Essay on The Design Philosophy of the DARPA Internet Protocols

André Rosa
DI/FCT/NOVA University of Lisbon, Lisboa, Portugal
Student № 48043
af.rosa@campus.fct.unl

I Introduction

Nowadays, the Internet is a fundamental service for the contemporaneous society, being leveraged for the most diverse applications, from leisure (e.g. media streaming and online gaming) to business (e.g. online banking, online stores, or ad services) as well as for military purposes. Although the Internet protocol suite (a.k.a. *TCP/IP*) specification is well known, sometimes it is difficult to determine the motivation which lead to its design. Therefore, in this essay, we inside on the article [1] which reviews the reasoning behind the decisions which shaped the architecture of the *TCP/IP* protocol suite.

The remainder of this document is structured as follows: Section §II provides an overview of the motivation for the development of the *Internet*; Section §III delves into the objectives of the *TCP/IP* protocol suite. Section IV discusses the origin and some implementation decisions of *TCP*; and Section V concludes the essay with some final remarks.

II The Origin of the Internet

Before the internet existed, there were several types of disjoint networks formed by different kinds of technologies. In particular, the *Defence Advanced Research Projects Agency (DARPA)*[1] was concurrently developing two types of networks: the *Advanced Research Projects Agency Network (ARPANET)* and the *ARPA Packet Radio Network (PRNET)*.

In this sense, *DARPA* felt the need to interconnect these already existing networks as well as to connect future networks, and thus the *Internet* emerged to address this necessity. Although designing a unified solution, which included several transmission mediums, would enable better performance, it would force to discard the already existing network architectures. Furthermore, each network usually corresponds to a separate administrative domain, which is independently managed. Thus, instead of a unified solution, it was preferred to design a solution that enabled the intercommunication between several already existing network architectures. The technique chosen to enable this interconnection was packet switching. This decision was due to packet switching being better suited for the desired applications in comparison to other alternatives, such as circuit switching, and the fact that the particular networks that were trying to be connected were already packet switching networks.

Thus, in a nutshell, the *Internet* corresponds to a network of networks, which are interconnected through Internet packet switches, called *gateways*.

III Objectives of the *TCP/IP* Protocol Suite

Having packet switching been defined as the technology used to interconnect the various networks, it was then necessary to define how devices on different networks could effectively communicate, i.e., it was necessary to specify a protocol that performed the intercommunication between devices belonging to different networks.

This protocol, called *Internet Protocol (IP)*, had the following objectives, in descending order by their respective priority:

1) ***Fault Tolerance***: the communication between devices must be guaranteed in the presence of failures of networks or gateways, provided that the networks remain connected.
2) ***Support Several Transport Services***: the *Internet* must be general enough to support multiple types of transport services, each with their requirements.
3) ***Deal with Several Types of Networks***: the *Internet* should enable to interconnect a broad spectrum of underlying networks, built with different architectures and technologies.
4) ***Distributed Management of Resources***: the *Internet* architecture should allow its distributed management.
5) ***Cost Effective***: the *Internet*'s communication cost should be adequate for the data being transmitted.
6) ***Easy to Join***: the hosts should be able to join to the *Internet* fairly easily.
7) ***Accountability***: the *Internet* should provide the ability to determine the entity responsible for a certain action.

This organization is a consequence of the *Internet* being developed in a military context, which involved hostile environments. Thus, fault tolerance was given a higher priority compared to other objectives, such as accountability. Next, we discuss each of these objectives in more detail.

A. Fault Tolerance

The capacity of maintaining communications, despite failures of networks or gateways, was the most important goal of

This essay was written in the context of the APRC course.

[1] Agency of the United States Department of Defense, which is responsible for developing emergent technologies for military purposes.

the *Internet*. As a result, the *IP* was responsible to completely mask any transient failures, providing the illusion that only one type of failure exists: a partition of the network between hosts. In this sense, state information associated with active communications, such as the number of packets acknowledged, has to be safeguarded. Thus, storing any state on intermediate gateways would require for this state to be replicated across multiple devices to survive failures. However, this is not scalable on the number of concurrent communications and is limited in the number of simultaneous failures that can be tolerated. Additionally, losing the state associated with an entity that is lost at the same time (fate-sharing), has no drawbacks in this case. For these reasons, it was decided that the *gateways* would have to be stateless, regarding on-going communications, and that it would be preferable that this state would be stored at the end-points of those communications. This alternative is much easier to manage and protects the state against any intermediate failures, however it delegates more responsibility to the hosts rather than the network.

Unfortunately, the *Internet* does very limited assumptions concerning the ability of a network announcing its failure, being error detection slower and less specific than in a multi-medium network design.

Nowadays, this state is no longer part of the *IP*, having been delegated to another protocol, the *TCP*, which is discussed in the next subsection.

B. Support Several Transport Services

The *IP* was designed to enable a panoply of several types of service , each with different requirements, such as speed, latency, and reliability. One of the most relevant types of transport services is the bi-directional reliable delivery of data. Initially, it was thought that this service could be general enough to support any other needed type of service. However, it became clear that supporting all types of service under one protocol was too troublesome. For instance, for the real-time delivery of data (streaming), it might be much more important to have low latency rather than having reliable delivery of data. On the other hand, for the transmission of a file over the *Internet* it is much more important reliability rather than latency. Consequently, this lead to the separation of these transport services from *IP* into isolated protocols, layered on top of the *IP*, with the *IP* providing a basic building block, called *datagrams*, which would be leveraged by these protocols to build transport services. In particular, the bi-directional reliable delivery of data service became the well-known *Transmission Control Protocol (TCP)*, while a simple application-level interface for the *datagrams* became the *User Datagram Protocol (UDP)*.

C. Deal with Several Types of Networks

The *Internet* must not only interconnect different networks but also interconnect a broad spectrum of network types, built with different architectures and technologies. The *IP* accomplishes this by assuming only a minimum set of functionalities the underlying networks are able to provide, which are: $i)$ be able to transport a packet or datagram, $ii)$ have a proper addressing mechanism if the network is more than just a point-to-point link, and $iii)$ be reasonably reliable (some packets might be lost). All other functionalities must be implemented on top of *IP*, as part of a transport protocol for instance, such as the reliable sequenced delivery of data provided by *TCP*.

D. Distributed Management of Resources

Another objective of the *Internet* is to enable its distributed management. Nowadays, this objective has been partially fulfilled, being the *Internet* composed by gateways of several autonomous systems, managed by several different entities. Within those systems, private routing algorithms can be used independently. To interconnect those systems, a different routing algorithm is used. Furthermore, the entities that manage the gateways do not have to be the same that manage the networks to which the gateways are connected to. However, the current solution is still very limited, especially in managing routing decisions across different domains.

E. Cost Effective

Unfortunately, the *Internet* is not as cost-effective as a more customized solution would have been. For instance, the *IP* headers are relatively large and if packets' payload is very small, the overhead is non-negligible. Another source of inefficiency is implementing all the mechanisms of the desired types of service at the hosts, rather than in the network. In case of poor implementation of these mechanisms, it might end up penalizing not only the hosts but also the networks themselves. Furthermore, even in cases of good implementations, this architecture may be a source of inefficiency. For instance, when packets are lost, the hosts themselves are responsible for detecting it and performing retransmissions, which is slower and generates more traffic, since the packets might travel across several intermediary devices, than the recovery at the network level would. Thus, the decision of delegating the implementation of the required types of services to the hosts rather than the network, to provide flexibility to the *Internet*, caused a dependency on the hosts correctly behaving, leading to a loss of robustness.

F. Easy to Join

Nowadays, the vast majority of computational devices has the ability to easily connect to the *Internet*. Furthermore, a new goal set for the future is to connect anything to the *Internet*, in the *Internet of Things (IoT)* paradigm.

G. Accountability

Currently, the *IP* has very poor accountability, i.e., the ability to determine the entity responsible for a certain action, since the source field of *IP* packets can be easily forged.

IV Transmission Control Protocol (TCP)

The *TCP* is the most widely used transport protocol on the *Internet*, being responsible for the bi-directional reliable sequential delivery of data between hosts. As previously mentioned, *TCP* was originally an integrating part of the *IP* that was later split into an isolated protocol.

Initially, the original *TCP* managed flow control based on both bytes and packets. However, it was established that regulating only the bytes was enough. This decision was a result of several factors, some of which became pointless while others revealed to be more important than initially predicted. The most relevant of these decisions was to enable grouping together several small packets into one larger packet in the case the retransmission of that data was required.

V Final Remarks

In summary, in this essay, we discussed the reasoning behind the decisions which shaped the architecture of the *TCP/IP* protocol suite, the foundation of the *Internet*. The *Internet* emerged to address the necessity of interconnecting several different networks. The fact that it was developed in a military context, prioritized fault-tolerance and flexibility over distributed management and accountability. Although the *Internet* accomplished its main priorities, there are still many challenges to address in the current architecture.

References

[1] D. Clark, “The design philosophy of the darpa internet protocols,” *SIGCOMM Comput. Commun. Rev.*, vol. 18, no. 4, p. 106–114, Aug. 1988. [Online]. Available: https://doi.org/10.1145/52325.52336