Computer Networks and the OSI model

Agenda

- What are computer networks, and why do we care?
- What happens when you type a URL into a browser?
- What is the OSI model?

Key Terms

Network

> A group of interconnected computers

IP Address

> An Internet Protocol address (IP address) is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: network interface identification and location addressing

DNS

> A system used to identify computers. These are most commonly used to map human-friendly domain names to the numerical IP addresses computers need to locate service.

Communication Protocol

A communication protocol is a system of rules that allows two or more entities of a communications system to transmit information via any kind of variation of a physical quantity

What are networks?

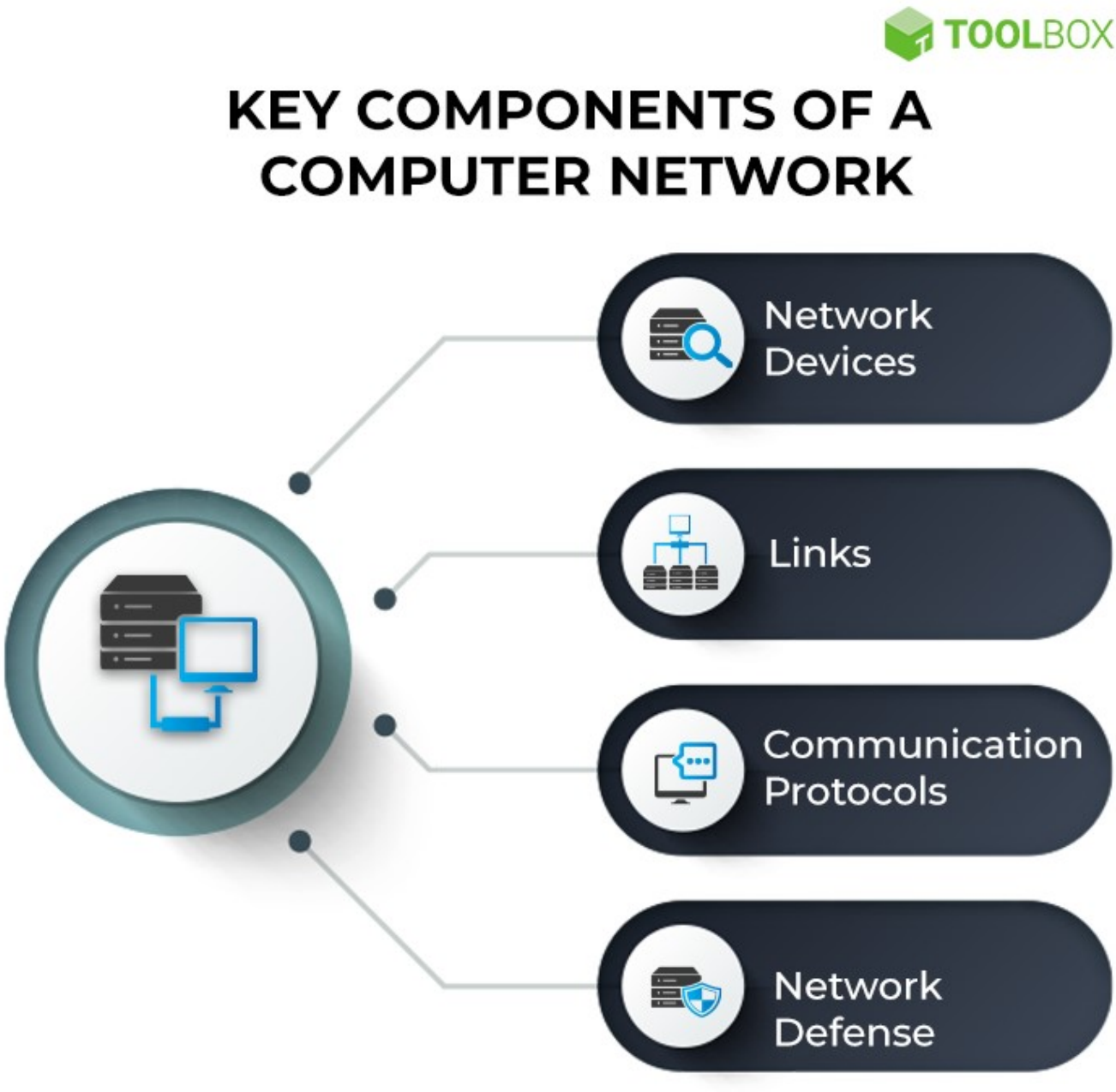
We come across a lot of networks daily in our lives.

> A group or system of interconnected people or things.

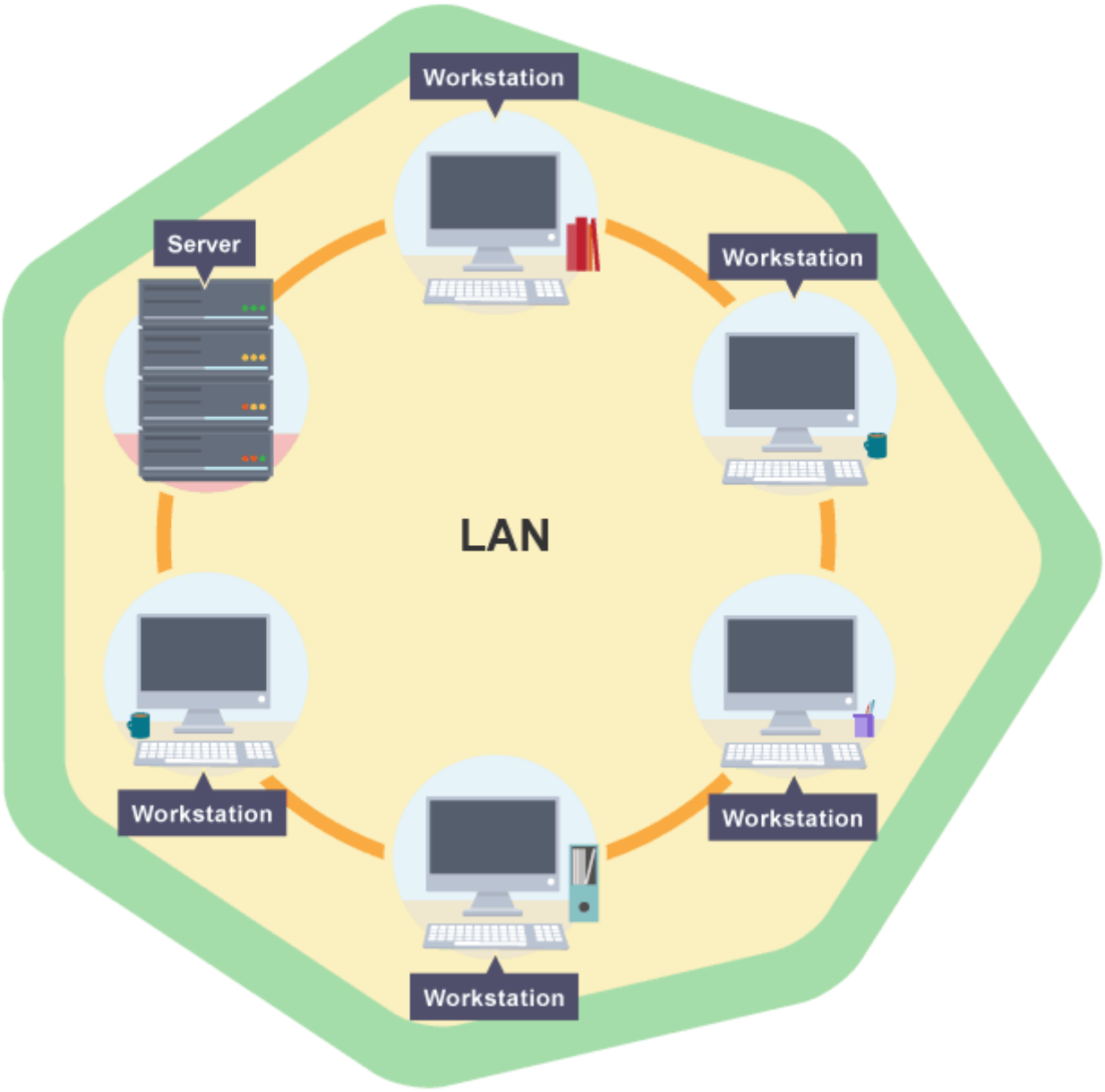
Some examples of real-world networks are:

- Social networks
- Postal networks
- Rail networks

A computer network is a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also be wireless.

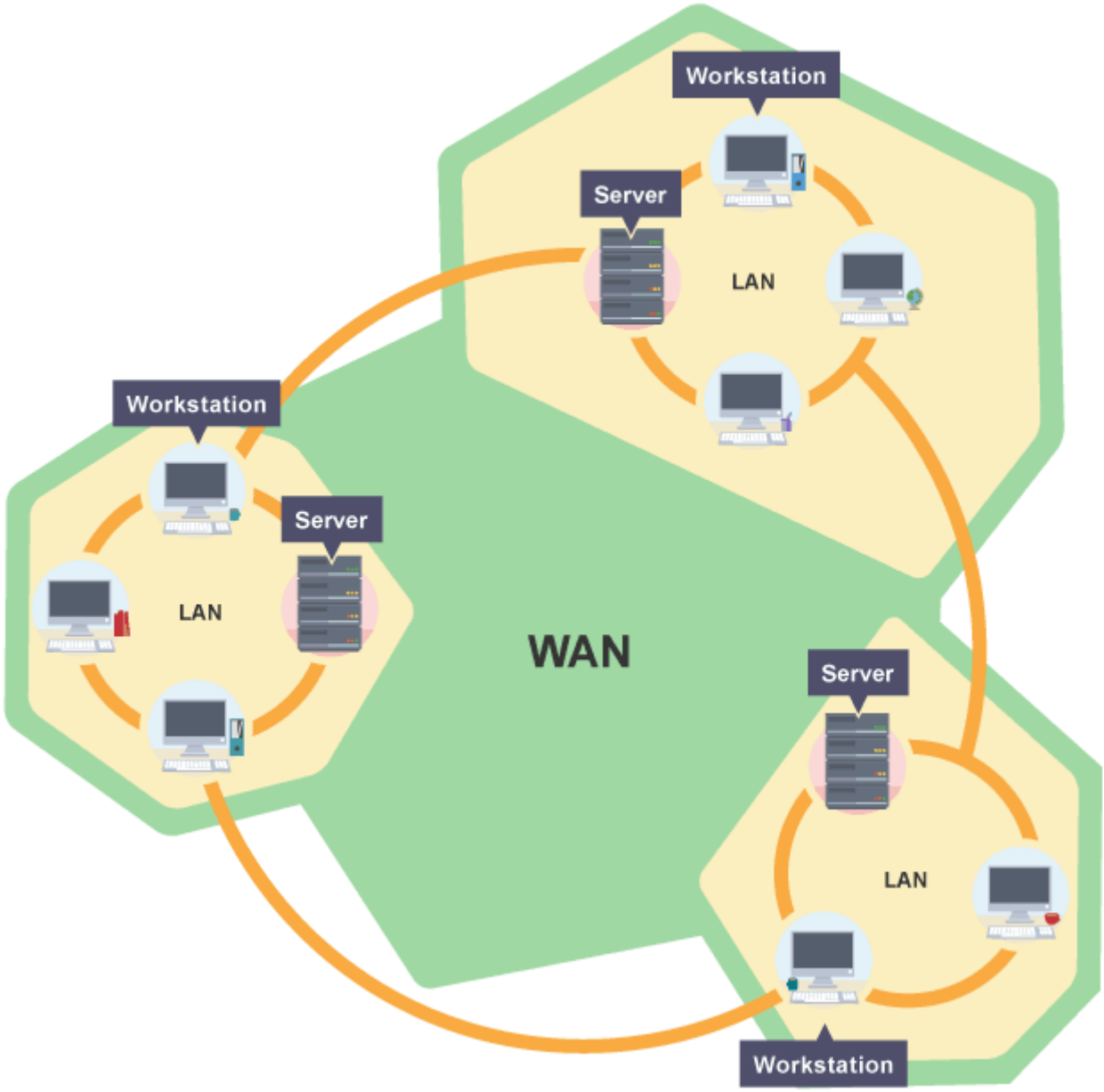

TOOLBOX
KEY COMPONENTS OF A COMPUTER NETWORK
Network Devices
Links
Communication Protocols
Network Defense

LAN



A local area network is when computers or devices are connected together over a small geographical area, such as within a home, a building or one site. A LAN can be created to share data or hardware such as a printer, or to share an internet connection

WAN

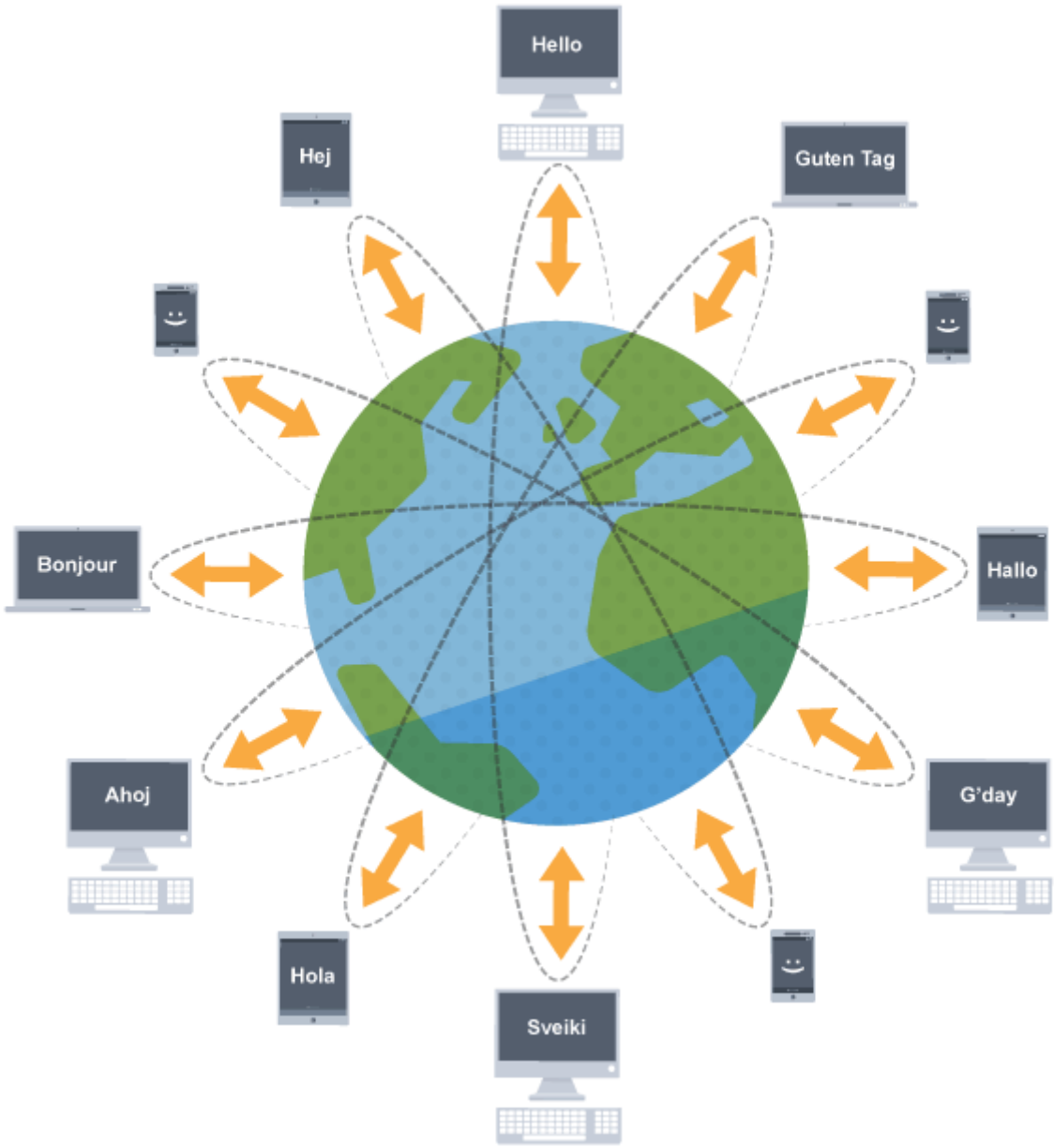


A wide area network is when computers or devices are connected together over a large geographical area. For example, a company with an office in London and another in Beijing would use a WAN to allow the employees to share one network. Some companies will connect a number of LANs in different areas together to create a WAN.

Why do we care?

Using a network allows you to share:

- hardware, such as a printer
- software, allowing multiple users to run the same programs on different computers
- data, so that other people can access shared work and you can access your data from any computer on the network



ARPANET

> The Advanced Research Projects Agency Network (ARPANET) was the first wide-area packet-switched network with distributed control and one of the first networks to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet.

Their aim was to help American military technology stay ahead of its enemies and prevent surprises, such as the launch of the satellite Sputnik 1, happening again. Among ARPA's projects was a remit to test the feasibility of a large-scale computer network.

Sending a mail - The post office analogy

Let's say we want to send a letter to a company called **The Evil company**. In order to deliver this letter, we need to know the address of the company. So we write a letter and add the address to the envelope. We also add our address to the envelope just in case the company is not there.

So to deliver the letter

- We need to find the address of the company from the name

- If we need to send the letter to a specific person, we would need to add their office number or extension number.

What happens when you type a URL into a browser?

There is a lot of similarity between sending a letter via a post office and sending a packet over the internet. We are unaware of how the letter actually gets to the destination. Did it go in a Tata or Mahindra truck to the airport, what was the name of the person driving the truck, did it fly straight to New Delhi or was it transferred to another plane in Bangalore etc.? We are communicating directly with each other, unaware of the underlying delivery mechanism.

What happens when you type a URL into a browser?

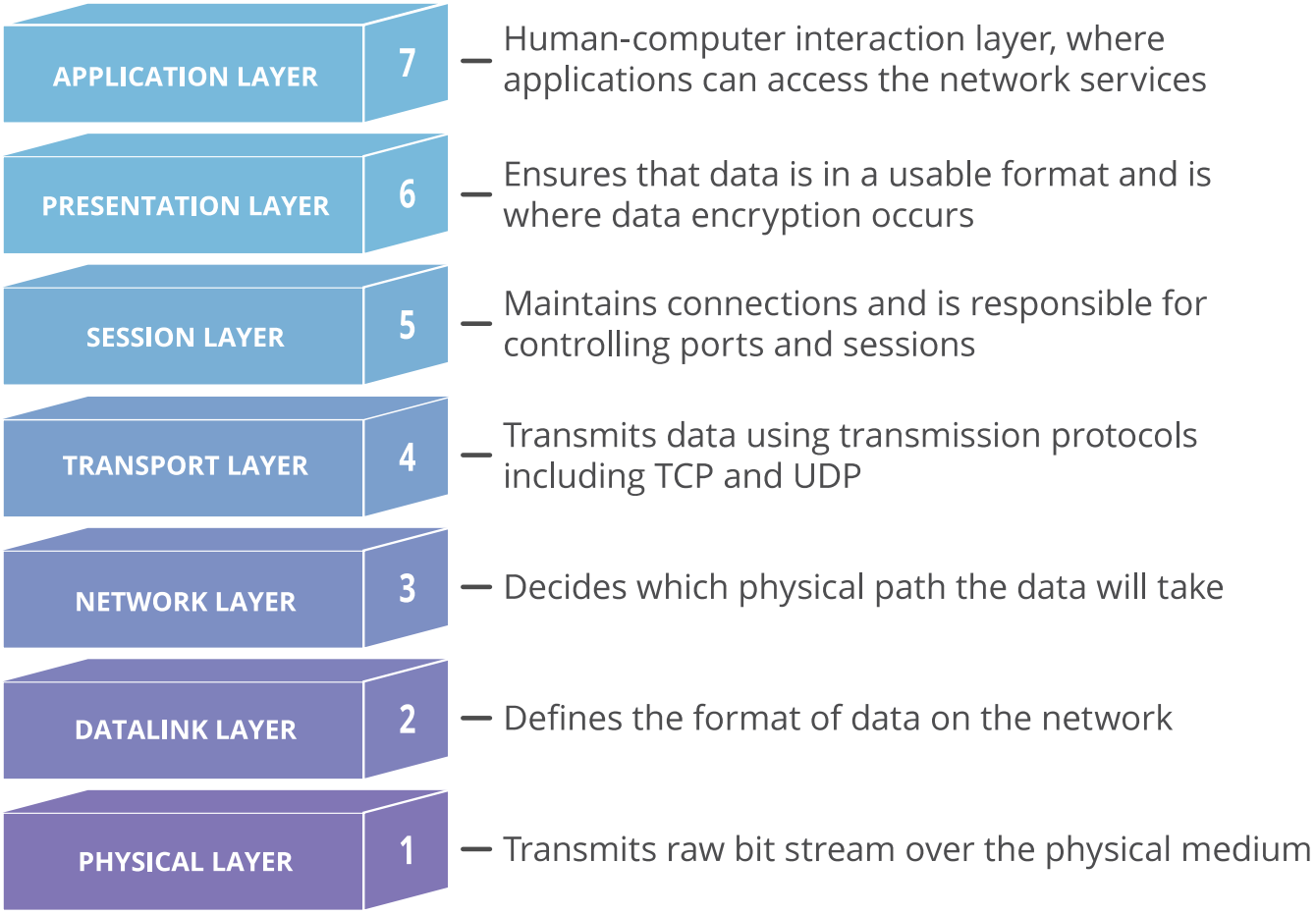
1. The browser parses the URL and figures out if the entry is a search query or a URL.
2. The browser checks if the URL needs to be served from HTTP or HTTPS. The browser checks its "preloaded HSTS (HTTP Strict Transport Security)" list.
3. Assuming a URL, the browser now needs to find the address of the server that will serve the URL.
    - Browser checks if the domain is in its cache. (to see the DNS Cache in Chrome, go to chrome://net-internals/#dns)
    - If not found in the cache, the browser also checks the local hosts file.
    - If the browser does not have it cached nor can find it in the hosts file then it makes a request to the DNS server configured in the network stack. This is typically the local router or the ISP's caching DNS server.
4. Once the browser receives the IP address of the destination server, it takes that and the given port number from the URL, the browser opens a connection to the server and sends the HTTP request.
5. The browser receives HTTP response and may close the TCP connection, or reuse it for another request
6. Finally, the browser decodes the response and displays the result on the screen.

What is the OSI model?

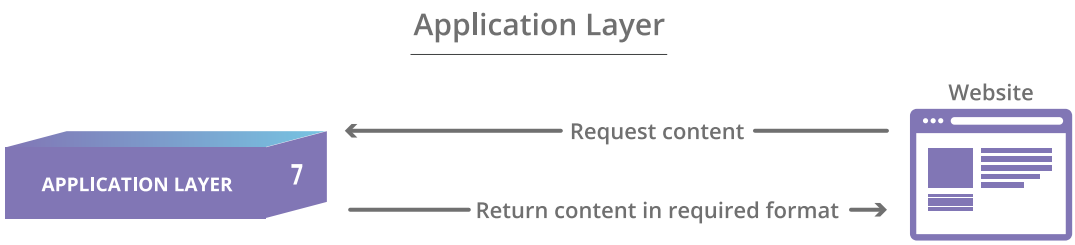
The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides a standard for different computer systems to be able to communicate with each other.

The OSI Model can be seen as a universal language for computer networking. It's based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.

Each layer of the OSI Model handles a specific job and communicates with the layers above and below itself.



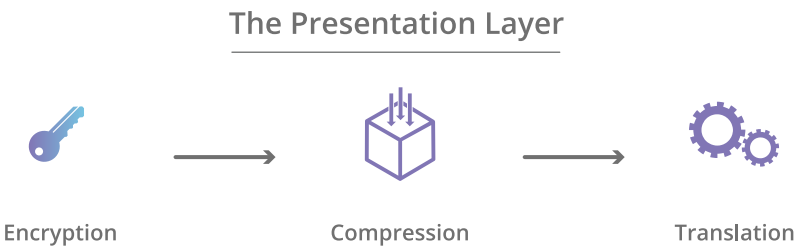
Application



> A user retrieves a Web page from a server in New York by typing a URL into a browser and clicking the enter key. The server receives the request, finds the page on its hard drive and sends it back to the user. Neither the user nor the client or server software is aware of the way the messages were delivered -- did they go over wireless connections, how many routers did they pass through, who manufactured the routers, was the server a PC or a rack-mounted machine, was it running IIS or Apache, etc.?

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications.

Presentation



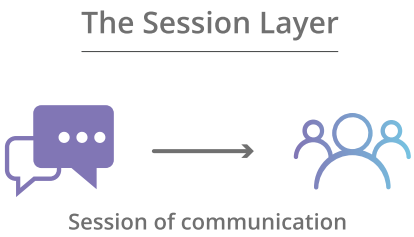
This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.

If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

Finally, the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

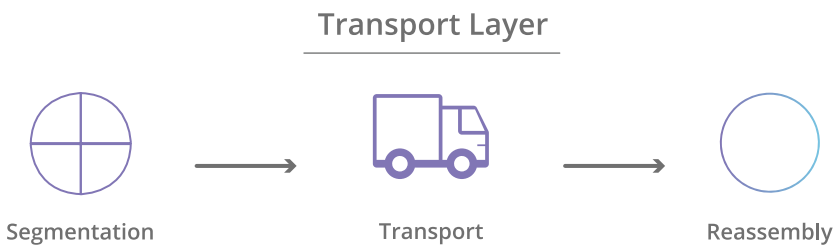
Session



This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

The session layer also synchronizes data transfer with checkpoints. For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

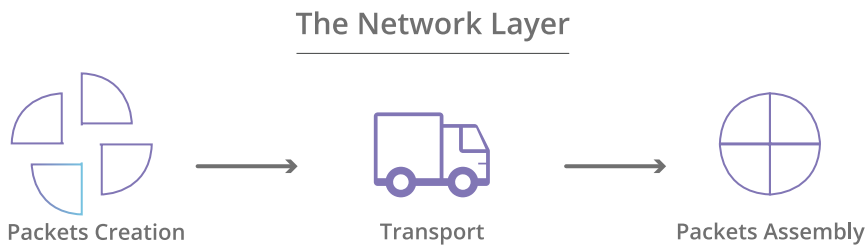
Transport



Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

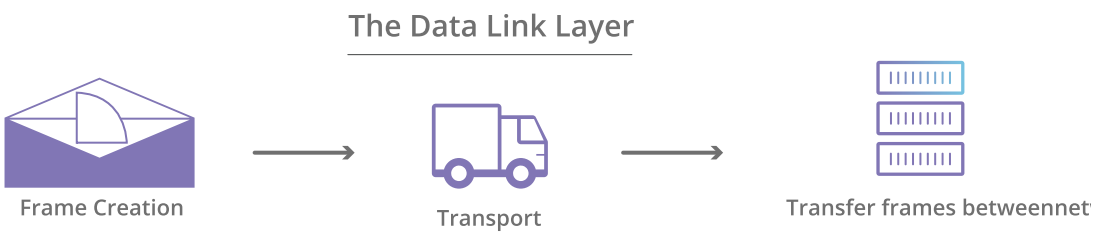
The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.

Network



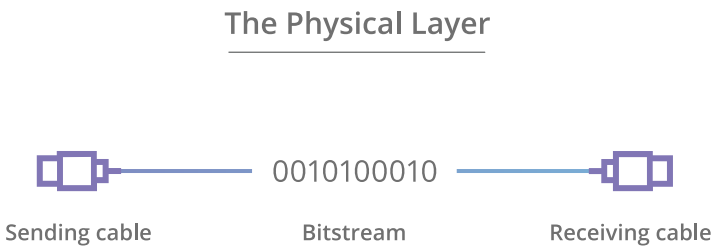
The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.

Data link



The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the SAME network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

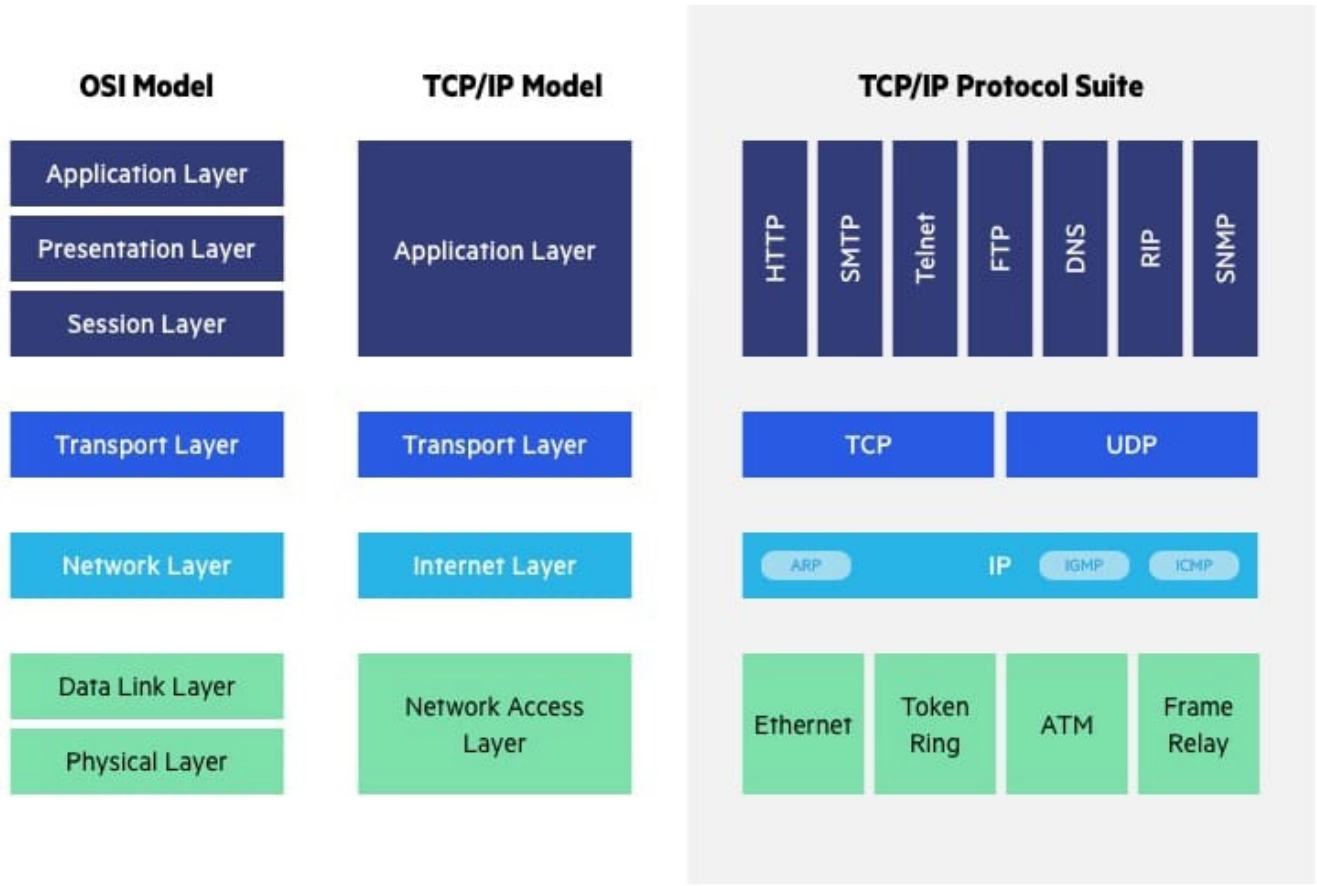
Physical



This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

TCP/IP vs OSI Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.



Some commands to get started

1. Find the IP address of the server you want to connect to. `nslookup <domain>`
2. Find the domain name from a given IP address. `whois <ip>`
3. `ifconfig`

4. Follow a network packet `traceroute <domain>`