012 from http://www.nist.gov/it/cloud/upload/cloud def.v15.pdf

[3] Buecker .A.loadewijkx. k. moss.h.,skapinetz.k & waidner.M(2009).cloud security guidance ,IBM recommendation for the implementation of security; the grad challenge.April 16,2012 from f/s /reap 464.pdf.

[4] Muratkayil and ismail kayri, (IJNGN) journat vol2.no:3, self 2010.

[5] Michal seheideli,"three undocumented layer of the osi model and their impact on security ",secnap network security corporation.

[6] Margaret Rouse, “OSI (Open Systems Interconnection)”,in http://searchnetworking.techtarget.com/definition/OSI.

[7] Hubert Zimmermann, “OSI Reference Model- The ISO Model of Architecture for Open System Interconnection” IEEE transaction on communications, vol.28, issue 4,April 1980.

[8] Web opedia (http://www.webopedia.com/quick_ref/OSI_Layers.asp).

[9] "J. Day, "Terminal protocols," this issue, pp. 585-593.

[10] "J. W. Conard, "Character oriented data link control protocols.