The infrastructure on which the Internet is based is made of three layers. The physical layer (telecommunication) includes the wires and cables through which 'packets' of information travel, the transport layer (protocols) refers to the technical rules that govern these packets, and the application layer deals with Internet content and its applications (content).

First layer

The telecommunication layer is the physical structure that allows Internet traffic to flow. This layer includes fibre optic cables, mobile networks, towers, submarine cables and all other wired and wireless technologies allowing for connectivity.

The 'backbone' of the Internet – the cables that link the world together – consists mainly of international submarine cables. There are also projects focused on terrestrial cables, which can be laid down at the same time as more traditional railroad and energy pipeline projects. Nonetheless, where possible, submarine cables tend to offer better performance. For more, see: http://www.itgsnews.com/mapping-internet-maps/.

The cables connect with each other, and with land-based networks, at Internet traffic hubs. Most Latin American cables, for example, reach land in Miami. Other important hubs are London, New York and Amsterdam.

Once the cable has reached land, another set of connections – the 'middle mile' – act like a trunk road or railway network, connecting cities and towns to these Internet traffic hubs, before a further set of lines (the last mile) connect the individual customer.

Therefore, downloading documents from a server in California to a user in Germany means that the three levels – or tiers – of ISPs, 1, 2 and 3 must work together. This is done through a combination of 'peering' and 'paid Internet transit' agreements.

A Tier 1 ISP provider (working at the level of the 'backbone') only exchanges traffic with another Tier 1 ISP provider and not with end users. The exchange of traffic occurs without costs (i.e. each carries traffic from the other. This is known as a peering agreement).

A Tier 2 ISP connects Tier 1 and Tier 3 ISPs through a mixture of peering agreements and the purchase of internet traffic. In fact, Tier 2 ISPs can pay a fee for traffic through Tier 1.

A Tier 3 ISP is a provider that exclusively purchases internet transit from Tier 2 ISPs, without peering agreements. Tier 3 ISPs receive traffic from homes and businesses.

First Layer policy issues and main actors

The International Telecommunication Union of the United Nations (ITU) is very active in questions relating to the first layer. The ITU develops rules for coordination among national telecommunication systems and sets voluntary technical standards. In addition, the World Trade Organization (WTO) has provided a framework for general market rules and e-commerce.

The current main policy issues at the telecommunication level are the reduction of government regulations and restrictions as a means of stimulating competition and new market entrants,

especially in least developed countries where telecommunications tend to be dominated by monopolies. Linked to this are the questions about the role of connectivity as a driver of development.

Second Layer

For information to travel, there need to be rules – or protocols – in place. The TCP/IP is the rule that governs the way in which that connection, and the transmission of data, takes place. Indeed, it is the standard that effectively allowed the Internet to develop globally.

The TCP/IP standard is governed by three principles: packet-switching (messages are split into smaller pieces and sent to their destination through different routes), end-to-end networking (the network should be neutral, and communications should take place at the origin and destination only), and robustness (the data sent always conforms to certain specifications, but can be received in a more flexible way).

Besides these standards, the Internet works through a system of addresses (IP addresses and domain name systems) that allows each user's machine to be identifiable (an IP address, for example, is like a person's physical address) and easy to remember by humans (Doman Name Systems translate a sequence of numbers into human language, i.e. 204.13.248.115 into Amazon.com).

Second layer policy issues and main actors

Many actors are active in the second layer (protocols). We will focus on the two most important, the Internet Engineering Task Force (IETF) and the Internet Assigned Name Authority (IANA) whose work is carried out regionally thorough two other affiliates, Primary Rate Interface (PRI) and the Internet Corporation for Assigned Names and Numbers (ICANN). The former is responsible for the revision of standards, the latter for the assignment of IP addresses.

This seemingly technical set-up is full of policy issues. At the IP/protocol level a major concern is the limitation of IP numbers. Because of the ever-growing number of devices connected to the Internet, the finite number of IP addresses that can be generated will soon reach capacity. A new standard, IPv6 (standing for Internet Protocol version 6), was developed in 1996 and would provide a response, but its deployment has been slow for several reasons including limited awareness and technical fragmentation.

A further concern is around the security of transport protocols, which can have major implications for device authentication, data integrity and users' privacy. Security controls exist for network communications at different layers of the TCP/IP model (individual links in the network, the network as a whole, the transport layer (TCP/IP), and applications - read more about this here), but not as an overall process. Because of this, a security control at a one layer cannot provide complete protection, because operations at one year will not be picked up at another.

Another important policy issue of the second layer relates to the Domain Name System (DNS). As highlighted, the Domain Name System (DNS) translates numbers into human-readable internet addresses. This is also subject to a number of policy discussions.

When we go to Google.com or Harvard.edu or archive.uk, we are looking at gTLDs (generic top level domains such as .com, .pub, .rentals, .edu etc.) and ccTLDs (country code top-level domains such as

.uk, .au, etc). This information is managed by a registry operator whose responsibility is to administer and maintain a database with the details of the so-called top-level domains (TLDs).

From a policy perspective, there are several sensitive areas related to the DNS. The first is the protection of trademarks and the resolution of possible disputes and the second are issues related to privacy and data protection. In an effort to reduce cybersquatting, a practice allowed by the fact that names were allocated on a first-come-first-served basis, the World Intellectual Property Organization (WIPO) and ICANN worked on a Uniform Dispute resolution Policy (UDPR) to reduce this behaviour.

There are also privacy and data protection issues related to the management of the registry database and the fact that it contains publicly available information (names, emails and postal addresses) of registrants.

Third Layer – Content transmission

Policy issues in the third year relate to how content itself is managed and transmitted. It includes questions around net neutrality, cloud computing, big data and the Internet of Things (IoT). Net neutrality has received particular attention recently.

The Internet Service Providers who provide internet access to users have an economic incentive to use their power over what users can see, and at what speed. In some cases, they offer particular additional services such as making phone calls over the internet (the idea of WhatsApp), or music and video-streaming. By making other providers' services run more slowly (and so violating network neutrality – or net neutrality), they can gain a competitive advantage. Alternatively, they can do deals with certain content or service providers to ensure that their services run faster.

However, many believe that traffic should not be subject to this sort of 'management', and argue that ISPs should be transparent in their network practices, and users' access should be unrestricted for any legal content on the Internet. This includes 'zero-rated services' (which are provided to users without it counting towards their data caps), which are also seen also a violation of the basic principle of neutrality, given the advantage it gives certain providers over others.

In addition to the economic advantage this brings, violations of net neutrality pose fundamental questions about the openness of the internet, and risks favouring those with more resources. This effectively limits freedom of access to information and freedom of expression.

This issue has led to calls in many countries for legislators and broadband regulators to act in order to ensure that the activities of operators do not harm users or providers of content unfairly.