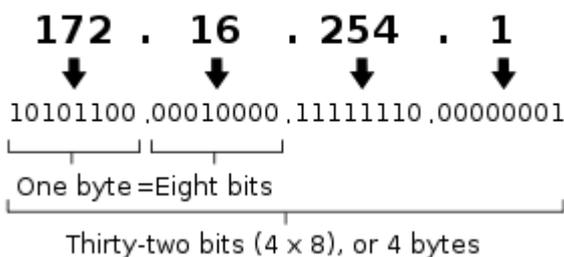**ZAK** ZAFAR ALI KHAN

Topic: 1.2.2 IP addressing

An IP address (Internet Protocol Address) is an exclusive number that all IT devices (printers, routers, modems, etc.) use which identifies and allows them the ability to communicate with each other on a computer network.

Take for example, if you are ordering pizza by home delivery, then you need to tell the delivery man your exact home address. Similarly, to print a document, you must know the IP address of your printer on your network.

The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the depletion of vacant addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995. IPv6 and its deployment has been ongoing since the mid-2000s.

IP addresses are binary numbers, but they are usually stored in text files and displayed in human-readable notations, such as 172.16.254.1 (for IPv4), and 2001:db8:0:1234:0:567:8:1 (for IPv6).

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1

10101100 .00010000 .11111110 .00000001

One byte = Eight bits

Thirty-two bits (4 × 8), or 4 bytes

In IPv4 an address consists of 32 bits which limits the address space to 4,294,967,296 (232) possible unique addresses. IPv4 reserves some addresses for special purposes such as private networks (~18 million addresses)

IPv4 addresses are canonically represented in dot-decimal notation, which consists of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1. Each part represents a group of 8 bits (octet) of the address. In some cases of technical writing, IPv4 addresses may be presented in various hexadecimal, octal, or binary representations.

Topic: 1.2.2 IP addressing

What are Public IP Addresses?

A public IP address is assigned to every computer that connects to the Internet, where each IP is unique. In this case, there cannot exist two computers with the same public IP address all over the Internet. This addressing scheme makes it possible for the computers to "find each other" online and exchange information. Users have no control over the IP address (public) that is assigned to the computer. The public IP address is assigned to the computer by the Internet Service Provider as soon as the computer is connected to the Internet gateway.

A public IP address can be either **static** or **dynamic**. A static public IP address does not change and is used primarily for hosting web pages or services on the Internet. On the other hand, a dynamic public IP address is chosen from a pool of available addresses and changes each time one connects to the Internet.

Most Internet users will only have a dynamic IP assigned to their computer which goes off when the computer is disconnected from the Internet. Thus when it is re-connected it gets a new IP.
You can check your public IP address by visiting www.whatismyip.com

What are Private IP Addresses?

An IP address is considered **private** if the IP number falls within one of the IP address ranges reserved for private networks such as a Local Area Network (LAN). The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks (local networks):

10.0.0.0 – 10.255.255.255 (Total Addresses: 16,777,216)

172.16.0.0 – 172.31.255.255 (Total Addresses: 1,048,576)

192.168.0.0 – 192.168.255.255 (Total Addresses: 65,536)

Private IP addresses are used for numbering the computers in a private network including home, school and business LANs in airports and hotels which makes it possible for the computers in the network to communicate with each other.

Say for example, if a network X consists of 10 computers, each of them can be given an IP starting from 192.168.1.1 to 192.168.1.10. Unlike the public IP, the administrator of the private network is free to assign an IP address of his own choice (provided the IP number falls in the private IP address range as mentioned above).

Topic: 1.2.2 IP addressing

Devices with private IP addresses cannot connect directly to the Internet. Likewise, computers outside the local network cannot connect directly to a device with a private IP. It is possible to interconnect two private networks with the help of a router.

If the private network is connected to the Internet (through an Internet connection via ISP), then each computer will have a private IP as well as a public IP. Private IP is used for communication within the network whereas the public IP is used for communication over the Internet. Most Internet users with a DSL connection will have both a private as well as a public IP.

You can know your private IP by typing `ipconfig` command in the command prompt. The number that you see against "IPV4 Address:" is your private IP which in most cases will be192.168.1.1 or 192.168.1.2. Unlike the public IP, private IP addresses are always static in nature.

Explain how a Uniform Resource Locator (URL) is used to locate a resource on the World Wide Web (WWW) and the role of the Domain Name Service

Every file on the Web has a URL (uniform resource locator). Whether it's an HTML file, a photo file, whatever, it has a URL. A file's URL is its unique address on the Web. Just as a cell phone has a unique telephone number, a file has a unique URL.
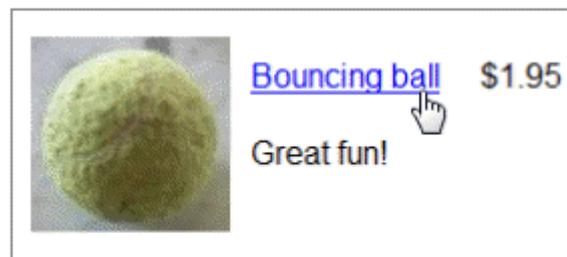
Suppose that a browser shows this:

Figure 1. Link rendered in a browser

It comes from URL `http://doomdogs.com/products/ball.html`. That's where the browser will go if the link is clicked.
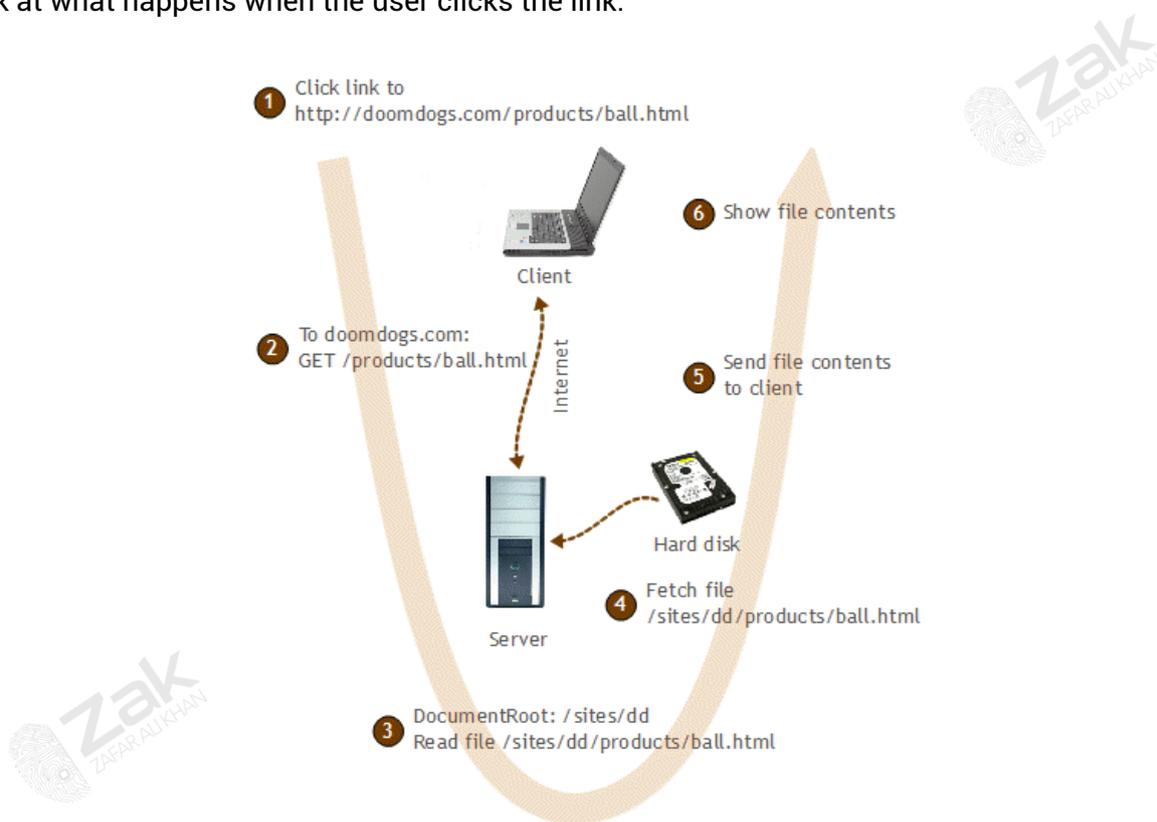
Topic: 1.2.2 IP addressing

Getting a page

A user clicks the "Bouncing ball" link. What does the browser do? The message is sent to a server. Which server? The one given in the URL of course. The URL of the desired page is `http://doomdogs.com/products/ball.html`. The part "doomdogs.com" is the domain name of the server. So that's where the message is sent: to the server at doomdogs.com. The rest of the URL "/products/ball.html" tells the server what data to return to the browser. That part of the URL matches a file on the server. A server might have 50,000 files that it can send to a browser. /products/ball.html is the particular file it should send.

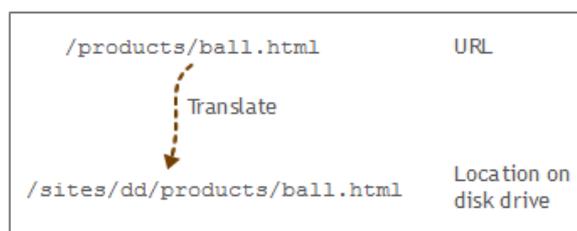Let's look at what happens when the user clicks the link.

Topic: 1.2.2 IP addressing

The user clicks on the link. The browser looks at the code that created the link. The server at doomdogs.com is a computer, with a hard disk spinning away. It runs the UNIX operating system. (Not which is to our concern) If you looked on the server's disk drive, you would see a file with the path/sites/dd/products/ball.html.

```
□ 📁 sites
   ⊞ 📁 dd
      □ 📁 products
             ball.html
```
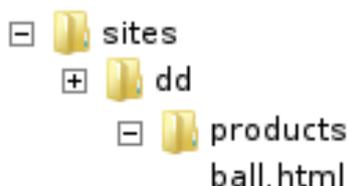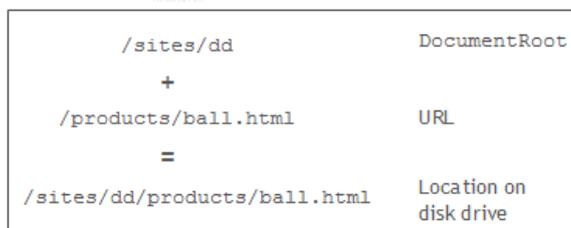
This is the file with information on the bouncing ball.

Somehow, we want the Web server to use the URL the browser sent, to fetch the right file from its disk drive. It needs to convert the URL into a file path, and then use the file path to read the file.

```
/products/ball.html              URL

        |
        Translate
        ↓

/sites/dd/products/ball.html     Location on
                                 disk drive
```

One of the settings in the file is DocumentRoot. The setting tells web server where on the computer's disk drive the files for the Web site are stored. The Web master puts all the data for the doomdogs.com Web site in the directory "/sites/dd". Then he map DocumentRoot folder to "/sites/dd", so that web server would know where to get the files.

The server takes its DocumentRoot setting "/sites/dd" and appends the URL path "/products/ball.html", giving "/sites/dd/products/ball.html."

```
/sites/dd                    DocumentRoot
    +
/products/ball.html          URL
    =
/sites/dd/products/ball.html Location on
                             disk drive
```

Now web server knows where to get the file the browser asked for. We're at step 3. Server has translated the URL to a file path on the server computer's disk drive.

Server reads the file, and sends its contents back to the browser. The browser renders the content for Jake (6). Recall that rendering is the process of making a display from code in a file. And finally the contents are displayed on the screen.

Topic: 1.2.2 IP addressing

What is a DNS server?

The Domain Name System (DNS) is a standard technology for managing public names of Web sites and other Internet domains. DNS technology allows you to type names into your Web browser like "*soundcloud.com*" and your computer to automatically find that address on the Internet. A key element of the DNS is a worldwide collection of *DNS servers.*

A **DNS server** is any computer registered to join the Domain Name System. A DNS server runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other Internet hosts.

A DNS server is similar to looking up contacts on your phone, to call a contact, you simply look up that person's name, but that name is of no use to the phone itself, it has to look up the contact number and dial that.

Simply speaking, both systems translate the website/contact name into an IP address or phone number.

DNS Root Servers

DNS servers communicate with each other using private network protocols. All DNS servers are organized in a hierarchy. At the top level of the hierarchy, so-called "*root servers*" store a complete database of Internet domain names and their corresponding IP addresses. The Internet employs 13 root servers that have become somewhat famous for their special role. Maintained by various independent agencies, the servers are aptly named A, B, C and so on up to M. Ten of these servers reside in the United States, one in Japan, one in London, UK and one in Stockholm, Sweden.

How DNS Works

The DNS is a distributed system, meaning that only the 13 root servers contain the complete database of names and addresses. All other DNS servers are installed at lower levels of the hierarchy and maintain only certain pieces of the overall database. Most lower level DNS servers are owned by businesses or Internet Service Providers (ISPs). For example, Google maintains various DNS servers around the world that manage the google.com, google.co.uk, and other domains. Your ISP also maintains DNS servers as part of your Internet connection setup.

Topic: 1.2.2 IP addressing

DNS networking is based on the client / server architecture. Your Web browser functions as a DNS client (also called *DNS resolver*) and issues requests to your Internet provider's DNS servers when navigating between Web sites.

When a DNS server receives a request not in its database (such as a geographically distant or rarely visited Web site), it temporarily transforms from a server to a DNS client. The server automatically passes that request to another DNS server or up to the next higher level in the DNS hierarchy as needed. Eventually the request arrives at a server that has the matching name and IP address in its database (all the way to the root level if necessary), and the response flows back through the chain of DNS servers to your computer.

DNS and the World Wide Web

All public Web sites run on servers connected to the Internet with public IP addresses . The Web servers at About.com, for example, have addresses like 207.241.148.80. Although people can type address information like http://207.241.148.80/ into their Web browser to visit sites, being able to use proper names like http://www.about.com/ is much more practical. The Internet utilizes DNS as a worldwide name resolution service for public Web sites. When someone types a site's name into their browser, DNS looks up the corresponding IP address for that site, the data required to make the desired network connections between Web browsers and Web servers.