From Concept to Connectivity: Designing the Internet

GUSTAVO COSTA, JOÃO PINHEIRO, JOÃO OLIVEIRA, PEDRO FONSECA, and RICARDO CAVALHEIRO

This paper aims to present our thought process when approaching the proposed problem of designing the Internet as well as the achieved solution. The goal of the problem is to design the Internet as if we were in the 1970s and it hadn't been invented yet. We started by thinking about the requisites of what our solution should accomplish and how the existing infrastructure could be used. Then, we devised and proposed both a protocol for communication between devices on the Internet. Finally, we found limitations and future improvements in our solution.

1 INTRODUCTION

In this assignment, we were asked to imagine that we were back in the 1970s and design the non-existent Internet.

With this in mind, some considerations had to be taken into account, like the number of users, the type of users, its reliability, and its resilience.

We were also imposed a restriction: to not research the Internet architecture. The reason for this comes from the fact that the assignment is mainly a learning experience and an entry point to software systems architecting rather than an attempt at actually designing a fully functioning Internet.

2 DESIGNING THE INTERNET: THE PROBLEM

As previously stated, the main objective of this assignment is to design the Internet without researching its architecture.

To do so, a couple of considerations had to be made:

- The Internet will be used worldwide by millions of people.
- It must be highly reliable.
- The different connected devices can change.
- Many different types of devices can connect to it.

Stemming from these considerations, some non-functional requirements can be listed:

- High-load tolerance: Reliability in the face of many users.
- Fault tolerance: Reliability in the face of faults.
- Change tolerance: The devices that are connected can change but the underlying structure cannot.
- Diversity acceptance: Different devices should be able to communicate between them.

Some other issues had to be taken into account, seeing as the Internet would be a new worldwide system, which meant that infrastructure would be of concern and had to be designed to fit the needs of the system.

Authors' address: Gustavo Costa, up202004187@up.pt; João Pinheiro, up202008133@up.pt; João Oliveira, up202004407@up.pt; Pedro Fonseca, up202008307@up.pt; Ricardo Cavalheiro, up202005103@up.pt.

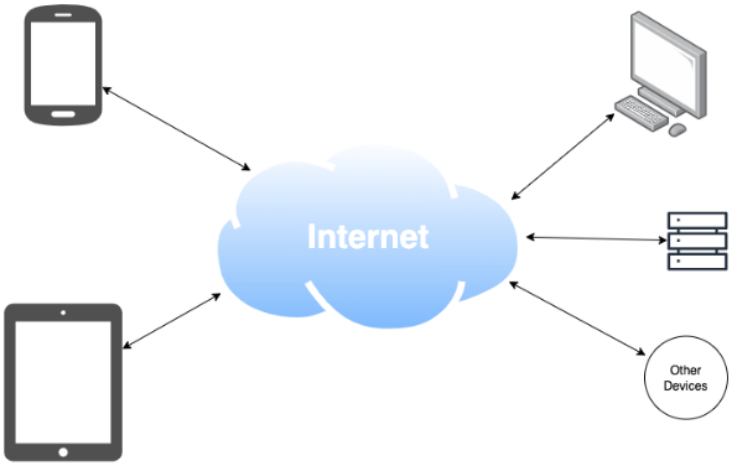

Fig. 1. Simple generalization of the Internet, that takes into consideration a plethora of devices

3 DESIGNING THE INTERNET: THE INFRASTRUCTURE

Generally speaking, there are two ways to approach a problem that involves architecting something: come up with a solution and then create the infrastructure to support it, or research the available infrastructure and come up with a minimally disruptive solution. Our approach involves the latter and we started by making a very broad architecture and then expanding its components.

3.1 Contextualization

Since we're working in the 1970s, we believe that it's important to contextualize that period so that we can best understand the problem at hand. It's also important to preface that due to the nature of the previously mentioned imposed restrictions, the following contextualization is mainly a set of assumptions, rather than historical and factual data:

- Telephone communication companies (landline) exist and allow for communication between multiple different telephones, at least in the same house, at most in the other half of the world.
- Said companies follow a hierarchical structure in which calls are routed between "centers" until they reach the desired destination.
- Radio waves technology has existed for decades and is well understood and used.

Although only assumptions, they are not baseless. Multiple historical events lead us to believe that, if not true, those assumptions were, at least, feasible. One of those events in particular is World War II. WWII happened in the 1940s and displayed the use of highly advanced pieces of technology that relied on radio waves for short-distance communication and some sort of long-distance communication mechanisms that allowed for, for example, upper echelons of the USA's army to communicate with field troops battling in Europe or Asia.

3.2 Telephone communication

Now that we had an idea of what was available, we could start working on developing the solution.

We know (we assume, at least) that telephone communication is capable of sending information worldwide. Abstractly, this is the same idea as what we're attempting to propose: a system capable of transferring information from one device to another in different parts of a network. This means that we can use the existing underlying infrastructure of telephone communication to support the Internet, ideally with minimal changes.

With this in mind, if we use the telephone cord to connect the devices to the pre-existing network we could, in theory, have the Internet.

3.3 Locating machines and resources

Unfortunately, to have a working Internet, a couple more things are needed. For instance, there's no way to know where to locate a certain resource or where the machine with said resource is physically located.

For that, we propose a hierarchical system of navigation, which can be seen in Fig 2. This system adapts the current schema of landline telecommunication between different scopes (local, regional, national, international) to allow for communication between different devices in any part of the globe.

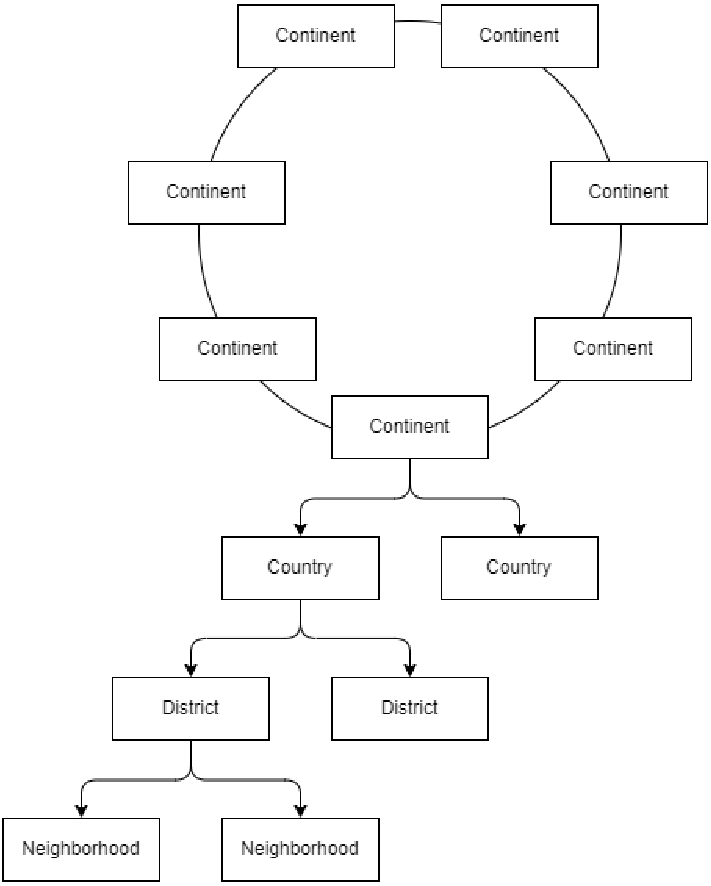

Fig. 2. Information navigation hierarchy on the Internet

Each neighborhood has a station responsible for distributing the information to the devices inside that neighborhood (local scope). Multiple neighborhoods can communicate via the district's station responsible for all the neighborhoods inside it (regional scope). To allow districts to communicate with each other, there are countrywide stations that route the information to the corresponding district (national scope). Finally, there are also continental stations that allow for international communication and are connected, ensuring a decentralized network is formed (international scope).

A simple analogy to help better understand this can be made with telephone numbers. Say person A lives in Cedar Hills, Utah Valley, USA, and wants to call person B, a Portuguese citizen living in Porto. For that to happen, A's call has to be routed through multiple stations before arriving at B's telephone. Firstly, it has to go from A's house to their neighborhood's station, Cedar Hills' station. From there it goes to Utah's district station. Then, to the station responsible for all of USA's calls. After that, to the North American continental station. Now, it's transferred to the European continental station, from where the process can be done backward, descending the tree up until it reaches a leaf, which is B's house.

We don't even have to worry about how to implement this for the Internet because it's already been done by telecommunication companies.

3.4 Wide-area networks

With all this laid out, we effectively have multiple interconnected wide-area networks, WANs for short, which represent a form of computer network designed to connect geographically distant locations.

3.4.1 ***Neighborhood WANs.*** The lowest level of the hierarchy contemplates the Neighborhood WANs responsible for connecting houses within the same neighborhood.

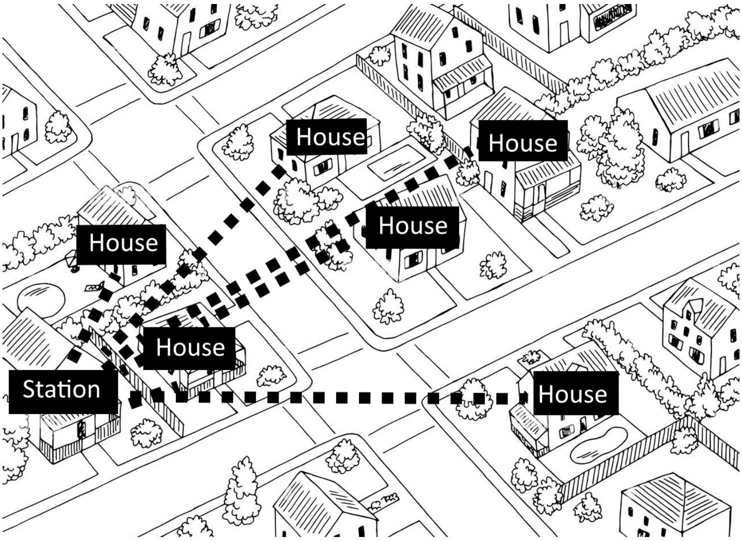

Fig. 3. Connections within neighborhoods

3.4.2 ***District WANs.*** At the second lowest level of the hierarchy are WANs serving districts. These WANs connect all Neighborhood WANs within a specific geographical area, typically covering cities or regions.

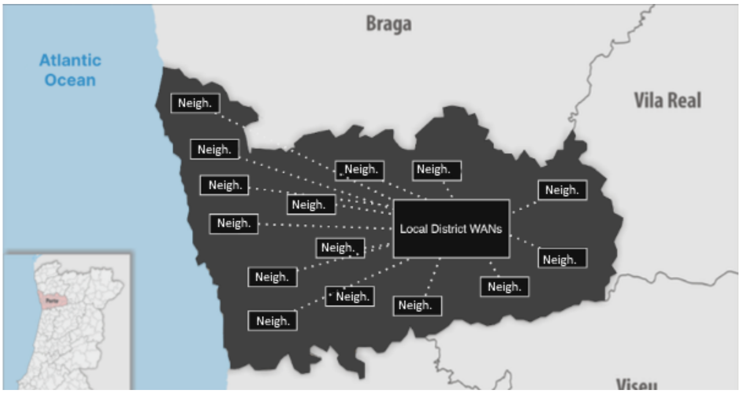

Fig. 4. Connections within districts

3.4.3 Country-level WANs.

Country-level WANs interconnect the local district WANs within a country. Each country has at least one WAN, serving as a hub for regional connectivity.

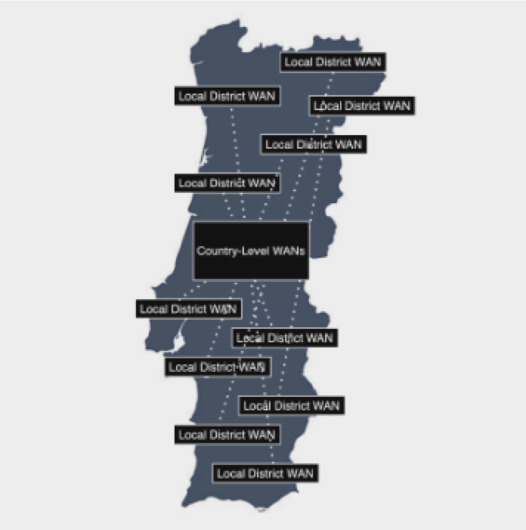

Fig. 5. Connections within countries

3.4.4 Continent-level WANs.

Continent-level WANs connect multiple country-level WANs within a continent. These WANs ensure intercontinental communication by linking countries within the same landmass.

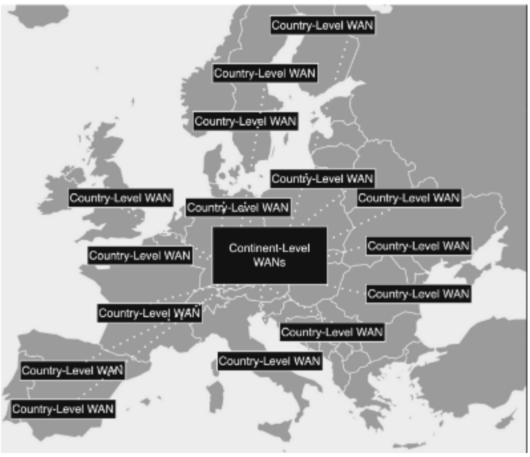

Fig. 6. Connections within continents

3.4.5 ***Global Reach.*** Finally, we have global reach as the highest level of the hierarchy, connecting all continent-level WANs worldwide. It ensures global connectivity by enabling communication between different continents.

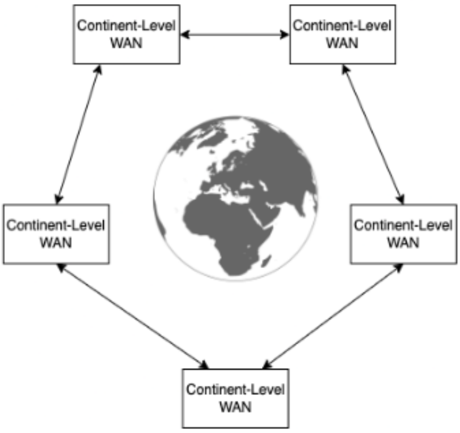

Fig. 7. Connections between continents

3.5 Device Identification

Device identification is a big issue when dealing with a multitude of devices in a network. How can one device know where to send the request to get the resource it wants? For this, we proposed a protocol and a new type of device: the router. As the name indicates, the router is responsible for routing the requests to each device inside the same local area network (LAN), effectively, inside each house. This also solves two problems we had:

- If we disconnect the phone cord from the telephone to have access to the Internet, we lose the ability to receive or make phone calls.
- Stemming from the prior issue, only one device per house could be connected to the Internet at the same time, unless the homeowners installed multiple landlines, which is not ideal.

The router serves as a network interface and hub for all requests that enter or leave a house, allowing for multiple devices to communicate, as well as having multiple publicly available resources on the same machine, for example.

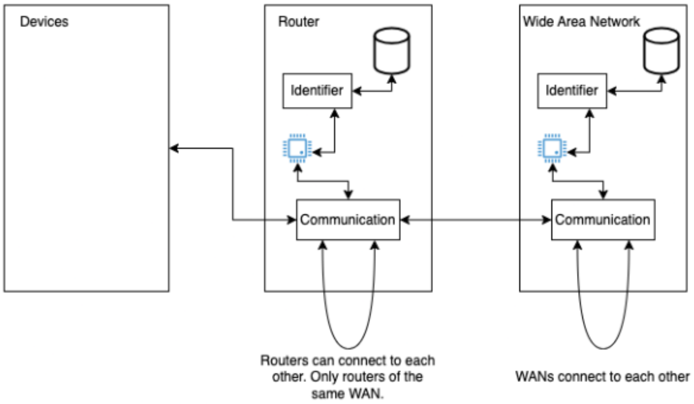
Devices
Router
Identifier
Communication
Wide Area Network
Identifier
Communication
Routers can connect to each other. Only routers of the same WAN.
WANs connect to each other

Fig. 8. Router functionality

Now, how does the network know where the requests are coming from and where to send them once they're inside one of the WANs? This is solved by the Identifier block within the Router and the Wide Area Network. For this Identifier Protocol, we took inspiration from how telephones work.

The Identifier Protocol is done by the routers and WANs. The Routers are responsible for attributing an ID to all of the devices on their LAN guaranteeing that the addresses used are not repeated to guarantee uniqueness and reliability. WANs also do the same with the routers. Each router is given a unique address by the WAN to identify the router when communicating across WANs. On the top-level of WANs, Continent-Level WANs, their IDs are manually decided as these are just a handful of machines.

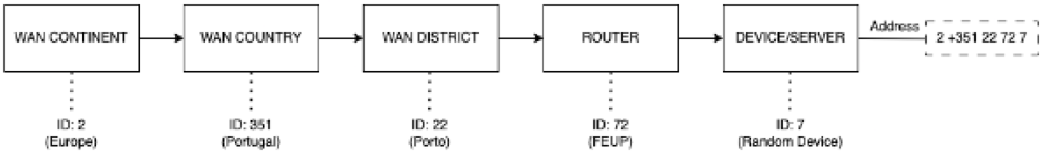

Fig. 9. Device Identifier Structure

The address for a device will look like this: 2 +351 22 72 7. The first digit 2 is the ID of the Continent-Level WAN followed by the country WAN ID with a plus before it to identify the country. Afterwards, we have the district ID followed by the router ID, and finally the device ID.

Besides that, we also introduced the concept of storage to the routers and WANs. The reasoning behind this is that the addresses of the devices/routers need to be saved for later identification. On top of that, when a router wants to find an address, it will ask its WAN for the location of the device and then these will proceed to connect directly to each other as long as they are on the same

WAN. If not, WAN will ask the other WANs for the location of the address and connect the router through it to the device associated.

In summary, our new system introduces a look into the inside of routers and WANs. Devices connect to the “Communication” block in the routers. Within the router, the router can use the “Identifier” block to attribute an address to the device which it will save in its local storage. Routers can also connect to each other to communicate and are also connected to a main WAN. This WAN does the same thing as the router (it identifies the router) and connects with the other WANs.

3.6 Network messages

Communication occurs through the exchange of packets using standardized protocols, ensuring efficiency and coherence within the system.

Devices have to be equipped with network interfaces, enabling connectivity to the network and facilitating data exchange. These interfaces serve as the bridge between devices and the broader network infrastructure.

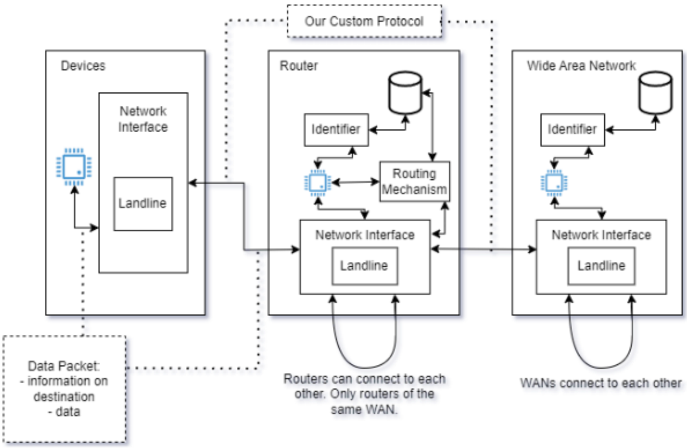

Fig. 10. Use of data packets

The interaction and exchange of data among devices would be facilitated through the transmission of packets. This method involves breaking down data into smaller units, known as packets, before sending them across the network. This is the packet format we came up with to guarantee the particular properties we desire, such as security and reliability.

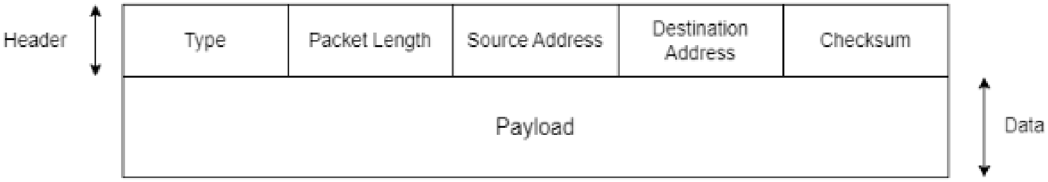

Fig. 11. Data Packet Structure

Header - Contains information about the data carried by the packet:

- **Type** - Specifies the purpose or nature of the packet, allowing devices to interpret and process it accordingly;
- **Packet Length** - Indicates the size of the packet, enabling efficient handling and allocation of resources during transmission;
- **Source Address** - Identifies the origin of the packet;
- **Destination Address** - Specifies the intended recipient of the packet;
- **Checksum** - Helps to verify the integrity of the packet during transmission, reducing the risk of data corruption.

Payload - This is the actual message/data that the packet is delivering to the destination.

The header components facilitate effective routing, error detection, and secure addressing, while the payload carries the essential information between devices.

By including these properties in the packet structure, we establish a foundation for reliable communication, but that's just the first step. Similar to how humans use registered mail when exchanging messages to verify their accuracy, we will also employ this technique to detect authenticity.

When a device sends a packet, it will expect an acknowledgment (ACK) from the recipient confirming successful reception. If no ACK arrives within a set timeframe, the sender automatically retransmits the packet, ensuring it reaches its destination. This design improves the communication protocol's overall robustness and security in addition to ensuring the efficient transmission of data.

3.7 Optimizations

Furthermore, we introduced the concept of "Routing Mechanisms" to optimize data transmission paths across the network. As previously mentioned, routers first ask the WAN where the router he is trying to connect is, and only after does it connect directly to it. A Routing Mechanism is what allows the router to communicate directly with the other router which allows for more efficient communication and improves reliability and scalability.

3.8 Considerations

To summarize, the inclusion of Network Interfaces across all components underscores the scalability of our system, as any device equipped with a Network Interface can seamlessly connect to the network. On top of that, we also added some protocols that can be used for communication, as well as a Routing Mechanism on the router. This Routing Mechanism is what will decide where the data packet is sent. Initially, it will be sent to the WAN but after discovering the destination router the routing mechanism with the use of a Routing Protocol will send the data packets directly to the destination node.

4 CONCLUSION

In retrospect, given the technological landscape of the 1970s and the available resources during that era, we believe that the proposed architecture for the Internet adequately addresses the prevailing needs. Considering the limitations of that time, this architecture not only meets the required specifications but also showcases an innovative and practical approach to the challenges presented.