Internet Architecture

Venkata Rama Lakshmi Gundala

CSE, I/II, M.Tech K.L.University

Email: ramalakshmi.gundala1@gmail.com

Abstract: **The classic layered OSI reference model has reached its limits for the Internet of today. The current Internet architecture is facing more serious technical challenges, and many countries around the world have started relevant researches on future Internet. In this paper we first discuss the drawbacks of the current Internet architecture, the design principles underlying the current Internet architecture, and we propose a clean-slate conceptual design of a new architecture as a contribution to the ongoing discussion on the Future Internet. In this paper we discuss Encapsulated Responsibility-Centric Architecture Model (ERiCA) – focuses on determining the responsibilities by using different planes in addition to a partitioning of the network into different decision domains. With this partitioning, we can reduce the complexity of providing a certain service.**

Keywords: **Internet Architecture, ERiCA Model, Design Principles.**

I.INTRODUCTION

A. Origin of Internet Architecture

The Internet is easily the largest computer system ever built, with tens of millions of nodes running hundreds of protocols. The Internet is essentially a network for transporting digital data (i.e., bit streams) between computer processes. In the most abstract form, a network simply consists of nodes connected by links. Consider a typical computer communication scenario where process A running on one computer wants to transmit a file to process B running on another computer. For this transmission to be successful, the following functions are required:

鋍*Data Formatting:* A and B must agree on a common data format so that B can extract and reassemble the content of the file from the bit streams received.

鋍 *Addressing:* Process A must have a means to both uniquely identify B from other Routing. Methods must be in place for determining a feasible path for moving bits from A to B, based on the addresses of A and B.

鋍 Forwarding Methods must be in place for actually moving bits from A to B, through a predetermined sequence of nodes.

鋍*Error recovery:* Since no physical transmission medium is perfect and bits may be inverted or lost in transit, algorithms are required to detect and correct these errors.

B. Introduction

The Internet system consists of a number of interconnected packet networks supporting communication among host computers using the Internet protocols. These protocols include the Internet Protocol (IP), the Internet Control Message Protocol (ICMP), the Internet Group Management Protocol (IGMP), and a variety transport and application protocols that depend upon them. All Internet protocols use IP as the basic data transport mechanism. IP is a datagram or connectionless, internetwork service and includes provision for addressing, type-of-service specification, fragmentation and reassembly, and security. ICMP and IGMP are considered integral parts of IP, although they are architecturally layered upon IP. ICMP provides error reporting, flow control, first-hop router redirection, and other maintenance and control functions. IGMP provides the mechanisms by which hosts and routers can join and leave IP multicast groups. Reliable data delivery is provided in the Internet protocol suite by Transport Layer protocols such as the Transmission Control Protocol (TCP), which provides end-end retransmission, resequencing and connection control. Transport Layer connectionless service is provided by the User Datagram Protocol (UDP).

II. ELEMENTS OF THE ARCHITECTURE

A. Protocol Layering

To communicate using the Internet system, a host must implement the layered set of protocols comprising the Internet protocol suite. A host typically must implement at least one protocol from each layer.

The protocol layers used in the Internet architecture are as follows:

1) Application Layer

The Application Layer is the top layer of the Internet protocol suite. The Internet suite does not further subdivide the Application Layer, although some application layer protocols do contain some internal sub-layering. The application layer of the Internet suite essentially combines the functions of the top two layers - Presentation and Application - of the OSI Reference Model. The Application Layer in the Internet protocol suite also includes some of the function relegated to the Session Layer in the OSI Reference Model.
We distinguish two categories of application layer protocols: user protocols that provide service directly to users, and support protocols that provide common system functions. The most common Internet user protocols are:

• Telnet (remote login)

• FTP (file transfer)

• SMTP (electronic mail delivery)

There are a number of other standardized user protocols and many private user protocols. Support protocols, used for host name mapping, booting, and management include SNMP, BOOTP, TFTP, the Domain Name System (DNS) protocol, and a variety of routing protocols.

2) Transport Layer

The Transport Layer provides end-to-end communication services. This layer is roughly equivalent to the Transport Layer in the OSI Reference Model, except that it also incorporates some of OSI's Session Layer establishment and destruction functions. There are two primary Transport Layer protocols at present:

• Transmission Control Protocol (TCP)

• User Datagram Protocol (UDP)

TCP is a reliable connection-oriented transport service that provides end-to-end reliability, resequencing, and flow control. UDP is a connectionless (datagram) transport service.

3) Internet Layer:

All Internet transport protocols use the Internet Protocol (IP) to carry data from source host to destination host. IP is a connectionless or datagram internetwork service, providing no end-to end delivery guarantees. IP datagram may arrive at the destination host damaged, duplicated, out of order, or not at all. The layers above IP are responsible for reliable delivery service when it is required. The IP protocol includes provision for addressing, type-of-service specification, fragmentation and reassembly, and security. The datagram or connectionless nature of IP is a fundamental and characteristic feature of the Internet architecture. The Internet Control Message Protocol (ICMP) is a control protocol that is considered to be an integral part of IP, although it is architecturally layered upon IP - it uses IP to carry its data end-to-end. ICMP provides error reporting, congestion reporting, and first-hop router redirection. The Internet Group Management Protocol (IGMP) is an Internet layer protocol used for establishing dynamic host groups for IP multicasting.

4) Link Layer

To communicate on a directly connected network, a host must implement the communication protocol used to interface to that network. We call this a Link Layer protocol. Some older Internet documents refer to this layer as the Network Layer, but it is not the same as the Network Layer in the OSI Reference Model. This layer contains everything below the Internet Layer and above the Physical Layer (which is the media connectivity, normally electrical or optical, which encodes and transports messages).

B. Networks

According to the IP service specification, datagrams can be delivered out of order, be lost or duplicated, and/or contain errors. Constituent networks may generally be divided into two classes:

• Local-Area Networks (LANs) LANs may have a variety of designs. LANs normally cover a small geographical area (e.g., a single building or plant site) and provide high bandwidth with low delays. LANs may be passive (similar to Ethernet) or they may be active (such as ATM).

• Wide-Area Networks (WANs) geographically dispersed hosts and LANs are interconnected by wide-area networks, also called long-haul networks. These networks may have a complex internal structure of lines and packet-switches, or they may be as simple as point-to-point lines.

C. Routers

In the Internet model, constituent networks are connected together by IP datagram forwarders which are called routers or IP routers. In this document, every use of the term router is equivalent to IP router. Many older Internet documents refer to routers as gateways. Historically, routers have been realized with packet-switching software executing on a general-purpose CPU. However, as custom hardware required, special purpose hardware is becoming increasingly common. A router connects to two or more logical interfaces, represented by IP subnets or unnumbered point to point lines. The term "router" derives from the process of building this route database; routing protocols and configuration interact in a process called routing. The routing database should be maintained dynamically to reflect the current topology of the Internet system.

D.Addressing Architecture

An IP datagram carries 32-bit source and destination addresses, each of which is partitioned into two parts - a constituent network prefix and a host number on that network. Symbolically:

IP-address::={<Network-prefix>, <Host-number>}

To finally deliver the datagram, the last router in its path must map the Host-number (or rest) part of an IP address to the host's Link Layer address.

E. IP Multicasting

IP multicasting is an extension of Link Layer multicast to IP internets. Using IP multicasts, a single datagram can be addressed to multiple hosts without sending it to all. In the extended case, these hosts may reside in different address domains. This collection of hosts is called a multicast group. Each multicast group is represented as a Class D IP address. An IP datagram sent to the group is to be delivered to each group member with the same best- effort delivery as that provided for unicast IP traffic. The sender of the datagram does not itself need to be a member of the destination group. That document describes how hosts and routers join and leave multicast groups. It also defines a protocol, the Internet Group Management Protocol (IGMP), that monitors IP multicast group membership. Forwarding of IP multicast datagrams is accomplished either through static routing information or via a multicast routing protocol. Devices that forward IP multicast datagram are called multicast routers. They may or may not also forward IP unicasts. Multicast datagram are forwarded on the basis of both their source and destination addresses.

III. DESIGN PRINCIPLES

To meet the overriding requirements of robustness and link heterogeneity, the original architects of the Internet made two important design decisions regarding how to organize

the core computer networking functionalities. First they recognized that a monolithic network architecture where each switching node can cope with all link technologies will not scale. The concept of adding specialized packet switching nodes, called Internet Message Processors (IMPs), to the network architecture was developed to address that problem and to take advantage of the then new store-and-forward communication paradigm. Each IMP, which we call a gateway or router today, would be an intermediary linking two or more different packet networks. A three-part address format was defined: one for identifying a communicating process, another for identifying the process's host computer, and the last one for identifying the host network. A packet would carry both source and destination addresses in its header. A gateway would only need to inspect the network portion of the destination address when making packet forwarding decisions. Once a packet arrived at the destination network, that network would use the other parts of the destination address to deliver the packet to the receiving process.

IV. CURRENT INTERNET ARCHITECTURE

Today, the Internet has evolved from a U.S. military system prototype into an open, world-wide infrastructure over which a rich set of applications, including Web, Ebusiness, voice over IP (VoIP), video broadcast, and on-line gaming, is deployed. These applications have imposed additional performance and security challenges on the network. The current Internet architecture can be decomposed into three planes:

1) Data plane: The data plane is local to an individual router, or even a single interface card on the router, and operates at the speed of packet arrivals, down to nanoseconds per packet. For example, the data plane performs packet forwarding, including the longest-prefix match that identifies the outgoing link for each packet, as well as the access control lists (ACLs) that filter packets based on their header fields. The data plane also implements functions such as tunneling, queue management, and packet scheduling.

2) Control plane: The control plane consists of the network-wide distributed algorithms that compute parts of the state in the data plane. The convergence times of these algorithms vary from seconds to minutes. For example, the control plane includes BGP update messages and the BGP decision process, as well as the Interior Gateway Protocol (such as OSPF), its link-state advertisements (LSAs), and the Dijkstra's shortest-path algorithm. A primary job of the control plane is to compute routes between IP subnets, including combining information from each routing protocol's Routing Information Base (RIB) to construct a single Forwarding Information Base (FIB) that drives packet forwarding decisions.

3) Management plane: The management plane stores and analyzes measurement data from the network and generates the configuration state on the individual routers. For example, the management plane collects and combines Simple Network Management Protocol (SNMP) statistics, traffic flow records, OSPF LSAs, and information extracted from BGP update message streams.

V. FUTURE OF INTERNET ARCHITECTURE

Current Internet's traditional approach to communications is based on a client-server model of interaction; communicating parties establish a relationship and then proceed to transfer information where data contained within IP packets are transported along a single path. Today, however, the most predominant use of the Internet is centered on content creation, dissemination and delivery, and this trend will continue into the foreseeable future. While the basic client-server model has enabled a wide range of services and applications, it does not incorporate adequate mechanisms to support secure content-oriented functionality, regardless of the specific physical location where the content resides. In this paper, we present a novel clean-slate for the Internet of tomorrow. In this paper, we considered the Future Internet challenges presented (i.e., mobility, scalability, security, etc.) and demonstrated that our architecture fulfills these criteria. Our goal is to extend the input to the process and to demonstrate an alternative concept. This concept describes an Encapsulated Responsibility-Centric Architecture Model (ERiCA-Model), which is based on the idea of recognizing the different actors in the network, their influence as well as their responsibilities. Our approach focuses neither on an application, service nor event driven architecture. Instead, its duty is to determine the responsibilities for the services concerned by establishing a complete transport chain.

ERICA-MODEL:

Basics and Terminology: A Network Segment is a network subset that builds a logical or physical connection between two communication partners during a data transmission. For example, network topology connecting Communication Partner1 (CP1) and Communication Partner 2 (CP2); each hexagon represents a network segment. A Network Cluster is the set of network segments that could be utilized to build a combination that allows a data communication between two communication partners. The network cluster consists of all network segments which could be utilized for connecting the two endpoints; they are represented by hexagons with plain structure. The hexagons with the streaked structure cannot be included in any segment chain

between CP1 and CP2 and therefore do not belong to this cluster. A possible combination of network segments which can be used for the data transfer is denoted as Path. The data packets which are sent via one path are denoted as Sub-Flow. The combination of all available subflows (in other terms: data which is transferred between CP1 and CP2) is denoted as Flow. We consider a communication partner representing a service-requesting instance. Within a flow, the logical entity of the data transferred is called Stream. Here two streams: here, packets belonging to different streams (Stream 1: plain; Stream 2: streaked) are sent via different path.

A. New Architecture Requirements:

Some important new requirements that may influence the new architecture are as follows:

1) Mobility: The Internet architecture should support flexible, efficient, and highly-dynamic Mobility.

*2) Policy-driven Auto-Configuration***:** The Internet architecture should provide auto-configuration of end systems and routers, subject to policy and administrative constraints.

3) Highly time-variable resources: The Internet architecture should support resources that are highly variable over short time-scales. This may for example be due to switched backbone links, or due to mobile devices that can switch physical transmission medium as the node moves.

4) Allocation of Capacity: In today's Internet, allocation occurs implicitly as a result of congestion control. The goal has generally been some approximation of "fairness"; all slow down together, but this is not always the right model. For commercial activities, there is a desire to allocate capacity based on willingness to pay. These will need to be provided in an intelligent manner, personalised to the needs and context of the user, and at the desired quality level and support the "vertical services":

• Information & knowledge services

• Business and applications services

• Sense and action on the real world

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we make several structural observations about Current Internet Architecture. First we have discussed about protocol layers used in the Internet architecture all these protocols works with OSI reference model. We have discussed Design principles. After that we have discussed a new, clean-slate approach for the Internet of tomorrow, which we denote as Encapsulated Responsibility-Centric Architecture Model (ERiCA). In this concept makes it possible to recognize the different actors in the network and their influence as well as to manage the different responsibilities by establishing a complete transport chain. We have also reasoned that the proposed architecture fulfills the challenges required by the Future Internet (i.e. security, mobility, scalability, etc.)

It is here to be noticed that we are in the early stage of this work. As ongoing and future work, we are going to realize a proof-of-concept implementation, in order to demonstrate the advantages of our concept and also to find out possible shortcomings. In addition to it, multiple points have to be analyzed and optimized, such as the clustering and aggregating steps in the NCA process or the efficiency of the decision making process. In addition to it, important milestones of our future work are the analysis of the scalability of the approach as well as the examination of our concept with a larger number of services with more fine-granular requirements.

REFERENCES

[1] S. Shenker, "Fundamental Design Issues for the Future Internet," IEEE Journal on Selected Areas in Communications, vol. 13, no. 7, pp. 1176–1188, ISSN 0733-8716.

[2] L. Volker, D. Martin, C. Werle, M. Zitterbart, and I. Khayat, "An Architecture for Concurrent Future Networks," in Proceedings of the 2ndGI/ ITGKu VS Workshop on The Future Internet, Karlsruhe/Germany, Nov. 2008.

[3] FP7 ICT ADVISORY GROUP Working Group on "Future Internet Infrastructure" Version 8.

[4] Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation Raj Jain, Fellow of IEEE Washington University in Saint Louis Saint Louis.

[5] Developing a Next-Generation Internet Architecture Robert Braden, David Clark, Scott Shenker, and John Wroclawski July15, 2000.

