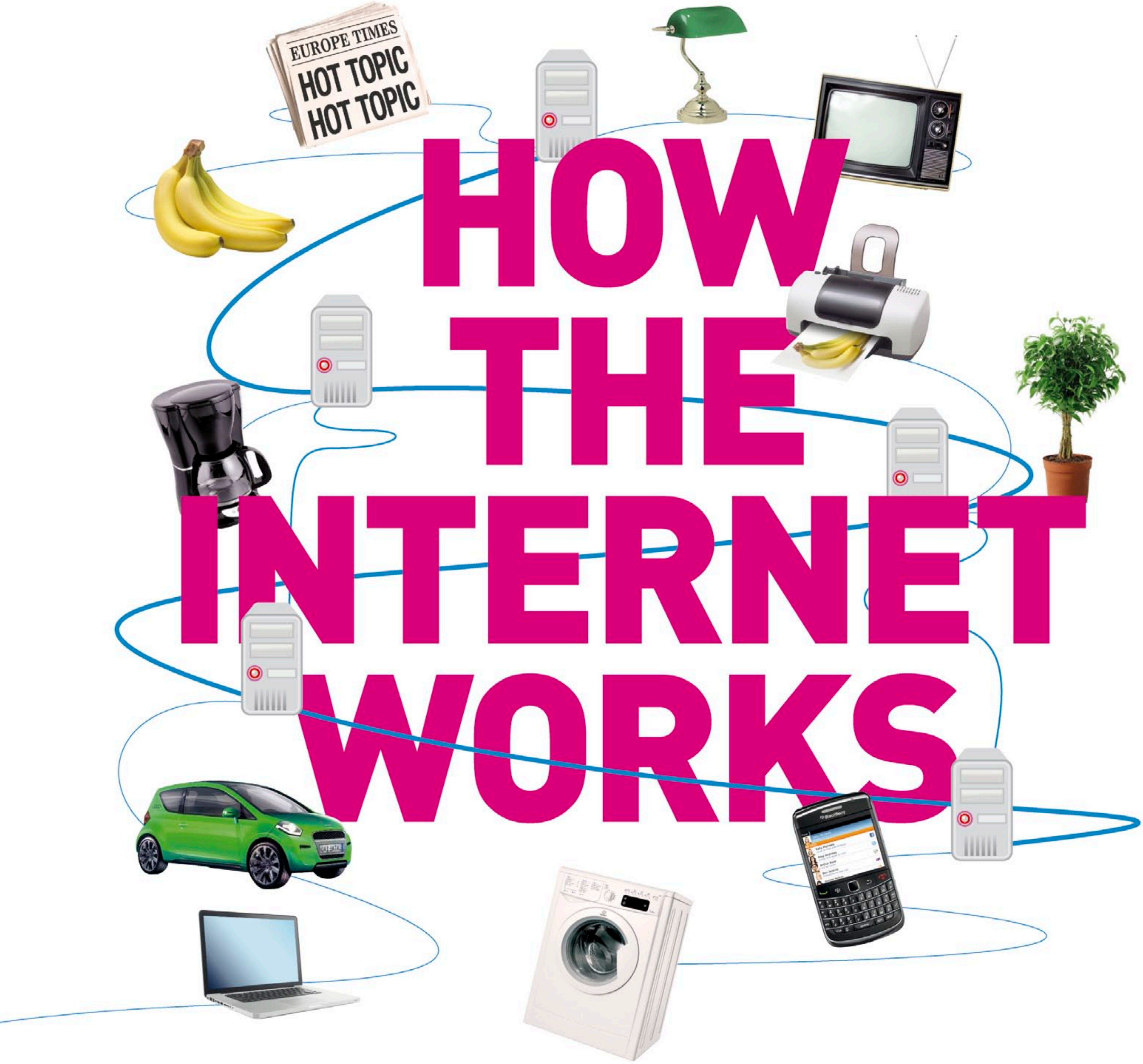
The EDRi papers

EDITION 03

HOW THE INTERNET WORKS



A guide for policy-makers

EUROPEAN
DIGITAL
RIGHTS

This booklet is intended to provide policy-makers with a basic overview of Internet and Internet-related technologies. The aim is to provide a user-friendly reference guide to some of the key technologies that are at the core of the Internet. We hope that this will provide a valuable reference tool, cutting through the jargon and demonstrating the functioning of the open Internet, on which so many civil rights and so much economic activity now rely.

CONTENTS:

Booklet written by:
Joe McNamee, Advocacy Coordinator
Kirsten Fiedler & Marie Humeau, Advocacy
Managers and Sophie Maisuradze, Intern

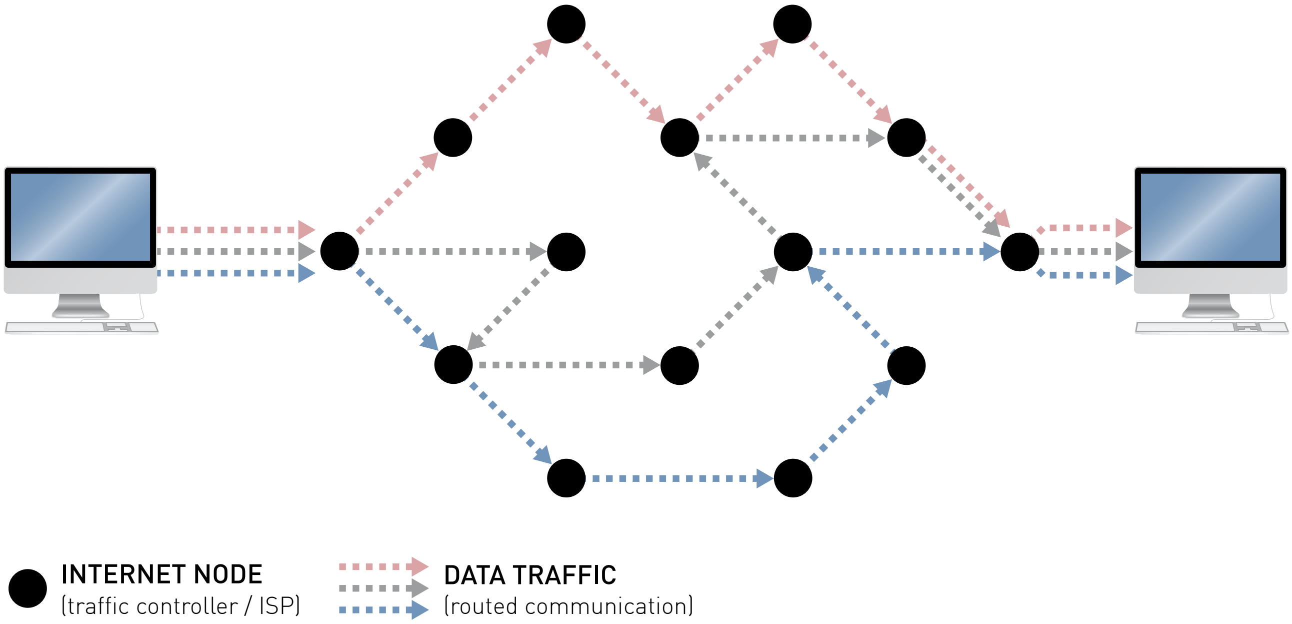
Design by: CtrlSPATIE

European Digital Rights (EDRi) is an association of 28 privacy and digital civil rights associations from 18 Countries.

European Digital Rights
39 Rue Montoyer
B-1000 Brussels
tel: + 32 (0)2 550 4112
brussels@edri.org

THE INTERNET

A NETWORK OF COMPUTER NETWORKS



The Internet is a global system of interconnected computer networks.

When two or more electronic devices (e.g. computers) are connected so that they can communicate, they become part of a network. The Internet consists of a world-wide interconnection of such networks, belonging to companies, governments and individuals, allowing all of the devices connected to these networks to communicate with each other.

In order to communicate, computers need to be able to understand each other. On the Internet, communication is possible because all devices use the same "language" or protocol, namely the Internet Protocol (IP), a "single market" with no physical, technical or national barriers. It forms the basis for all other systems of communication on the Internet.

Sending any communication over the Internet using the Internet Protocol is quite like sending the pages of a book by post in lots of different envelopes. All of the envelopes use the same sender address and the same destination address. Even if some envelopes are transported by ship and others by air, the envelopes all eventually arrive at their intended destination and the book can be reassembled. The fact that page 47 was received before page 1 is of no importance.

On the Internet, the contents of the envelope are also based on conventions/ protocols (agreed formats), one for each type of communication. Examples of such conventions on top of IP are:

- SMTP for sending emails
- HTTP for accessing web sites and
- BitTorrent for peer-to-peer (P2P) file sharing (a way to exchange data files with large groups of people).

Anyone is free to invent their own convention/ protocol and use it on the Internet, as long as it works on top of the Internet Protocol. In other words: the only limit is the limit of the human imagination, the only rule is that the address on the envelope is in a standard format. The openness of the system is what makes the Internet the global phenomenon it is. Every restriction on the openness of the Internet reduces its potential for future development. The universal use of a single protocol for all communications has a number of important advantages. The devices that are responsible for transporting Internet data (called routers) do not need to be programmed differently to deal with different types of data – they don't even need any information about the data they are transporting as long as it is all using the Internet Protocol. Like the postman delivering traditional mail, they only have to look at the outside of the envelopes to be able to deliver the message. It doesn't matter if the envelope contains a bill or a love letter (except to the recipient of course).

This leads to :

- Unlimited innovation possibilities in terms of new protocols and applications;
- ”Privacy by design”: there is no need to know anything about the contents of any communication;
- Flexible, fast data flow;

At its core, the Internet offers only one flexible service: getting data from one device to another regardless of the nature of the devices, regardless of how and where the devices are connected to the Internet and regardless of the nature or content of the data.

It is this openness and flexibility that is the primary reason for the innovation and democratic and economic successes of the Internet.

> **“It is this openness and flexibility that is the primary reason for the innovation and democratic and economic successes of the Internet.”**

THE IP-ADDRESS

A DIGITAL ADDRESS

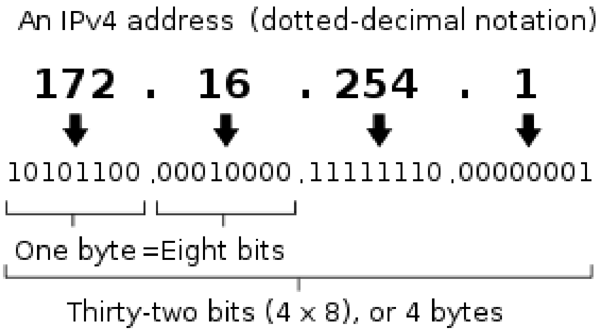
An IP address is a numerical address that is assigned to every device connected to the Internet.[01]

In many cases, IP addresses may be used to identify an organisation or individual that has acquired the services of an Internet Service Provider in order to connect one or more devices to the Internet.

In other cases, particularly on corporate networks, public or unprotected wireless connections and mobile Internet connections, the IP address does not always identify the person behind some digitally traceable act.

As the common household and business router will often display just one IP address for all of the people connected to it, the IP address will identify a group of people rather than just one individual. As a result, it is often hard, if not impossible, to be sure who exactly did what, purely on the basis of an IP address.

On the other hand, IP addresses are very often personally identifiable, and so, following a basic precautionary principle, must be treated as such unless they can definitively proven not to be.

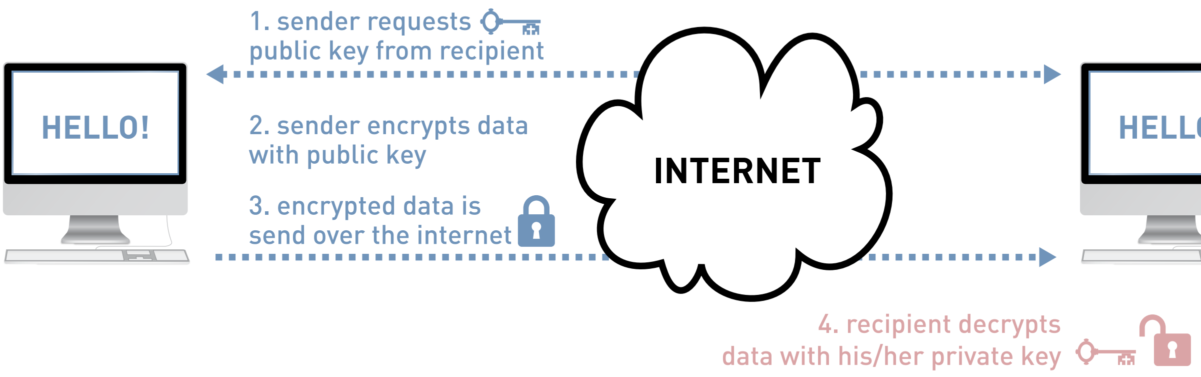


> “the IP address does not always identify the person behind some digitally traceable act”

[01] Due to shortages in the current generation of IP addresses, it is increasingly common, particularly in business networks, for IP addresses to be shared – by all of the computers in one office, for example. The current shortages are being addressed by the roll-out of IPv6 addresses.

ENCRYPTION

PRIVACY IN A PUBLIC NETWORK


1. sender requests public key from recipient
HELLO!
2. sender encrypts data with public key
3. encrypted data is send over the internet
INTERNET
HELLO!
4. recipient decrypts data with his/her private key

How can a user send a sensitive message so that it remains secure from prying eyes? If you send a letter, it could be intercepted, opened, read and then closed without leaving a trace. A telephone call can be wiretapped.

Rapid development of cryptography started in 20th century together with development of computing technologies. Computers allowed not only much faster encryption of electronic messages, but also much faster cracking of encryption keys used so far.

Encryption is not a silver bullet and doesn't guarantee total confidentiality. A frequent technique to bypass encryption is to capture the message before it even gets encrypted – for example by a stealth Trojan horse program installed on sender's computer that will monitor all keys pressed on the keyboard or even in the victim's mobile telephone.

Another attribute you almost always need to protect when encrypting a message is its integrity (i.e. the completeness of the file) – otherwise the message can be manipulated, without even knowing the encryption key. Most respected encryption tools will do that for you automatically.

The following image demonstrates the stages of public key encryption – this works on the basis of a pair of keys – one public and one private:

1.The sender requests a copy of this public key.

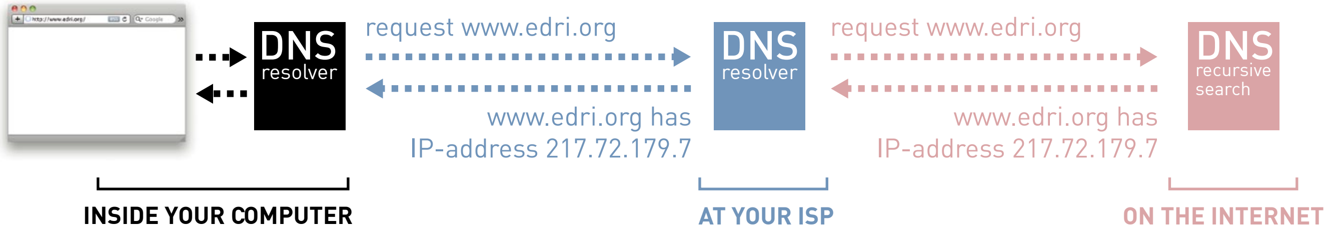
2.Using the appropriate software, the sender encrypts the message using the recipient's public key.

3.The message is sent.

4.The recipient decrypts the message by using the public key and the private key together.

THE DOMAIN NAME SYSTEM (DNS)

THE INTERNET'S PHONE BOOK



When you put a website on the Internet, it will be reachable via the numerical IP address of the web server hosting it (at time of writing, EDRi.org's address is 217.72.179.7, for example). IP addresses are, however, not easy to remember for humans. Using them to identify online resources is also not practical as services on the Internet occasionally have to move to a new IP address (if they change service providers, for example).

As the use of IP addresses for websites is neither practical nor user friendly, "domain names" (such as edri.org) were created. The global Domain Name System works a little like a phonebook for the Internet.

If you know the domain name of the website you want to visit, the Domain Name System is used – invisibly and automatically – to find the corresponding IP address of the web server where the website can be found. So, when you type http://edri.org, your computer identifies this as being 217.72.179.7 and sends a request specifically for our website to retrieve it.

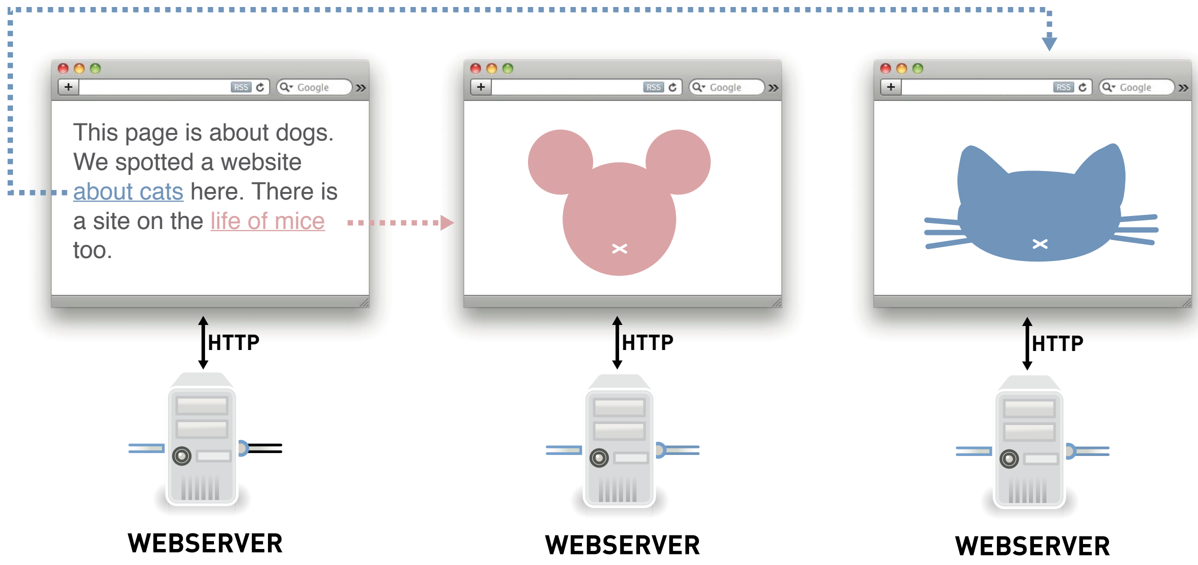
The system for looking up a domain name works on the basis of a hierarchy. When you type http://edri.org, your computer first connects with a server to ask for the address.[02] The default DNS server is usually run by your Internet provider, but it is possible to use a different one.

If somebody has recently accessed http://edri.org, the DNS server will "remember" the details and provide you with the correct IP address. If not, it will refer the query to a higher level of authority, where the same process is followed. At the highest level of authority are 13 "root servers" that ultimately collect together DNS servers. The 13 root servers are very robust and have huge capacity. They have so much capacity that they continued to work efficiently even when under major attacks (so-called "distributed denial of service" attacks).

[02] If your computer has accessed the http://edri.org recently, then it already knows the IP address and does not need to check it with the service provider.

THE WORLD WIDE WEB

LINKING THE INFORMATION SOCIETY



This page is about dogs. We spotted a website about cats here. There is a site on the life of mice too.
HTTP
HTTP
HTTP
WEBSERVER
WEBSERVER
WEBSERVER

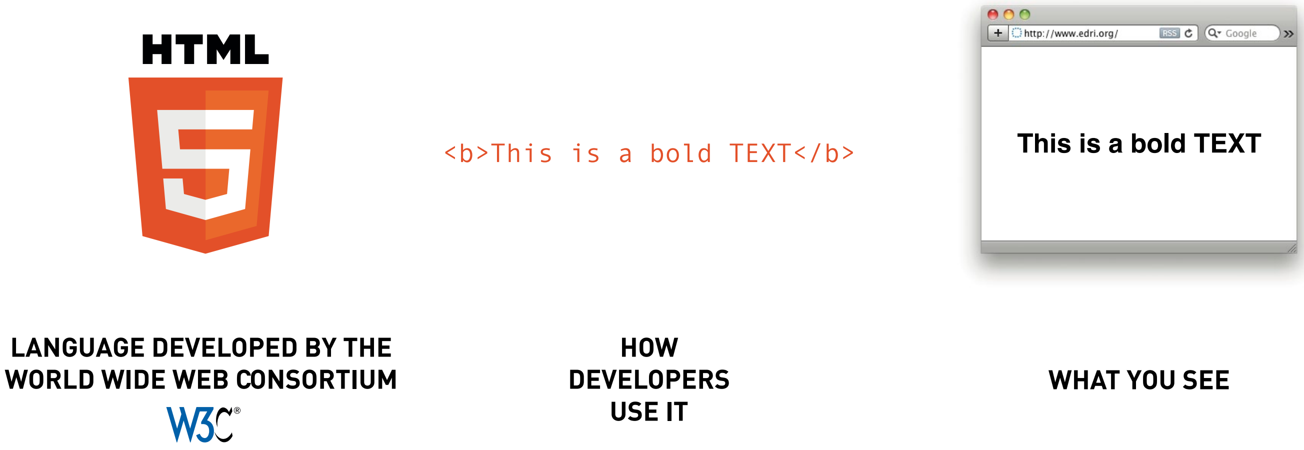
The World-Wide Web is built on HTTP, a relatively young protocol (language) that is built on top of the Internet Protocol (IP). HTTP stands for HyperText Transfer Protocol, and was designed to download so-called hypertext documents (what are now known as "web pages") and to send some basic information back to the web server.

Web pages are created using the formatting language HTML, (HyperText Markup Language). The rules of this language are set by the World Wide Web Consortium (W3C), and specify special markers to indicate typograhy and layout properties. For example, text in bold will have <b> **before it and** </b> after it.

While there are several versions of the specification (HTML5 being the most recent), the HTML development process is continuous and open to participation. Once the standards have been set, there is no licence or fee for using HTML. The advantage is that all available computer systems understand the instructions in HTML in the same way – so anyone can use the language (for free) and be sure that every device will display the web page in the same way. The Web (and the world) would be far poorer if people had to pay to develop pages in the languages of different types of computer.

This open and free character of HTML is essential to ensure compatibility of web pages across all sorts of devices: desktop computers, mobile phones, tablets, laptops and more. Proper application of the HTML specification to format webpages also ensures accessibility for people who are visually impaired – otherwise text reading systems will not be able to understand the pages being accessed.

Webpages are published on machines known as "web servers". A web server is a computer that can be found by its unique IP address (as described on page 5). Usually many domain names (such as www.edri.org and www.bitsoffreedom.nl) can be found at the same IP address because they are stored ("hosted") on the same server. Thus, a single web server with a unique IP address can host numerous websites. In the case of commercial web hosting companies, there can be hundreds of unrelated websites on one single web server. Attempts to "block" individual websites on the basis of their IP address have therefore always had disastrous consequences for the unrelated pages on the same server.



```
<b>This is a bold TEXT</b>
```

LANGUAGE DEVELOPED BY THE WORLD WIDE WEB CONSORTIUM

HOW DEVELOPERS USE IT

WHAT YOU SEE

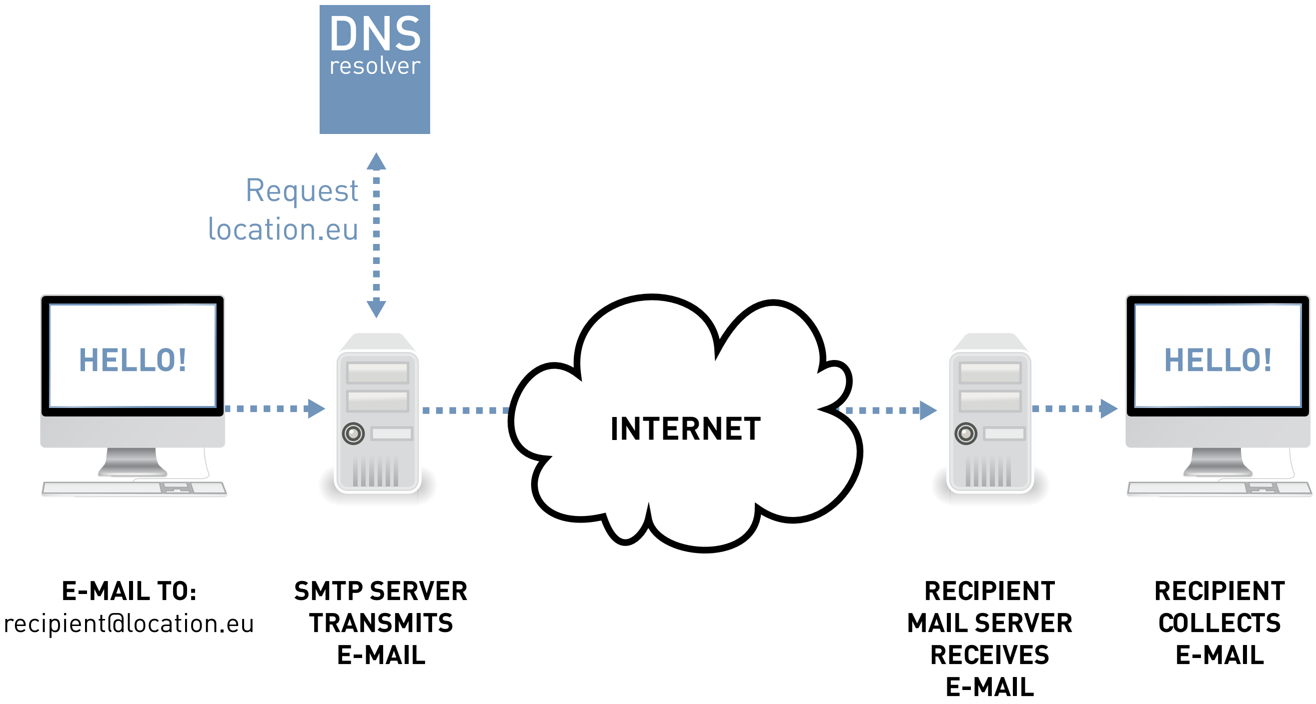
In addition to HTTP, there is also a secure variant called HTTPS. HTTP connections (and, therefore, uploaded and downloaded information) are not encrypted, and anyone with access to the network cables or equipment between the computer of the end-user and the web server can gain access to all information going back and forth.

HTTPS adds encryption to this connection, so that (in theory) only the end-user and the web server can decipher the information that is going back-and-forth. This is based on trust: the web page publisher asks a trusted party to give them a strictly personal certificate, digitally signed to confirm the identity of the publisher; much like a wax seal used in previous centuries to seal documents.

When a user buys a new computer or installs a new web browser, it comes with a standard set of trusted certificate authorities, a secure list of entities from which the user will trust the certificates given out to web page publishers. The weakness in this system is a result of this default list: there are dozens on this list. If just one of these entities turns out not to be trustworthy, users will be putting their trust in an unreliable service.

E-MAIL AND E-MAIL SECURITY

MAIL IN THE DIGITAL WORLD



Electronic mails, or e-mails, are messages sent by one sender to one or more recipients. The transfer of these messages is handled using SMTP (Simple Mail Transfer Protocol) which, like HTTP, is also built on the Internet Protocol.

After composing an e-mail on a webmail site or in an e-mail program, it is transferred to an outgoing e-mail server using SMTP. It will then be transferred from one e-mail server to another, again using SMTP, until it reaches its final destination mail server.

E-mail servers figure out where to send the e-mails by querying the earlier described Domain Name System (DNS) information. This system also includes information about which servers are responsible for handling emails for each domain. The domain can be extracted from the part of the recipient's email address that comes after the @-sign.

Once the message arrives at the e-mail server that handles all e-mails for the recipient, it will remain there until the recipient deletes it. Some e-mail software will do this automatically as messages are downloaded to the user's PC or smartphone.

E-mail security E-mails can be intercepted by third parties as they are being sent from one e-mail server to another. There are two ways to prevent this from happening: secure the communication between the e-mail servers, or encrypt the contents of the e-mails. Securing the communication between e-mail servers happens in the same way as the HTTPS protocol secures HTTP communication (described above).

A weakness in the case of e-mail is that your computer does not communicate directly with the final destination e-mail server. As a result, if one single intermediate e-mail server does not use encryption to send on your message, it could still be intercepted at that point.

Because of this weakness, it may be a better idea to encrypt the message itself. A popular and freely available encryption method for e-mail is PGP (Pretty Good Privacy), also available as OpenPGP and GPG.

DEEP PACKET INSPECTION

TAKING A LOOK AT YOUR INTERNET TRAFFIC

Data on the Internet is sent in "packets", which are basically small blocks of data. Each packet has a header that describes its origin and destination (like an envelope with a sender and recipient address). This information allows the network equipment to determine the best path to send a packet at given moment.

Historically, network equipment only looked at origin and destination information. But with rapid increase of malicious activity network owners decided that they need to look at more details of each packet to distinguish "safe" packets from those being part of hacking or denial of service attacks.

For example, network security programs ("firewalls") could initially only block a packet travelling from a specific origin, to a specific destination and to a specific service. Using these criteria you could block all incoming service requests to your office's network, because you make no services available for general public. And you could still enjoy all other services available on Internet by allowing service requests originating from your office network.

At some point you might decide to start a web server at your network to publish documents. You would need to modify your firewall settings to allow incoming service request, but only for the web service. But then, there are numerous attacks against web servers that look quite innocent from firewall's point of view. It is impossible to distinguish legitimate packets from malicious ones based just on origin and destination details.

Network engineers soon realised that it would be easier to detect attacks if the network equipment started looking a bit deeper into the packets. In theory it is easy – the headers in packet are not "separated" in any other way than logical definition of boundaries. It's just a matter of analysing a few next bytes than we were analysing so far e.g. for routing purposes. Or go even deeper and look inside the block of data in the packet.

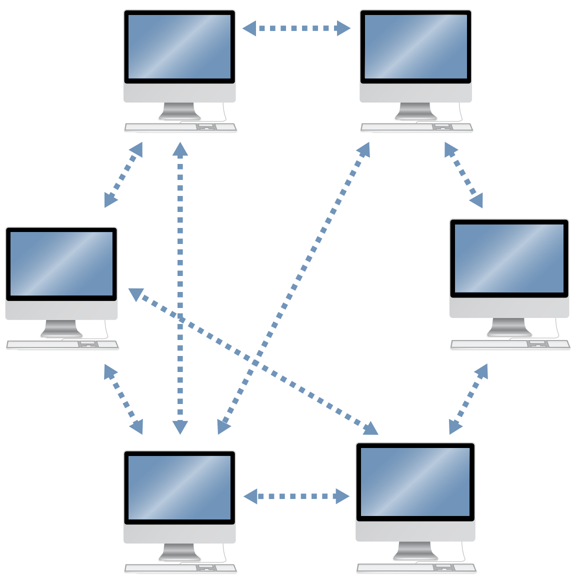
Devices that started doing that were initially called Intrusion Prevention Systems (IPS) and soon these features were introduced into most network equipment. When it was used to block hacking attacks, this caused no controversy.

However, over time, governments, content providers and network operators started to realise that the technique – in general use called deep packet inspection (DPI) – gives them much more control over the network users' data than it was possible before. DPI techniques are already in use for law enforcement (surveillance, blocking, etc), market profiling, and advertisement targeting, service level agreement enforcement and is being proposed for copyright enforcement.

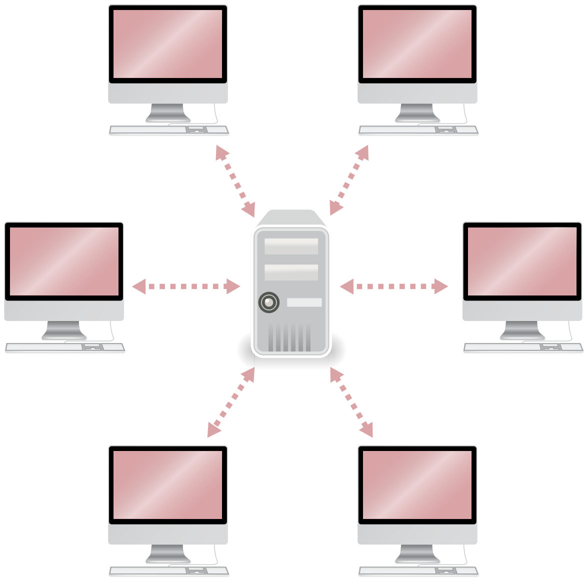
From a user's point of view DPI techniques can be blocked by using encryption – the "deep" contents of an encrypted packet is completely opaque to the operator.

PEER-TO-PEER

FROM ME TO YOU, WITH NO ONE IN THE MIDDLE



PEER TO PEER
SYSTEM OF NODES WITHOUT A CENTRAL INFRASTRUCTURE



CENTRALIZED
SERVER-BASED SERVICE MODEL (NOT PEER-TO-PEER)

Peer-to-peer networks consist of devices (web servers or end user computers) that participate on equal terms in a type of communication. Each "peer" (i.e. each device) can communicate with other peers and there is no distinction between consumers and producers, clients and servers, etc. It is simply many devices communicating with many devices.

This is in contrast to the client-server or one-to-many model where one computer serves requests of many clients – a website providing content to many website users, for example (one device communicating with many devices).

On the Internet, peer-to-peer applications use peer-to-peer protocols that are based on the IP-protocol.

Peer-to-peer networks have a series of particular advantages:

- They have no single point of failure because there are no centralised entities. In a one-to-many network, if the "one" fails, the system fails. In a "many-to-many" network, if one fails, there is minimal overall damage;

- They can grow easily because each additional participant adds extra resources (traffic capacity, storage, computing power) to the network;
- There is no administration because there is no central authority;
- Faults have minimal impact because there are no centralised resources and there is a naturally high level of duplication of resources;
- They grant freedom to their users. Not only are the participating devices equals, the participating users are also on equal footing.

One of the important tasks of a peer-to-peer application is to organise the network and locate resources in the network.

To a certain extent, e-mail servers are an early example of peer-to-peer applications. Using the SMTP protocol, any server can send an email to any other server. The Domain Name System can also list multiple servers that are capable of handling incoming e-mail for a particular domain, increasing the reliability of the system.

Peers in file sharing networks do not immediately know the IP addresses of other peers participating in the network and they do not know which peers have which files (or parts of these files). This is typically handled by a process in which participating peers share information about other peers regarding the content that they have. Files are identified using "hash" keys, which are basically fingerprints that allow individual files to be uniquely identified. Distributed Hash Tables (DHTs) allow "peers" to discover which other peers are available to download all or part of a particular file.

Users of the peer-to-peer network need a way to obtain hash fingerprints for the files they want to obtain. Some are published on websites, e.g. to download versions of the Ubuntu operating system, for example. There are dictionaries that map human readable descriptions of files to hash fingerprints so that it is possible to search for files in the peer-to-peer network.

Websites such as thepiratebay.org and mininova.org provide such dictionaries. However, fingerprints can also be distributed through e-mail, chat and social networks – meaning that there is no centralised system.

There are also peer-to-peer networks that provide anonymity to participating peers.

BEHAVIOURAL ADVERTISING

LET'S GET PERSONAL

Behavioural advertising (also called 'behavioural targeting') is a technique based on tracking the activities of users on the Internet. It is used to build profiles of Internet users in order to display advertising which, if the profile is correct, will be more relevant to them and, as a result, will be more effective.

Behavioural advertising uses an easy to understand principle: if a user first visits a web site on e.g. football, a little file (a so-called cookie) will be stored in their web browser (such as Internet Explorer, Firefox or Chrome). A web site usually consists of content from several sources, for example the text and pictures come from the site you entered in your browser, but additional content such as advertisements is downloaded from other sources (even sources unrelated to the website itself). Every time content is loaded, the request might also send cookie data back from your computer.

For behavioural advertising, cookies usually include an identification number. If the user then reads a news article on cars, the behavioural advertising companies will be able to make assumptions about somebody who reads articles about both cars and football. In our example, a primitive assumption might be made that the user is someone who would react favourably to beer advertising. The assumption might also be made that it is not a good idea to show special offers on car insurance to the user, because it is probably a young man.

The more websites the user visits that are part of the tracking network of the behavioural advertising services, like most newspaper web sites and many others, the more data is collected on their profile. Within a relatively short period of time of reading somebody's online habits, a very detailed profile can be developed — and the "identifiability" of the data grows, even though in theory it is "anonymous".

Large amounts of behavioural data can reduce the size of the group that an individual belongs to a very small number of individuals that might fit to this pattern. Several years ago, one search engine published a large set of "anonymous" data on searches done thorough its service. As a result of analysing this “anonymous” data, journalists were able to identify individuals, demonstrating that “anonymous” data is not anonymous after all.

Whether additional data from other sources is also used for behavioural advertising is not known. Many companies that are active in the behavioural targeting business, such as Google and Yahoo!, provide other online services as well, including search. The merging of databases would create vast amounts of comparatively easily identifiable personal data.

Behavioural advertising is claimed to be one of the drivers behind the online advertisement industry’s economic success over the past years. The technique is also used on an experimental basis for delivering other content, such as news to Internet users.

Users are not prompted for their consent for this processing of their personal data. The advertisement business argues that this kind of tracking is in the interest of the user, because this helps to ensure that they only receive ‘relevant’ advertisement. They also propose an opt-out-procedure that is claimed by some to fulfil the requirements of the e-Privacy directive.

The key issue in question is, whether the cookies settings (that are rarely set to “privacy by default”) in the user’s browser already constitute a meaningful expression of consent by the user. The European Data Protection Supervisor[03] says that it is not. Many Internet users neither know about cookies nor ever change their cookie acceptance settings. Technically the proposed solution also faces difficulties, since the opt-out regime does not include all advertisers. Furthermore, the current “opt-out” system itself uses cookies, so deleting cookies also deletes the opt-out.

Additionally, modern browsers and browser extensions (so-called plug-”ins”, such as Flash) offer many more ways to store and retrieve data in addition to the traditional cookies. This additional data is hard to manage for the average user and not always covered by cookie preferences in browsers.

Currently European citizens have a European law to protect them, but remain de facto unprotected due to a lack of will to implement the law.

[03] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf

THE SEARCH ENGINE

AN INDEX OF THE INTERNET

Navigation on the World Wide Web works through hyperlinks (text or images which, when clicked on, will cause another website to be opened).

Any Web author can link to any other online content. Through the practice of linking all Internet users help with organising the information online into a Web of interconnected resources.

Importantly, the Web does not provide for a centralised index that keeps track of what is available on the network. Search engines are therefore the most important services to help meet the need of Internet users to navigate the Internet more effectively.

There are different kinds of search engine services. The most important search engine model is the crawler-based search engine.

This uses software (referred to as "crawlers" or "spiders") to look for what is available online and systematically indexes this content. The sophistication and effectiveness of the crawler determines the size and the freshness of the index, which are both important measures of a search engine's quality. In simple terms, the spider/crawler follows every link on every page, indexes the linked pages and then follows the links on those pages, indexes them, and so on.

The most important operation the search engine performs is making the match between a user's search query and the information in the index. Typically, the output of this matching process is a ranked list of references . These hits normally consist of a title, snippets of information and hyperlinks to the pages that the search engine's technology has determined as possibly relevant.

Alongside the 'organic results' (i.e. the pages found by the search engine), commercial search engines place sponsored results determined by a bidding process on keywords by marketeers. The matching process for organic results is complex and commercial search engines protect their precise ranking algorithms as trade secrets. The PageRank algorithm of Google is one of the most famous Web search ranking algorithms. It predicts the relevance of websites in the index by analysing the linking structure on the Web (i.e. the types of pages that link to that page).

Other important techniques for better

matching the user's information needs with the index include the analysis of the content of the websites and the analysis of user data. Commercial search engines use cookies to store users' search queries, clicks on the links and more in individualised form in their databases for long periods of time.

A "vertical" or specialised search engine focuses on search for a specific type of subject, such as travel, shopping, academic articles, news, or music. The large crawler-based search engines include specialised search engines in their service as extra features. A "meta-search engine" is a search engine that does not produce its own index and search results, but instead uses the results from one or more other search engines. A "directory" is a repository of links classified into different categories. The Yahoo! directory and the Open Directory Project are famous examples.

CLOUD COMPUTING

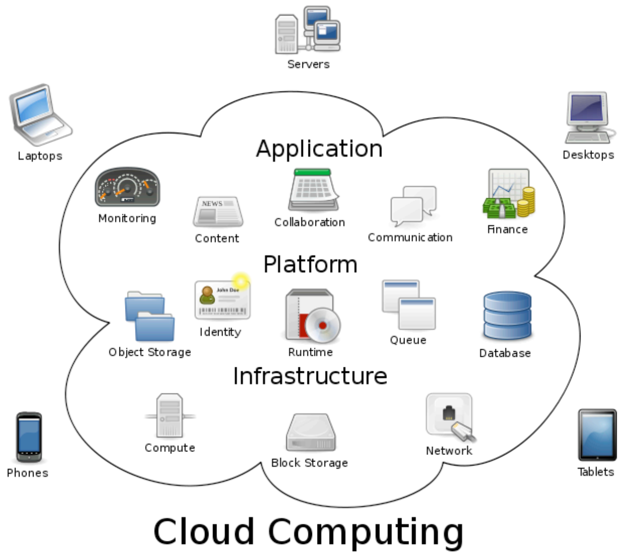
THE INTERNET BECOMES YOUR COMPUTER

Cloud computing has become a marketing "buzz-word" recently. The concept itself is far from new, although there has recently been a huge increase in applications made available.

In diagrams representing a communications network, a cloud is used to demonstrate the network that is outside the network of a user. Cloud computing, therefore refers to any computing service which is performed inside the network rather than inside the end-user's computer.

One of the first examples of cloud computing is web-based e-mail ("webmail"). Users of webmail can access their e-mail from any Internet-connected device, rather than on just one machine. Common webmail services include Yahoo! Mail, Hotmail and Gmail.

With ever-increasing Internet connection speeds, the range of services which can be offered by cloud computing services has grown exponentially in recent years. Now, for example, it is possible to store vast amounts of data in the "cloud" using virtual hard disks, such as the one provided by Microsoft Live.



Similarly, online office softwares such as word processing and database technologies are increasingly being offered.

Google's Chrome Operating System project is a further step in the move towards cloud-based computing. Using the Google Chrome web browser as its base, it aims to automatically incorporate cloud technologies by default, meaning that the amount of software used on the computer is minimal, with a heavy reliance on services available online – in many ways opposite to the approach used in traditional computing, where almost all software is built into the computer with little or no reliance on software in the cloud.

SOCIAL MEDIA

WHERE WE MEET

Social media are a set of online communication tools that allow the creation and exchange of user generated content.

Social media are fundamentally different from regular media as they do not just give information, but interact with you while giving you that information. The interaction can be as simple as asking for your comments, letting you vote on an article or "like" or "unlike" any action of other users. Each user is not just a spectator but part of the media, as other users can also read their comments or reviews.

People are getting used to having the ability to react to what others write and to express and show their own point of view. This enlarges the community involvement in ongoing debates. Every year the number of social media users is increasing, so its influence is increasing and is becoming more and more powerful.

Any website that invites visitors to interact with the site and with other visitors can be considered as part of social media. They can be divided broadly into six different types:

1. Collaborative projects (e.g. Wikipedia), where users interact by adding articles and editing existing articles;
2. Blogs and microblogs (e.g. Twitter);
3. Content communities (e.g. YouTube, Flickr), where users interact by sharing and commenting on photos or videos;
4. Social networking sites (e.g. Facebook, Myspace, Hi5, google+), where users interact by adding friends, commenting on profiles, joining groups and having discussions;
5. Virtual game worlds (e.g. World of Warcraft);
6. Virtual social world (e.g. Second Life).

Protection, in particular privacy protection, of social media users is an important topic. While users can usually choose to share personal information or hide it, the default settings and additional protection for children are subjects of considerable controversy. Furthermore, certain sites, such as Facebook, have unilaterally changed their users' privacy settings already several times in the past.

INTERNET GOVERNANCE

The first attempts to define the term Internet Governance (IG) were made during the preparatory meetings for the United Nations World Summit on the Information Society.

A first common-accepted definition was developed within the Working Group on Internet Governance, a multi-stakeholder group created by the UN Secretary General and was included in the Tunis Agenda for Information Society:

"development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."

This definition emphasises the multi-stakeholder approach in discussing Internet-related policies: the participation of all actors, in an open, transparent and accountable manner.

To achieve this goal, the Internet Governance Forum was created as a multi-stakeholder forum for discussions of public policy issues related to key elements of Internet Governance. The forum, which already had 6 editions (between 2006 and 2011) triggered the organisation of similar national and regional fora (e.g EuroDIG –the pan-European dialogue on Internet governance). It is important to outline that these fora do not function as decision-making bodies, but they influence policies.

What does IG cover?

- Infrastructure and standardisation;
- Technical issues related to the running of the Internet: telecommunications infrastructure, Internet standards and services (e.g. Internet Protocol, Domain Name System), content and application standards (e.g. HyperText Markup Language);
- Issues related to safeguarding the secure and stable operation of the Internet: cybersecurity, encryption, spam;
- Legal issues: national and international legislation and regulations applicable to Internet-related issues (e.g. copyright, cybercrime, privacy and data protection);
- Economic issues: e-commerce, taxation, electronic signatures, e-payments;

- Development issues: the digital divide, universal access to Internet;

- Socio-cultural issues: human rights (freedom of expression, the right to seek, receive and impart information), content policy, privacy and data protection, multilingualism and cultural diversity, education, child safety online.

Who participates in IG?

- Governments: they elaborate and implement Internet-related public policies and regulations;

- Private sector: Internet service providers (ISPs), network providers, registries and registrars for domain names, software companies, content companies;

- Civil society: non-governmental organisations representing Internet end-users;

- International organisations: International Telecommunication Union, UN Educational, Scientific and Cultural Organisation, United Nations Development Programme;

- Technical community: Internet Society, Internet Engineering Task Force, Internet Architecture Board, Internet Corporation for Assigned Names and Numbers.

More info:

Jovan Kurbalija, An Introduction to Internet Governance, Diplo Foundation, 2010

Last modified on: 23 January 2012 13:39

EUROPEAN
DIGITAL
RIGHTS

EDRI.ORG/PAPERS

With financial support
from the EU's
Fundamental Rights and
Citizenship Programme.