Computer Networking Chapter 1 (Layer 1 and 2)

Garen Ikezian

Based on the book by Mike Meyers: “CompTIA Network+ book”

The OSI Model

0.0.0 Learn OSI before anything else...

How does networking work? Is it magic?

To answer such questions, one had to make a graph or a model of some sort to better illustrate networking. There are too many acronyms in networking and they have to be somehow grouped into separate categories.

So the **OSI (Open Systems Interconnect) model** came into being:

Layer #	Description
Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

The OSI model helped standardize computer networking. It helped enable each layer to be its own bubble with little to no interaction with other layers. It is simple and is modular by design.

Another model to consider is the TCP/IP model. It is a simpler version of the OSI model.

TCP/IP	OSI Model
Application	Application
	Presentation
	Session
Transport	Transport
Internet	Network
Network Interface	Data Link
	Physical

TCP/IP model came out 10 years before the OSI model. It is inspired by the ARPANET Reference Model made by the US Department of Defense.

These two models are extremely important when you want to be acquainted into computer networking. It is advised to memorize them as they will be asked during exams.

0.1 Layer 1 and Layer 2 Explained

Layer 1

0.1.0 Cables

Layer 1 devices are very primitive. The do not do much as they do not posses much intelligent solutions. One of the first devices that should come to mind are cables.

Cables come into different forms, there is the UTP (unshielded twisted pair) cable, coaxial cable, and fiber optic cable.

The most common type of cable is the UTP cable as it cheap and easy to install.

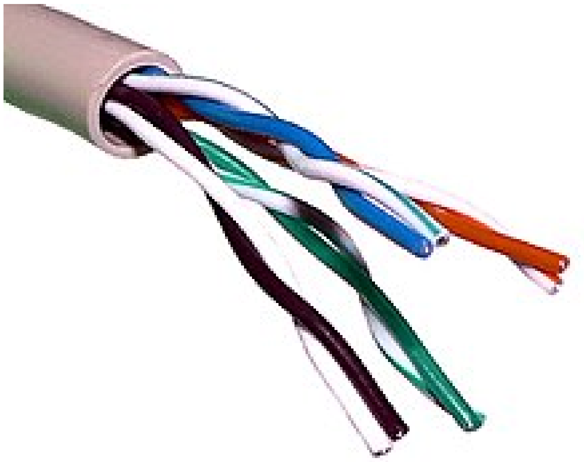

Figure 1: UTP Cable

Another device that comes to mind is the *hub*.

Figure 2: Hub Device

Hubs are not intelligent and cannot filter traffic by MAC address. They only broadcast data across each connection. In other words, it makes an exact copy of the receiving frame then distributes it for every connected port except for the port it originated from.

Hubs operate at layer 1 of the OSI model as they do not interact with incoming frames. It is a mere physical extension for other physical nodes.

Layer 2

0.1.0 NICs

We all know what cables are don't we? Ethernet cables are now the standard. But cables are nothing without NIC cards...

NIC (network interface card): It is a device that acts as an interface between the computer and the network. It is what enables internet access to your computer. It is quite a complicated device. The only getaway from here is that it helps facilitate cables and operating systems.

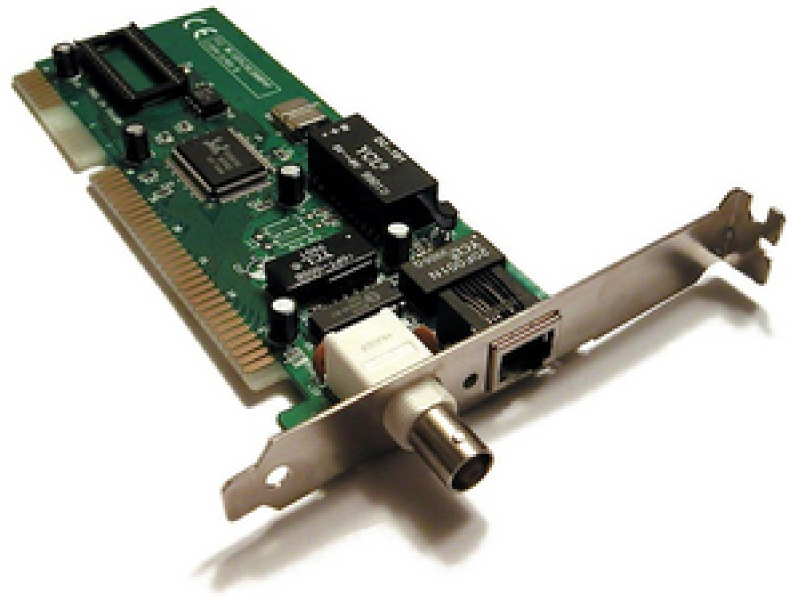

Figure 3: NIC

Back in the 90s or early 2000s, NIC cards were usually separate devices but are nowadays integrated into the system motherboard.

Inside the NIC card, you will find a ROM chip with a special firmware built with identity in mind. This physical identity is the **MAC (media access control) address**. It is 48 bit (6 bytes) value long of which no two addresses will ever be the same. In other words, it extremely unusual to find two different devices with the same MAC addresses.

The first 24 bits of the MAC address are dedicated to the manufacturer of the NIC card, known as the **OUI (Organizationally Unique Identifier)**. The remaining 24 bits represent the serial number of the NIC card, which is referred to as the **device ID**.

The IEEE (Institute of Electrical and Electronics Engineers) decides the formation of MAC addresses from a numbering scheme originally called MAC-48 (now called EUI-48).

0.1.1 What are Frames?

The flow of data is done through cables. And inside these cables have signals of data that are represented as frames. It is the frames that are sent to the computer and are retrieved by a NIC card.

Frames are data units within the data-link (layer 2) of the OSI model. They wrap around streams of data with 1s and 0s . Think of them as “atoms” for any partial data. They are no different from charges on wires.

How are frames represented? In order from left to right, they are represented like so:

Preamble	Recipient’s MAC Address	Sender’s MAC Address	Type	Data	FCS

It is divided into three parts/fields:

Header: Preamble, MAC addresses and type

Payload: Data

Trailer: FCS (frame check sequence)

What is preamble? It is not part of the frame per se. However, it helps the receiving device to identify the beginning of the incoming frame. It is basically a “heads-up” to show that a frame is coming.

What is type (the field)? The **Type** field specifies the protocol received for the upper layer (in this case, the network layer). It is usually either IPv4 or IPv6. These two protocols help to better identify MAC addresses and will help ensure their proper use.

What is FCS? FCS (Frame Check Sequence) is a field dedicated to verify and check if the received frame is intact. It relies on an algorithm known as CRC (Cyclic Redundancy Check) whereby the NIC does binary arithmetic to calculate the remainder with a divisor against this field. If it does not match, the frame gets dropped.

It is no different from the last digit(s) of a barcode number that helps to confirm the integrity of the barcode number.

0.1.2 Where do Frames Go?

It depends on how the network is configured and what call is made by a NIC sender.

Often, once a signal is sent to transmit data across the network, frames go into varying boxes and/or devices.

The first two important boxes to bear in mind are hubs and switches. They're good extensions for cables.

While we are familiar with hubs and their placement in layer 1 of the OSI model, switches exhibit greater intelligence compared to hubs.

Figure 4: Switch Device

Unlike hubs, switches can filter traffic by MAC address and have the ability to send frames to a specified connection. They help facilitate a network between different nodes.

Switches belong to layer 2 data-link of the OSI model.

So if a situation arises where a computer needs to send something to another recognizable computer in the same network, the NIC needs to create a **unicast frame** in order to commit **unicast addressing**.

Unicast frame: A frame dedicated a specific device in the local network.

Unicast addressing: The *ability* of which the unicast frame was sent to a specific device.

Now with all these in mind, the sending NIC can interact with other NICs. However, before it sends anything to a particular NIC, it needs know the *address* of that NIC.

But what if you brought a new computer in your network, how will that computer be recognized?

How will the sending NIC know the address of the receiving NIC? The sending NIC typically knows the receiving address. However, there might be situations where the sending NIC doesn't "remember" or needs to discover a new address that is not familiar with.

This is where the ARP protocol comes in.

With ARP (Address Resolution Protocol), it facilitates the cooperation of IP addresses and MAC addresses. IP addresses and MAC addresses are both used to identify nodes. Since IP addresses are automatically created when a node is connected to its ISP (internet service provider), the NIC will take that advantage to enable mapping of a recognizable IP address to its MAC address.

1. It starts with the sender sending an ARP Request as a broadcast with the address FF:FF:FF:FF:FF:FF (layer 2 data-link). It will notify every NIC in the network (**Who has this IP address? Please send me your IP address**).
2. If the receiving node determines whether it is the intended target, it will provide its own MAC address (**I am IP address blahblah. Here is my MAC address: blahblah**).
3. The sender now knows the address of the receiving NIC. It can now interact with ease.

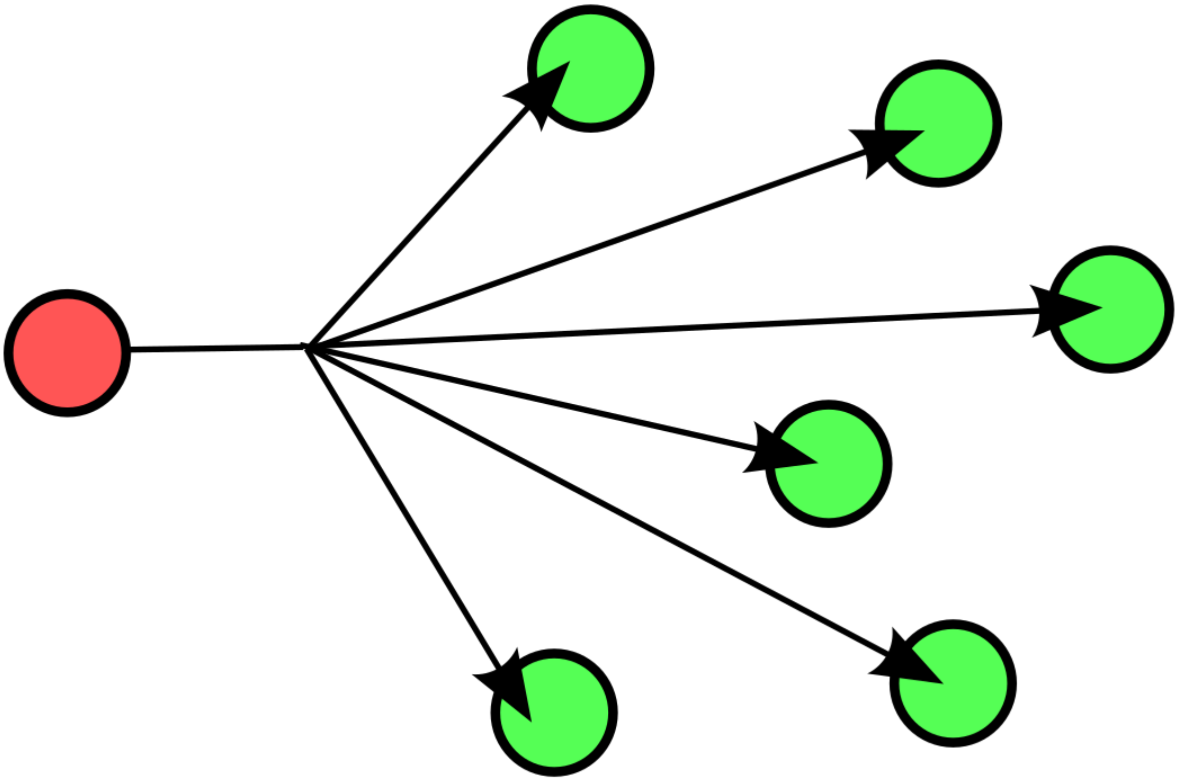

Figure 5: Broadcast

0.1.3 Explaining NICs

NICs facilitate two bridges. It helps frames to move in and out of itself and the cables connected. It also helps bridging data back and forth between itself and the Operating System. There's a reason why the word *interface* in the acronym NIC.

To start, there are important functions NICs have to commit: - Media Access Control (MAC): - Creates and addresses frames for/to the network. - Enables broadcasting and validates incoming frames. - Logical Link Control (LLC): Interacts device OS drivers and links the gap between the physical and the networking layer through different protocols.

> **! It is important to note that NICs are both Layer 1 and Layer 2. If asked if NICs are both layer 1 and 2, it is a correct and accurate statement. If asked if NICs are only in layer 2, is a reasonable statement only if you wish to consider its special purpose. !**

Because of NICs inconsistency on whether it belongs to Layer 1 or 2, to solve its ambiguity, it has been made more modular. Thus,

Layer 2 is the only layer in the OSI model with sublayers.