**OSI model & TCP/IP cheat sheet**

**1. Devices:**

- **Repeater**: regenerate signals to allow long distance communication => fix the distance problem for networking

- **Hub**: simply a multi-port repeater => fix the scale problem for networking. But all devices connected to the hub will receive data.

- **Bridge**: sit between hub-connected hosts, it only has two ports and can learn which hosts are on each side. This will prevent data in one network from being sent to another network. However, all devices in the network can still receive the data

- **Switch:** is a combination of hub and bridge, it can facilitate multi-port connection and can learn which host are on each port. This will enable data transmission to its destination only and all other devices inside its network won’t receive the data. However, Switch only facilitate communication within a network (192.168.1.x for example)

- **Router:** facilitate communication between networks, router also acts as a physical traffic control point for filtering, security and redirecting. Router can learn which network they are connecting to.

=> Traditional switches cannot perform such tasks, as devices within a network don’t need filtering, if devices in a network have different work scopes, then it’s better to separate them.

**2. OSI model:**

**- Layer 1 – Physical – Transporting bits:**

+ L1 technologies: cables, Wi-Fi, repeater, hub.

- **Layer 2 – Data Link – Hop to Hop:**

+ Interact with the wire: NIC (Network Interface Cards), Wi-Fi Access Cards, Switches.

+ Addressing Scheme – MAC addresses: 48 bits, represented as 12 hex digits. Every NIC has a unique MAC address

* 94-65-9C-3B-8A-E4 (Windows)
* 94:65:9C:3B:8A:E4 (Linux)
* 9465.9C3B.8AE4 (CISCO)

**- Layer 3 – Network – End to End:**

+ Addressing Scheme – IP addresses (32 bits, represented as 4 octets, each 0 – 255)

+ L3 technologies: Router, Hosts, (anything with an IP)

* **ARP – Address Resolution Protocol – Link a L3 address to a L2 address**.

**- Layer 4 – Transport – Service to Service:**

+ Distinguish data streams: when a device receives bits from L1,L2,L3, they are different data packets and without further configuration, the device won’t be able to give the correct data packet to the correct service (or application).

+ Addressing Scheme – Port:

* 0-65535 – TCP – favors reliability.
* 0-65535 – UDP – favors efficiency.

+ Servers listen for requests to pre-defined Ports.

+ Clients select random Port for each connection.

Text

Description automatically generated

* The randomly selected port from the client is crucial as it will be the destination that the server will send data to. In the picture above, the client select port 9999 to connect with server with the port at TCP / 80.
* Therefore, the connection between the client and server above can be simplified as:

**Chart

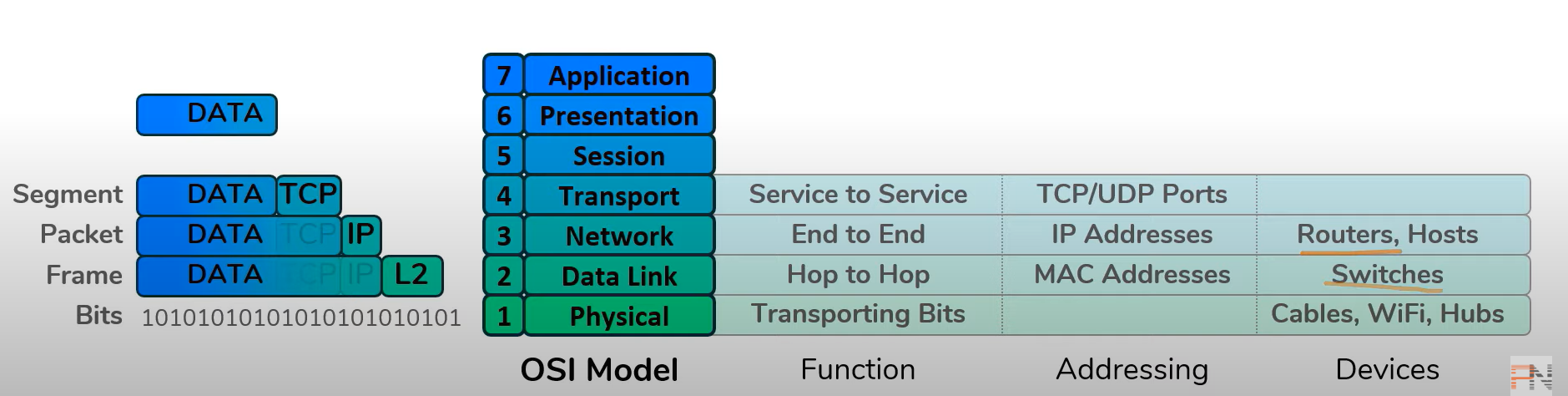
Description automatically generated**

* By this method, connection between different applications on different ports can be established and maintained

**A picture containing text

Description automatically generated**

* It can also facilitate multiple connection on the same server by opening new ports and connect them to the wanted port on the server.

****

***Cheat sheet***

**3. Everything hosts need to do to communicate online:**

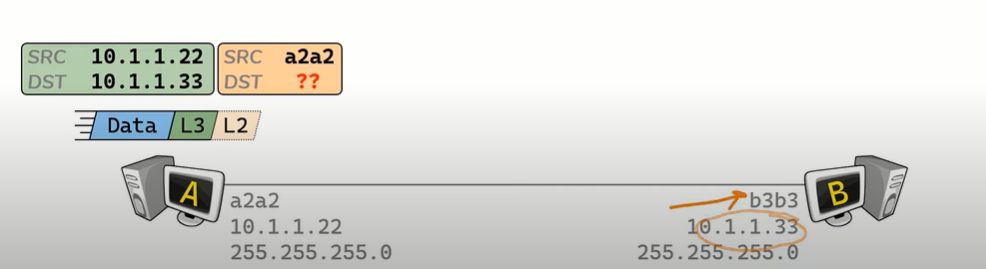
Situation 1: a computer connects with another computer using wired cables.

Computer A perform data encapsulation with its application layer (L7, L6, L5) and it needs to transmit this data to Computer B. For this data to be sent, Computer A need to know:

+ Computer B’s IP address (which is L3 scheme): this can be done by pinging B’s IP address or B’s domain name.

+ Computer B’s MAC address (which is L2 scheme): this can be done using ARP (address resolution protocol).

This can be illustrated with the picture below:

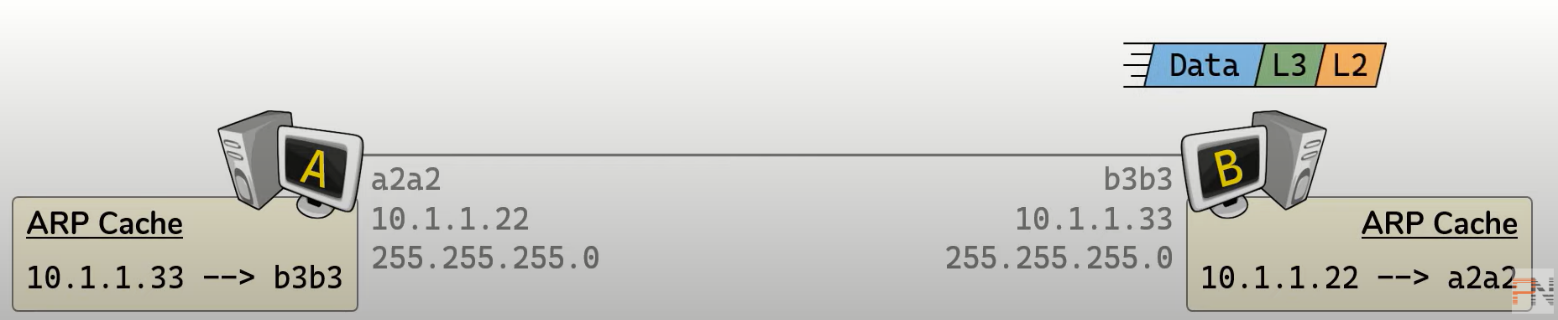


**The process of A’s figuring out B’s MAC address:**

1. As A knows B’s IP address, A can send ARP Request to ask for the MAC address associated with B’s IP address.
2. Graphical user interface, text, application, chat or text message

   Description automatically generatedThis Request will also include A’s MAC address as B’s also doesn’t know A’s MAC address. However, as A doesn’t know B’s MAC address, it cannot send the ARP directly to B, instead, the ARP Request is a Broadcast meaning that it is send to every device in the local network. (Broadcast MAC address is ffff.ffff.ffff). Step 1 and 2 is illustrated with the picture below:
3. Graphical user interface, text, application

   Description automatically generatedARP Mapping are stored in an ARP Cache, which is a table that store devices’ IP addresses and their according MAC addresses. After received A’s ARP Request, B can now populate its ARP Cache with A’s MAC address and send back to A an ARP Response. Note this the ARP Response is Unicast meaning that it is send directly to A as B already has A’s IP address and MAC address. The process can be illustrated with the picture below:
4. Once A receive the ARP Response, it can populate its ARP Cache with B’s MAC address. This will mean that A has everything it needs to perform communication with B and the data will be sent.



**Everything that a Switch does**

**Graphical user interface, text, application

Description automatically generated**

**Text

Description automatically generated with low confidence**

**Exercise:**

**Diagram

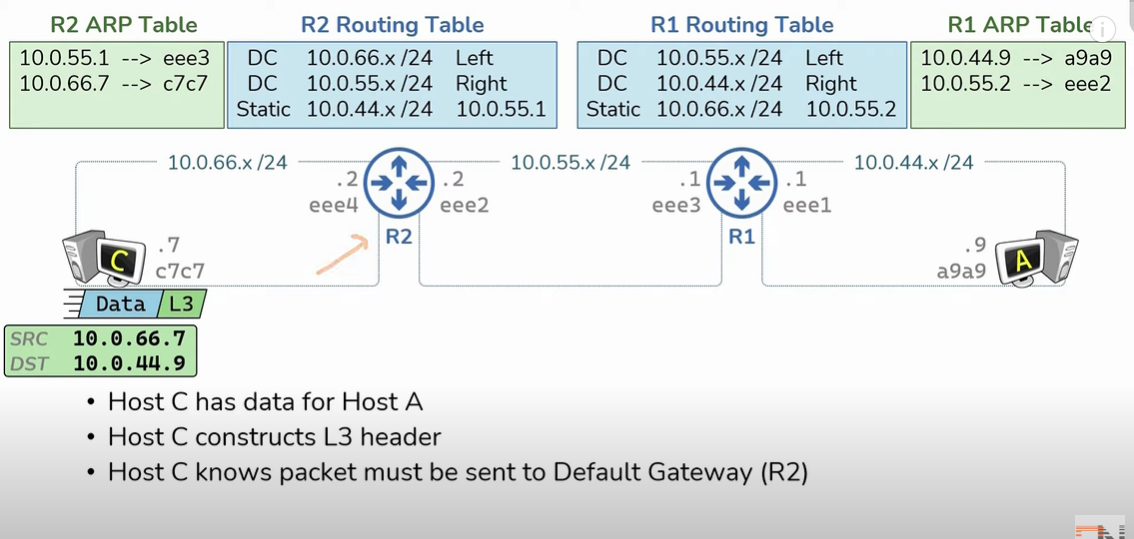
Description automatically generated**

**Everything that a router does:**

**Graphical user interface

Description automatically generated with medium confidence**

**Exercise**

****