Web fundamentals. Request and Response. SSL.

IT Learning &
Outsourcing Center

www.pragmatic.bg

Lector: Stefan Vadev
Skype: stefanvadev77
E-mail: stefan.vadev@gmail.com
Facebook:
https://www.facebook.com/stefan.vadev.7

Summary

- Internet, WWW, Hosts, Ports
- Clients and Servers
- Request and Response
- HTTP and HTTPS
- SSL

What is the Internet

The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

What is the Internet

What is The Internet?

Internet is a massive network of networks, a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. Information that travels over the Internet does so via a variety of languages known as protocols.

What is the Internet

Quick Points about The Internet:

It is a global network connecting millions of computers.

The Internet is decentralized.

Each Internet computer is independent.

There are a variety of ways to access the Internet.

There are more than 3,700,000,000 Internet Users in the world.

World Wide Web

The **World Wide Web**, or simply **Web**, is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet. The Web uses the HTTP protocol, only one of the languages spoken over the Internet, to transmit data. Web services, which use HTTP to allow applications to communicate in order to exchange business logic, use the the Web to share information. The Web also utilizes browsers, such as Internet Explorer or Firefox, to access Web documents called Web pages that are linked to each other via hyperlinks. Web documents also contain graphics, sounds, text and video.

World Wide Web

Quick Points about The Web:

It is a system of Internet servers that support specially formatted documents.

Documents are formatted in a markup language that supports links to other documents.

You can jump from one document to another simply by clicking on hot spots (hyperlinks).

Applications called Web browsers that make it easy to access the World Wide Web.

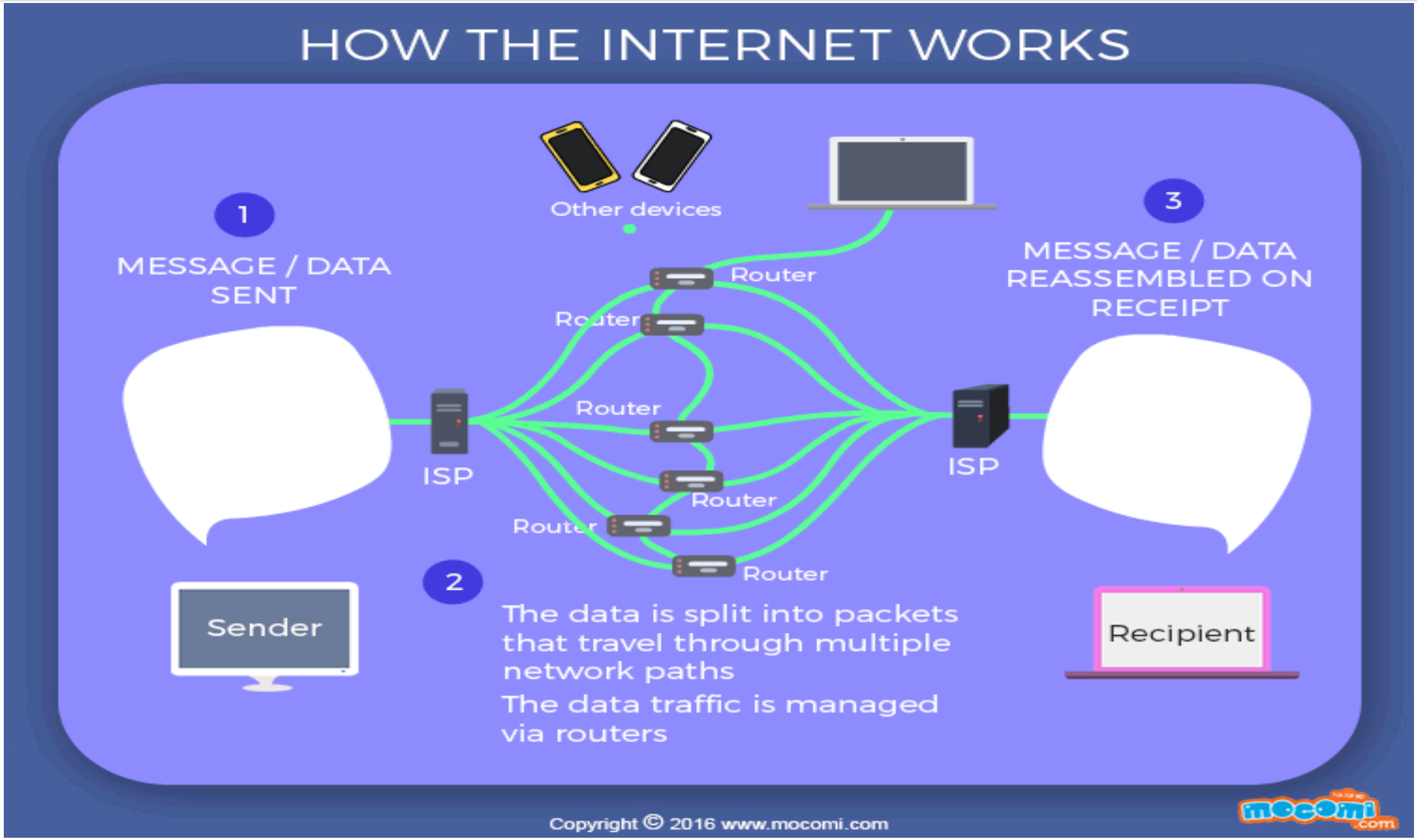
There are more than 1,275,000,000 Websites.

World Wide Web

The Web is a Portion of The Internet

The Web is just one of the ways that information can be disseminated over the Internet. The Internet, not the Web, is also used for email, which relies on SMTP, Usenet news groups, instant messaging and FTP. So the Web is just a portion of the Internet, albeit a large portion, but the two terms are not synonymous and should not be confused.

How the Internet works



HOW DOES INTERNET ACTUALLY WORK?

1

www.domainname.com

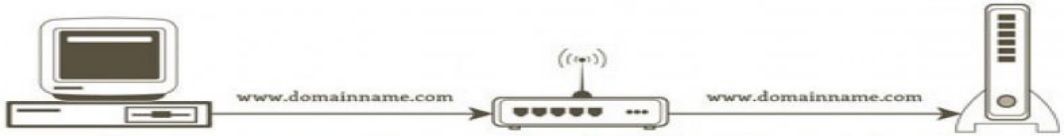
A company registers a domain with a registrar, and assigns that domain to reference a certain nameserver.

2

www.domainname.com

User types in a web address (domain) in their browser.

3



The request goes to their router (if applicable) and then to their modem.

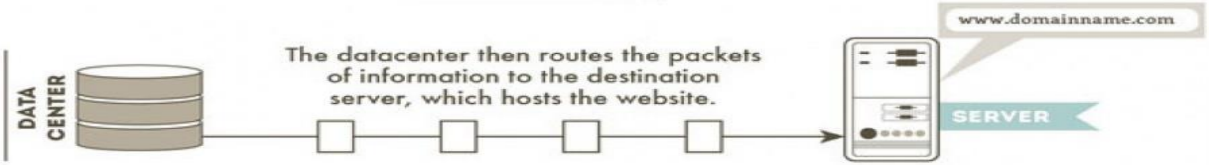
4

The modem sends the request to the user's ISP, who checks their nameservers to find out where to send the request. Some users override their ISP's name servers by using something like OpenDNS

5

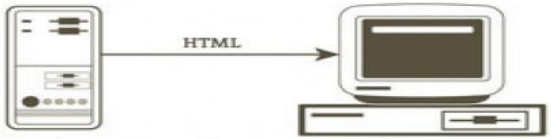
The request is then routed to another machine that is the nameserver, which identifies if the request is related to email or if it is looking for a website. If it's a website, it's routed to a datacenter.

6



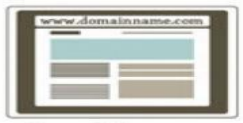
The datacenter then routes the packets of information to the destination server, which hosts the website.

7



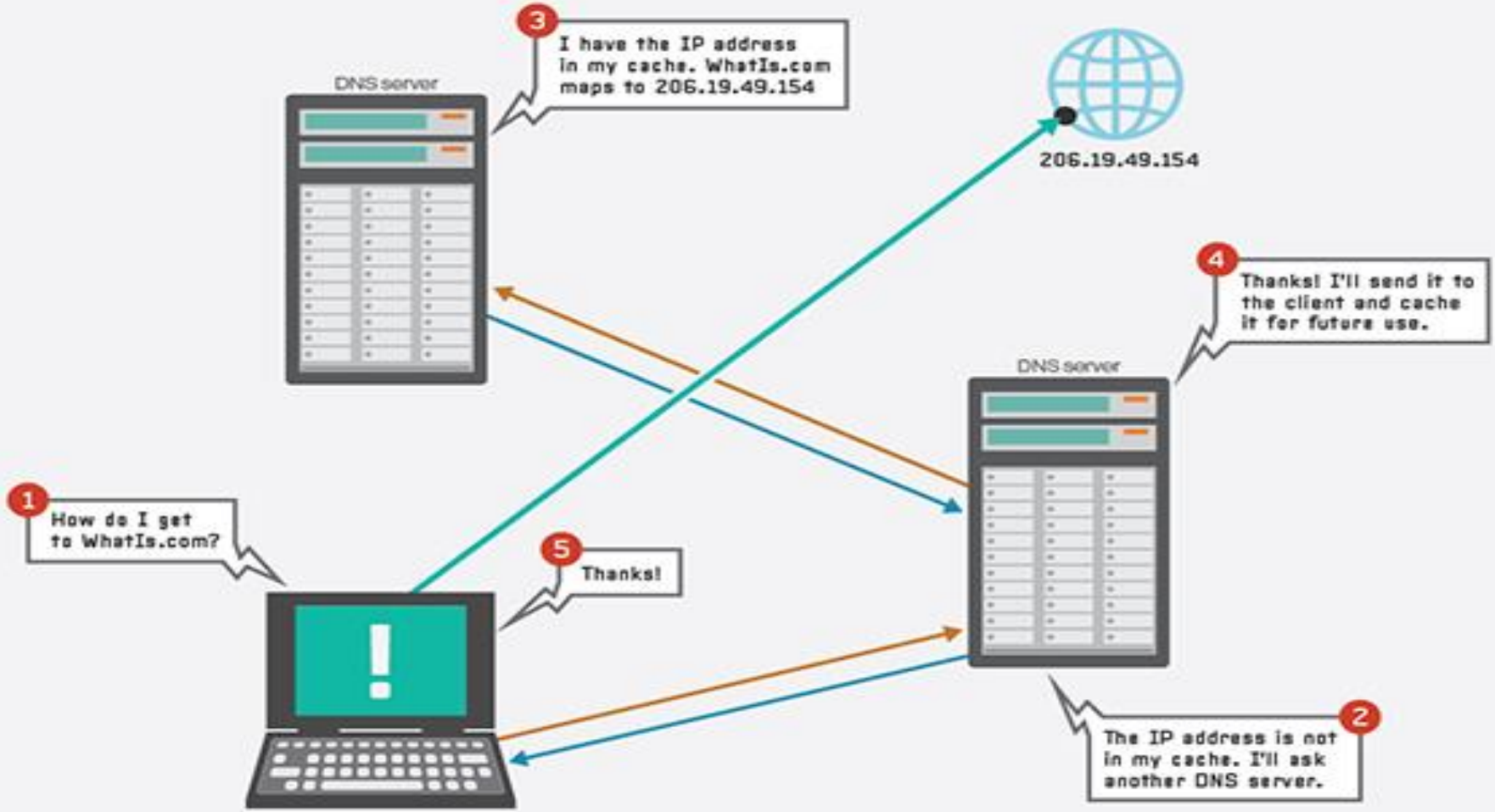
The host server then executes the request, and returns HTML code to the "client PC" (the user)

8



The user's web browser receives the information and renders the HTML as a visual web page

What is a DNS (Domain name server)?

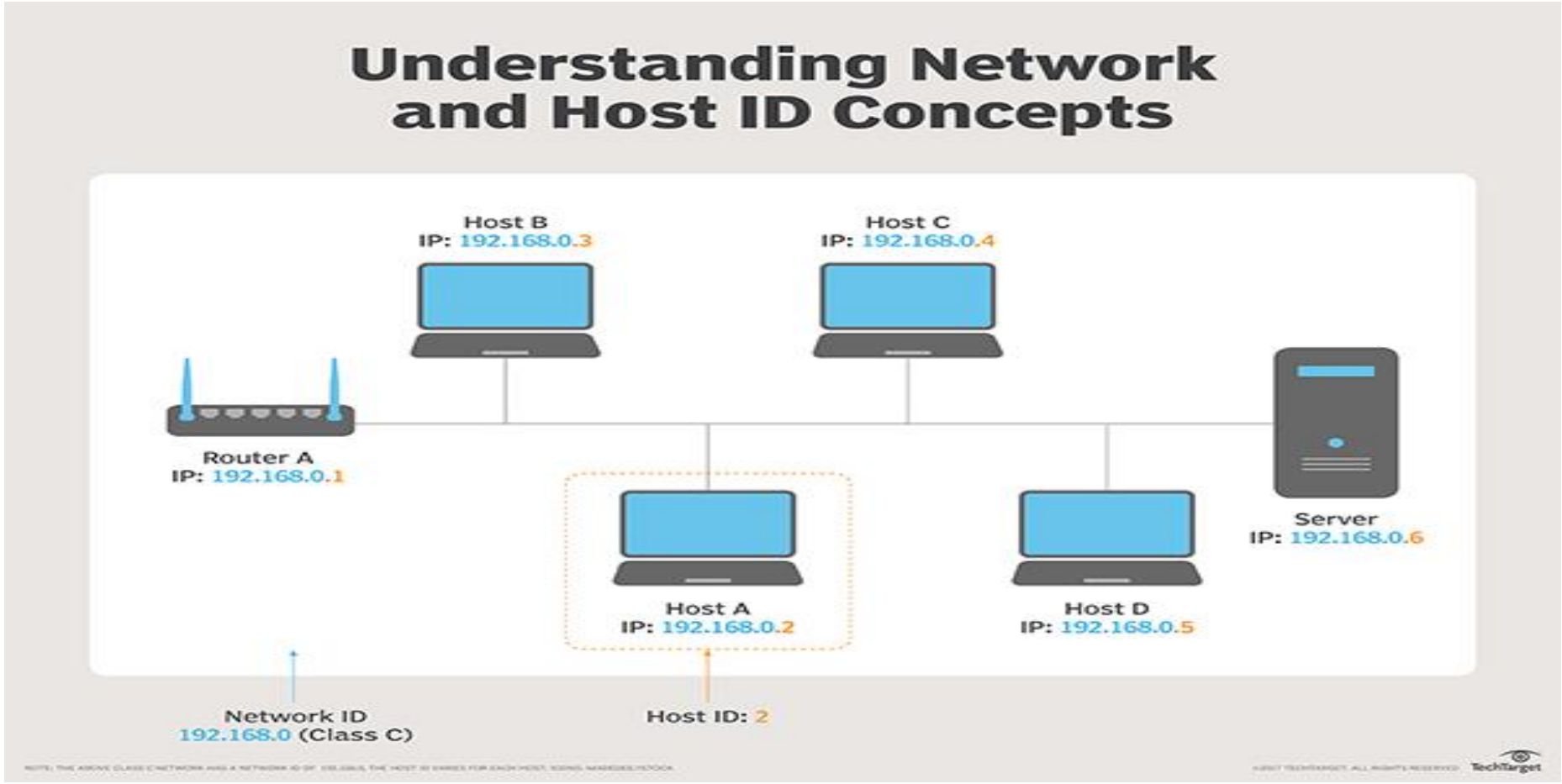


URL anatomy

https://doepud.co.uk/blog/anatomy-of-a-url

Hosts

A network host is a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network address.



Ports

In computer networking, a port is an endpoint of communication in an operating system. While the term is also used for physical devices, in software it is a logical construct that identifies a specific process or a type of network service.

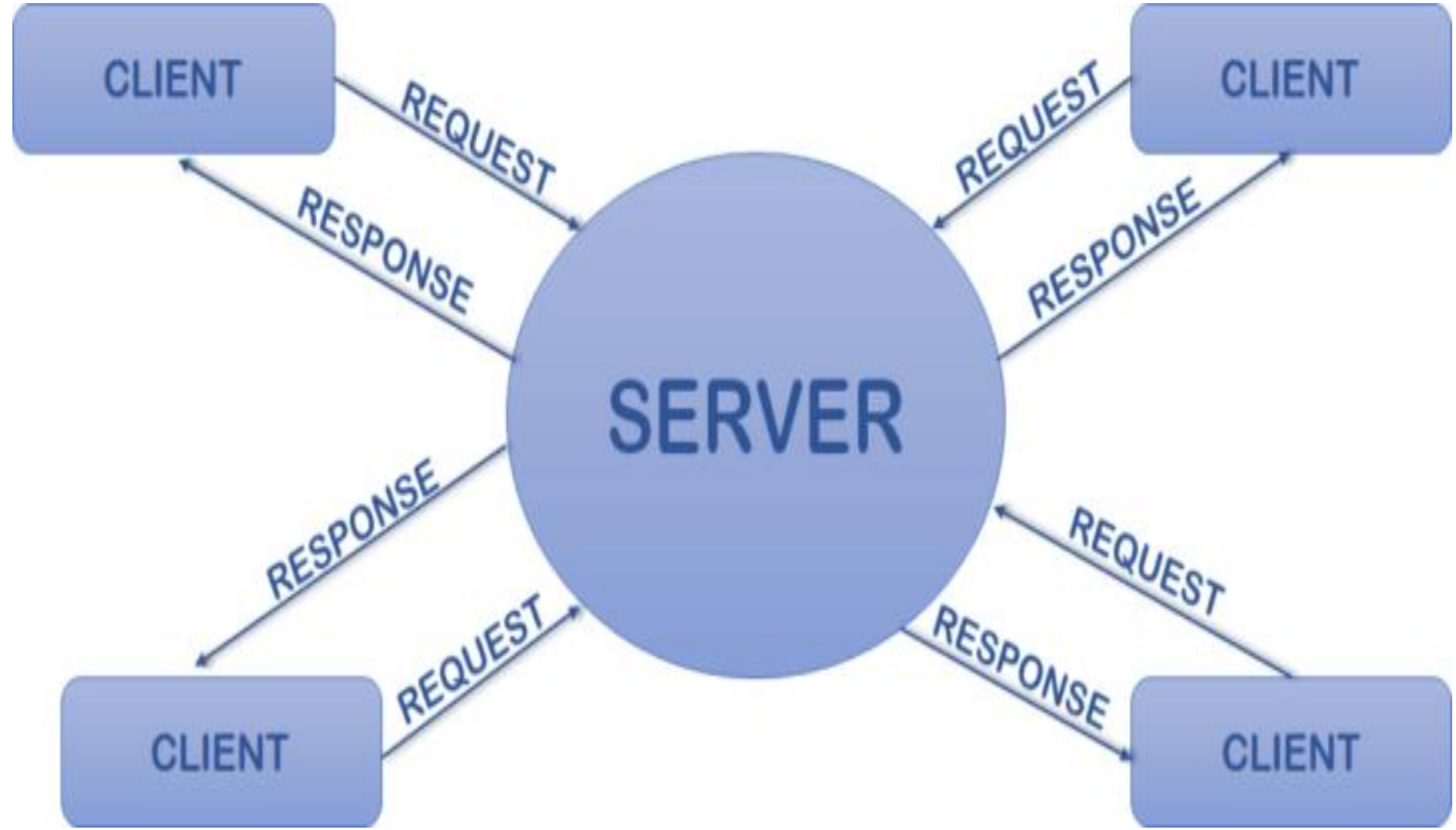
A port is always associated with an IP address of a host and the protocol type of the communication. It completes the destination or origination network address of a message. Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the port number.

Ports

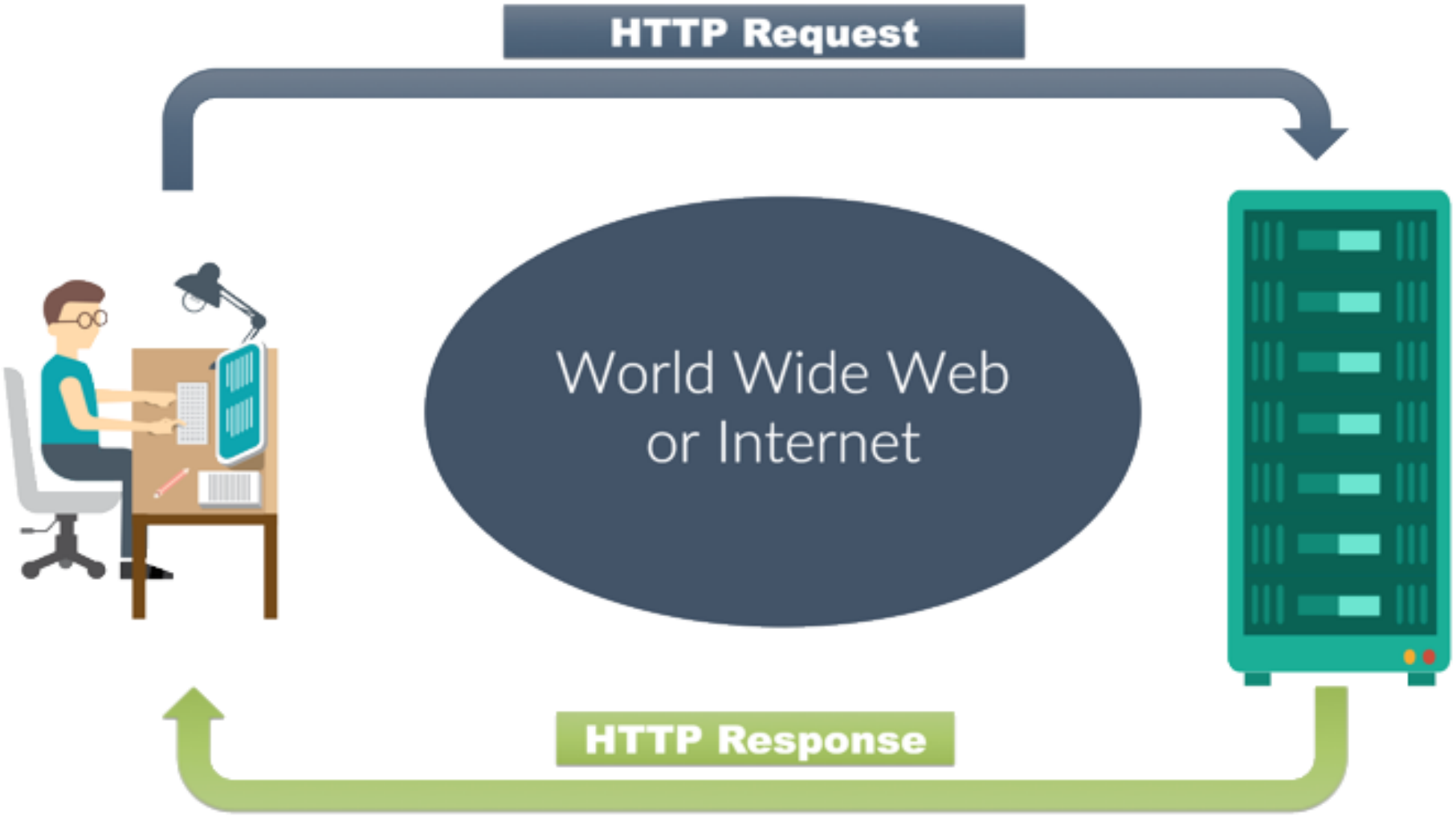
Specific port numbers are commonly reserved to identify specific services. The lowest numbered 1024 port numbers are called the well-known port numbers, and identify the historically most commonly used services. In the client–server model of application architecture, the ports that network clients connect to for service initiation provide a multiplexing service, so that multiple simultaneous communication sessions may be initiated from these ports.

After an initial service request connects to the well-known port number, the port is freed by switching the servicing of the request to a dedicated, connection-specific port number. The protocols that primarily use ports are the transport layer protocols, such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

Client and server



Request and Response



HTTP

HTTP means HyperText Transfer Protocol. HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

HTTP

HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including **Java, JavaScript** and cookies.

HTTP status codes and errors

Errors on the Internet can be quite frustrating — especially if you do not know the difference between a 404 error and a 502 error. These error messages, also called HTTP status codes are response codes given by Web servers and help identify the cause of the problem.
For example, "404 File Not Found" is a common HTTP status code. It means the Web server cannot find the file you requested. This means the webpage or other document you tried to load in your Web browser has either been moved or deleted, or you entered the wrong URL or document name.

HTTP status codes and errors

This is a list of Hypertext Transfer Protocol (HTTP) response status codes. Status codes are issued by a server in response to a client's request made to the server. It includes codes from IETF Request for Comments (RFCs), other specifications, and some additional codes used in some common applications of the Hypertext Transfer Protocol (HTTP). The first digit of the status code specifies one of five standard classes of responses.

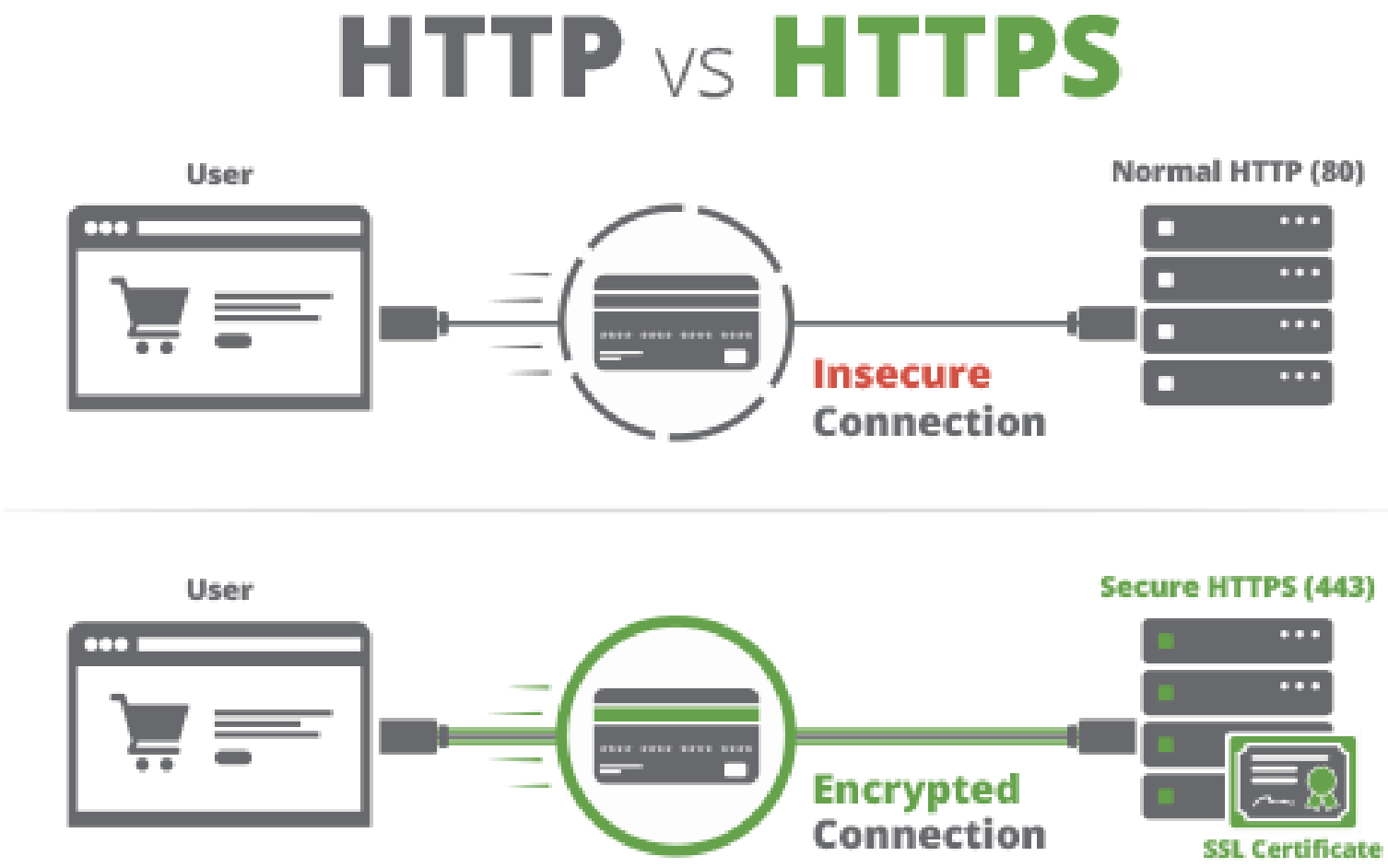
Let’s have a look at them:
https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

HTTPS

HTTPS

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for **'Secure**'. It means all communications between your browser and the website are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.

SSL Certificate



SSL Certificate

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

SSL Certificates bind together:

- A domain name, server name or hostname.
- An organizational identity (i.e. company name) and location.

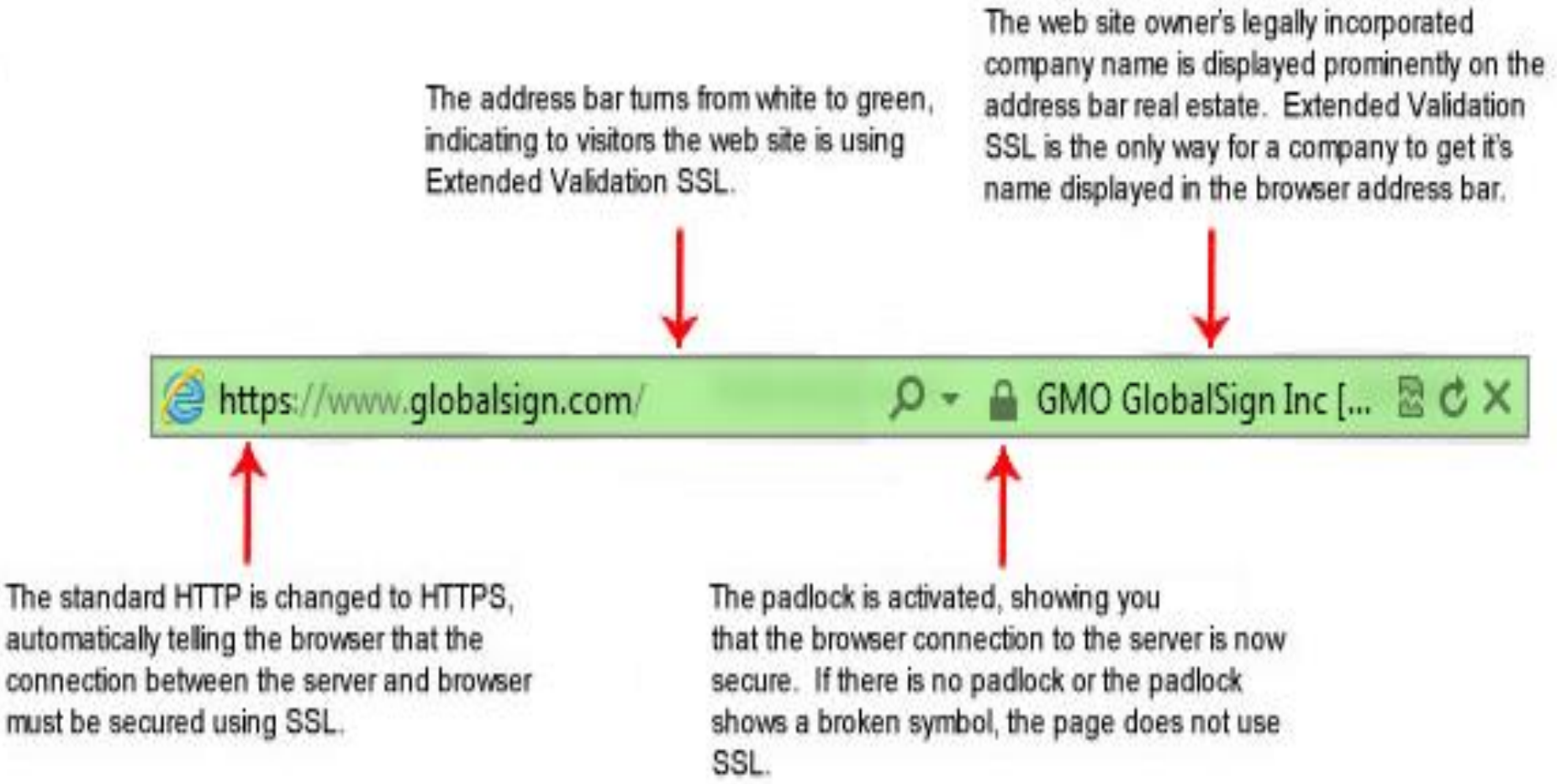
SSL Certificate

An organization needs to install the SSL Certificate onto its web server to initiate a secure session with browsers. Once a secure connection is established, all web traffic between the web server and the web browser will be secure.

When a certificate is successfully installed on your server, the application protocol (also known as HTTP) will change to HTTPs, where the ‘S’ stands for ‘secure’. Depending on the type of certificate you purchase and what browser you are surfing the internet on, a browser will show a padlock or green bar in the browser when you visit a website that has an SSL Certificate installed.

How do SSL Certificates look like?

Extended validation:



How do SSL Certificates look like?

Standard SSL certificate:

The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The padlock is activated, showing you that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

How do SSL Certificates work?

SSL Certificates use something called public key cryptography.

This particular kind of cryptography harnesses the power of two keys which are long strings of randomly generated numbers. One is called a private key and one is called a public key.A public key is known to your server and available in the public domain. It can be used to encrypt any message. If Alice is sending a message to Bob she will lock it with Bob's public key but the only way it can be decrypted is to unlock it with Bob's private key. Bob is the only one who has his private key so Bob is the only one who can use this to unlock Alice's message. If a hacker intercepts the message before Bob unlocks it, all they will get is a cryptographic code that they cannot break, even with the power of a computer.

Why do I need an SSL certificate?

SSL Certificates protect your sensitive information such as credit card information, usernames, passwords etc. It also:

- Keeps data secure between servers
- Increases your Google Rankings
- Builds/Enhances customer trust
- Improves conversion rates

Where do I buy SSL certificate?

SSL Certificates need to be issued from a trusted Certificate Authority. Browsers, operating systems, and mobile devices maintain list of trusted CA root certificates.

The Root Certificate must be present on the end user's machine in order for the Certificate to be trusted. If it is not trusted the browser will present untrusted error messages to the end user. In the case of e-commerce, such error messages result in immediate lack of confidence in the website and organizations risk losing confidence and business from the majority of consumers.

Where do I buy SSL certificate?

Companies like GlobalSign are known as trusted Certificate Authorities. This is because browser and operating system vendors such as Microsoft, Mozilla, Opera, Blackberry, Java, etc., trust that GlobalSign is a legitimate Certificate Authority and that it can be relied on to issue trustworthy SSL Certificates. The more applications, devices and browsers the Certificate Authority embeds its Root into, the better "recognition" the SSL Certificate can provide.

GlobalSign was founded in 1996 in Europe and remains one of the longest running Certificate Authorities in the region.

Summary

- Internet, WWW, Hosts, Ports
- Clients and Servers
- Request and Response
- HTTP and HTTPS
- SSL