

# Chapter 1

## Issues with Current Internet Architecture

**Mohamed Boucadair**  
*France Telecom, France*

**David Binet**  
*France Telecom, France*

### ABSTRACT

*It is commonly agreed that the continuous increase of routing and forwarding tables (Huston, 2001; Meyer, Zhang, & Fall, 2007) is a sensitive issue which may question the growth of the overall Internet. Some technical practices such as multi-homing using Provider Independent (PI) prefixes and shrinking advertised prefixes to support advanced inbound traffic engineering policies exacerbate the increase of inter-domain routing tables (Narten, 2010). This chapter synthesizes routing and forwarding issues encountered by current Internet routing architecture and provides an overview of analyzed solutions.*

*Internet actors should work on an action plan to mitigate the increase of Routing Information Base (RIB) and Forwarding Information Base (FIB) table sizes and the load induced by routing updates churn (BGP Instability Report, n.d.).*

### PROBLEMS TO BE SOLVED

Simplicity, flexibility and extensibility were the main characteristics of the Internet architecture [Clark, RFC1958, RFC3426, RFC3439], but unfortunately these design principles are not the actual characteristics of the Internet. More precisely, the Internet is suffering from a wide range of complications which may impact its evolution.

Examples illustrating encountered complications include:

- **IPv4 address shortage:** Both the run out of Class B addresses and the whole IPv4 address space were a concern for the Internet community as soon as the early 90's. In 2011, the exhaustion of public IPv4 addresses has become a con-

DOI: 10.4018/978-1-4666-4305-5.ch001

crete concern for Fixed and Mobile IP Connectivity Providers. Both backward (e.g., The Extended Internet Protocol (EIP, [RFC1335, RFC1385])) and disruptive proposals (e.g., (Ullmann, 1993)) have been considered in the past to solve IPv4 address depletion.

- **Emergence of middleboxes such as CGNs (Carrier Grade NATs), firewalls and DPI (Deep Packet Inspection):** It has been reported recently that some enterprise networks contain as many middleboxes as routers (Bonaventure, 2011); as such, packets are altered in the forwarding path without any notification to the sender or the receiver.
- **Inability to extend protocols which are part of Internet foundations such as IP and TCP:** These protocols were designed to support options but in practice these options are “not anymore an option” (Fonseca et al., 2005) or their use is not reliable (Honda et al., 2011). This issue is likely to be encountered by IPv6 extension headers. The review of Internet’s history shows, as documented in (Handley, 2006), two evolution periods: period of fundamental changes (1970-1993) and a second period of failures (1993 to the present).
- **Inability to introduce new transport protocols at large, e.g., SCTP (Stream Control Transmission Protocol, (Stewart, 2007)) or DCCP (Datagram Congestion Control Protocol, (Kohler, Handley, & Floyd, 2006)):** This is a direct consequence of the massive deployment of middleboxes which break the end-to-end principle.
- **Restriction of reachability to some protocols:** Only TCP/UDP, and in some cases only HTTP, is accepted. This was a driver for several solutions that suggest to develop layer applications over HTTP (or in DNS) [RFC3205, RFC3426].
- Brokenness of bi-directional communications because reachability is not symmetric due to the presence of NAT and tunnels (e.g., If “A” can reach “B,” this does not mean “B” can reach “A”). The reachability asymmetry is now part of the “new” characteristics of Internet just like path asymmetry. Applications should be designed to accommodate this new constraint.
- Brokenness of applications which make wrong assumptions based on the IP address (Ford et al., 2011). A non-exhaustive list of these issues is provided below:
  - Incoming port negotiation mechanisms may fail
  - Incoming connections to Assigned Ports will not work
  - Port discovery mechanisms will not work
  - Some applications will fail to operate
  - Parallel/serial connections may fail
  - TCP control block sharing will be affected
  - Reverse DNS will be affected
  - Inbound ICMP will fail in many cases
  - Amplification of security issues
  - Fragmentation will require special handling
  - Port randomization will be affected
  - Penalty boxes will no longer work
  - SPAM blacklisting will be affected
  - Geo-location services will be impacted
  - Geo-proximity mechanisms will be impacted
  - Load balancing algorithms may be impacted
  - Authentication mechanisms may be impacted

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/issues-current-internet-architecture/77496](http://www.igi-global.com/chapter/issues-current-internet-architecture/77496)

## Related Content

---

### The Acceptance Process of the Internet of Things: How to Improve the Acceptance of the IoT Technology

Elodie Attiéand Lars Meyer-Waarden (2019). *Smart Marketing With the Internet of Things* (pp. 21-45).

[www.irma-international.org/chapter/the-acceptance-process-of-the-internet-of-things/208503](http://www.irma-international.org/chapter/the-acceptance-process-of-the-internet-of-things/208503)

### An Architecture to Implement the Internet-of-Things using the Prometheus Methodology

Bogdan Manae, Florin Fortiand Philip Moore (2020). *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications* (pp. 609-629).

[www.irma-international.org/chapter/an-architecture-to-implement-the-internet-of-things-using-the-prometheus-methodology/234965](http://www.irma-international.org/chapter/an-architecture-to-implement-the-internet-of-things-using-the-prometheus-methodology/234965)

### Using New Tools to Attract Visitors to Museums and Heritage Sites

Lia Bassa, Melanie Kay Smithand Árpád Ferenc Papp-Váry (2022). *Handbook of Research on Digital Communications, Internet of Things, and the Future of Cultural Tourism* (pp. 291-310).

[www.irma-international.org/chapter/using-new-tools-to-attract-visitors-to-museums-and-heritage-sites/295509](http://www.irma-international.org/chapter/using-new-tools-to-attract-visitors-to-museums-and-heritage-sites/295509)

### Network Security Policy Automation: Enterprise Use Cases and Methodologies

Myo Zarny, Meng Xuand Yi Sun (2019). *Emerging Automation Techniques for the Future Internet* (pp. 232-261).

[www.irma-international.org/chapter/network-security-policy-automation/214435](http://www.irma-international.org/chapter/network-security-policy-automation/214435)

### Modeling Secure 3D Web Applications

Krzysztof Walczak (2011). *Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management* (pp. 263-283).

[www.irma-international.org/chapter/modeling-secure-web-applications/49525](http://www.irma-international.org/chapter/modeling-secure-web-applications/49525)