
Protocol TCP/IP and Wifi 802.11



Contents

1.1	Introduction	3
1.2	TCP/IP Model	3
1.3	Protocols of TCP/IP	5
1.3.1	Internet protocol: IP	5
1.3.2	User datagram Protocol: UDP	7
1.3.3	Transmission Control Protocol: TCP	8
1.4	Wifi 802.11	10
1.4.1	Introduction	10
1.4.2	Physical Layers	10
1.4.3	Wifi frame	11

List of Figures

1.1	Structure of Model OSI and TCP/IP	3
1.2	IP datagram	5
1.3	UDP datagram	7
1.4	successful transmission	8
1.5	transmission error	8
1.6	TCP datagram	9
1.7	Header MAC	11

1.1 Introduction

This is the US government with his various agencies who understood the essential aspect of interconnection. It therefore decided to fund research in this field through the DARPA (Defense Advanced Research Project Agency) Agency Advanced Research Projects of the Ministry of Defence.

DARPA has developed a number of standards, specifying the principles and conventions communications between computers, which are often referenced by the name TCP / IP, because the two main standards: TCP and IP. These protocols can be used to communicate within a set of interconnected networks of any size, they are connected to the outside world or not.

1.2 TCP/IP Model

It is important to remember that the TCP / IP model has been proposed ten years before the OSI model, the latter being strongly inspired by some TCP / IP protocols. Nevertheless, it is interesting to place the OSI model defines a 7-layer model, based on the Internet protocols that operate on four layers.

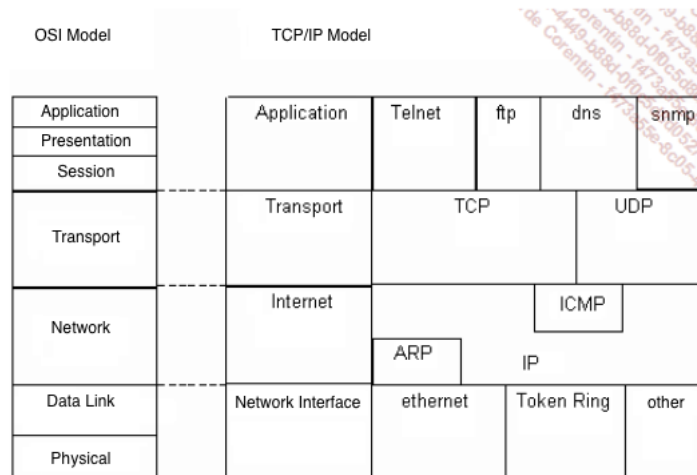


Figure 1.1: Structure of Model OSI and TCP/IP

The TCP / IP model is relatively simple and only has four layers:

-Application Layer:

The user receives TCP / IP as a set of programs providing services using the network for different purposes. The main services can be of type file transfer, messaging, Web service, or other remote connection. Thus we find in TCP / IP both protocols for this kind of service and interface programs allow the user to implement. FTP (File Transfer Protocol) is a typical example.

-Transport Layer:

In this layer we have two kinds of interconnections.

Packet delivery service no secure mode

This service is the basis for all other services. Data packets are transmitted from one machine to another using the addresses contained therein. At this level, the packets are routed independently of each other, also, there is no guarantee of reliable delivery and not more arrival sequence. UDP (User Datagram Protocol) is responsible for this kind of transport.

Reliable Transport Service

Network applications require error-free communications, including through the use of automatic times in error. The reliable transport service handles such problems. It allows an application to establish a connection end to end with an application running on another machine in the same manner as if it were a direct and permanent connection. TCP (Transmission Control Protocol) ensures that reliable transport service.

The networks are interconnected by machines that can be dedicated or not, called routers. These routers make the decision to refer the information to one direction or another, depending on their tables for how to achieve a particular network. World-wide TCP / IP, routers are also called Gateway.

-Internet Layer:

The term "internet" (lowercase) designates said functional layer whose role is to implement protocols for interconnecting physical networks via the fundamental operation of said routing. The global network "Internet" (first letter capitalized) naturally borrows the name of this layer because it appears as one large logical network that interconnects millions of physical networks.

This layer corresponds to more protocols, the most important is the IP protocol. This is fundamental. He realizes the routing of information between machine (called hosts) via an addressing plan requiring any routing. It uses logical addresses encoded on 32 bits (Protocol version 4) or 128 bits (version 6).

-Host network Layer:

This layer will hide the characteristics of the physical network.

It appears as a combination of pilots (drivers) and related programs that include:

The mapping logical addresses (IP addresses described below) and physical addresses (Ethernet addresses for example).

The encapsulation of the data in the frames transmitted on the network.

1.3 Protocols of TCP/IP

A TCP / IP network interconnection provides three types of services, based on one another:

- Application Services
- Reliable transport service (UDP/TCP)
- Packet delivery service connection less (Internet Protocol)

At the lowest level, the packet delivery service connection less provides basic transportation for all other services.

At the next level, a reliable transport service allows to transmit their information to higher level services(applications).

1.3.1 Internet protocol: IP

The packet delivery service connection less is called IP (Internet Protocol). It is described in RFC 791 and defines three importants standards:

- Unit of data transferred in IP interconnections. Describes the exact structure of all data transmitted over a TCP / IP interconnection.
- Routing function. This is the selection of the path to be used
- A set of rules for the unreliable packet delivery, error handling, packet destruction conditions.

Structure of IP datagram:

As a physical frame has a structure. an IP datagram contains two parts: the header and the data portion.

0			481631	
Version	LGMAT	Type of service	LGR Totale	
IDENTIFICATION			DRAP.	Fragment offset
Time to live	Protocol		Header checksum	
Source IP Adress				
Destination IP Adress				
IP options				Jam
Data				
...				

Figure 1.2: IP datagram

Version: Coded on 4 bits, contains the version number of the IP protocol used to create the datagram. It is used to ensure that all participants, transmitter, receiver and intermediate gateways, are agreed on the structure of the datagram. If the standard evolves, the machines reject datagrams whose version number is different from theirs.

LGMAT: Also encoded on 4 bits, this field indicates the length of the header in 32 bit words. All fields are of fixed size, with the exception of "IP Options" and "Jam". A running head, devoid of these two fields, has a length of 20 bytes, so the value of 5 in the LGMAT field.

LGR Total: It indicates the total length, in bytes, of an IP datagram, header and data included. The size of the data field can be calculated by subtracting "LGMAT" to "LGR TOTAL". The maximum size of the datagram is 65,535 bytes, as the LGR TOTAL field is coded on 16 bits.

Type of service: Coded on 8-bit, it indicates how the datagram should be handled.

Identification: It contains a unique integer identifying the datagram.

Fragment offset: This field expressed in multiples of 8 bytes the data offset from the original datagram and starts at zero.

Flag: Coded on 3 bits. It is used for the fragmentation.

Time to live: Specifies in seconds the maximum transit time of the datagram.

Protocol: It indicates which transport protocol that was used to create the conveyed message.

Header Checksum: It ensures the integrity of the header data. That is considered as a 16-bit integer result, where the arithmetic sum is performed in one's complement.

Source/Destination IP Address: They contain the IP addresses of 32 bits of the sender and the recipient of the frame.

Data: It indicates the beginning of the datagram data area.

Options: It is of variable length and is not required in all datagrams. It is used primarily for testing or development.

Jam: Depends on the selected options and ensures that the datagram header has a size which is an integer multiple of 32 bits. It contains zero bits.

1.3.2 User datagram Protocol: UDP

UDP (User Datagram Protocol) uses a simple connectionless transmission model with a minimum of protocol mechanism. The transmitted data integrity checking is the responsibility of the application that will use the UDP services. It is located above the IP and uses thereof services.

Structure of UDP datagram:

Each message is called User datagram or UDP datagram. But both parties are distinguished with UDP header and a data part:

0	8	16	31
Port UDP source			Port UDP destination
UDP Length			Checksum
Data			
...			

Figure 1.3: UDP datagram

UDP protocol is often used with multimedias applications such as streaming media, real-time multiplayer games and voice over ip (VOIP). Indeed, with this kind of applications, loss of packets is not usually a fatal problem. If using UDP and you want reliability, the end user applications must provide any necessary handshaking such as real time confirmation that the message has been received.

1.3.3 Transmission Control Protocol: TCP

TCP (Transmission Control Protocol) is a reliable delivery service in connected mode. It allows applications to not have to worry about reliability problems.

How TCP can be reliable?

This is possible by an acknowledgment / retransmission mechanism.

Example of successful transmission:

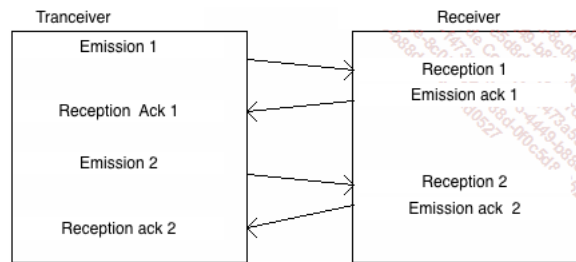


Figure 1.4: successful transmission

Example of transmission problem:

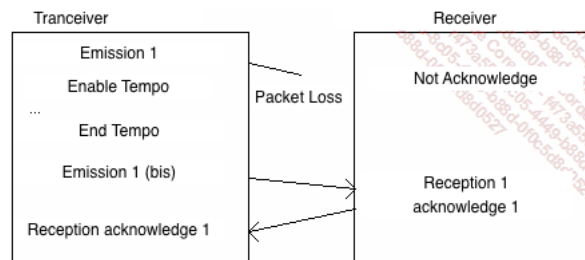


Figure 1.5: transmission error

It is more difficult to manage the problem of duplicate packets, whether data sent or acquittals. This is solved by assigning each packet a serial number and forcing the receiver to store the list of received numbers.

The positive acknowledgment and retransmission protocols also place the sequence number in the acknowledgments.

Structure of TCP datagram:

0	4	10	16	24	31
source port				destination port	
sequence number					
acknowledgement number					
data offset		Reserved	Bits code	window	
Checksum				Urgent pointer	
options				padding	
Data					
...					

Figure 1.6: TCP datagram

1.4 Wifi 802.11

1.4.1 Introduction

It was in 1997 that 802.11 working group after several years of work, standardizes the definition of Wireless LAN type networks. As 802.3, these specifications cover the layers of the OSI model Physical and Data Link. The latter is divided into two sub-layers: Medium Access Control (MAC), for access to the transmission medium and Logical Link Control (LLC) for controlling the transmission.

802.11 physical layer defines three modes of transmissions. The first using infrared diffusion, which but not retained in the implementations of these specifications. The two other techniques use radio transmission. Finally, a single, called Direct Sequence Spread Spectrum (DSSS) is exploited.

1.4.2 Physical Layers

Many specifications have improved the original 802.11. Among these, three define the physical layer use.

802.11.b

This standard, published in September 1999, just increase the maximum transmission speed at 11Mbps, with possible declines to 5.5, 2 and 1 Mbps. Its operating frequency is 2.4 GHz. Besides, The network now has a name, the SSID (Service Set Identifier).

802.11.a

Like 802.11b, 802.11a is published in September 1999. But the physical layer is designed to work in 5 GHz. The maximum transmission is 54 Mbps. As before, folds of solutions are provided, 48, 36, 24, 18, 12, 9 and 6 Mbps. Because of the frequency change, 802.11a antennas are incompatible with 802.11b.

802.11.g

This standard, ratified in June 2003, finally succeeds 802.11b. Operator, as the latter, the 2.4 GHz band, it allows data rates to 54 Mbps. Possible folds are the same as 802.11a, 48, 36, 24, 18, 12, 9 and 6 Mbps.

802.11.n

802.11g remains, since 2003, the specification most exploited commercially. The evolution 802.11n been finalized by the IEEE in September 2009.

802.11n uses the frequency bands 2.4 and 5 GHz. In the latter, it is possible to double the width of the channel used, which saves even speed. The maximum speed of the final version of 802.11n is 200Mbps. The techniques used in theory possible to go up to 540 Mbps.

The indoor range is approximately 50 meters against 125 meters outdoors.

802.11.ac

802.11ac has been standardized in January 2014. It utilizes the frequency band 5 GHz to 6 GHz and can reach up to 7 Gbps throughput through different mechanisms. It guarantees backward compatibility with 802.11n on the frequency band of 5 GHz.

1.4.3 Wifi frame

The Medium Access Control layer (MAC) sublayer lower data link is the heart of Wi-Fi.

It must manage the media, or rather the lack of physical media, characterized by a radio frequency. This channel must be shared between the different network nodes. Each has a MAC address of its own, as in Ethernet. But the media management mechanism can not use collision detection, inconceivable in the air. A frame avoidance solution, CSMA / CA type is thus exploited.

The management of bandwidth sharing is not the only use of the MAC layer. Before transmitting data to an access point, a station must be connected to Basic Service Set (BSS), network of the master device. An association process is previously necessary. And before that, an authentication of the station can be requested by the AP.

Other problems are also taken into account at this level. The fragmentation / de-fragmentation of transmitted frames, and the ability to communicate at different flow rates are managed. The error control and energy savings are also not forgotten. Securing can also be managed at the MAC layer.

Wireless frame header is much more complex than its Ethernet. The frame body has a maximum size of 7956 bytes. Note that four fields are reserved for the MAC addresses. They allow the use, in addition to source and destination addresses, access as intermediate points.

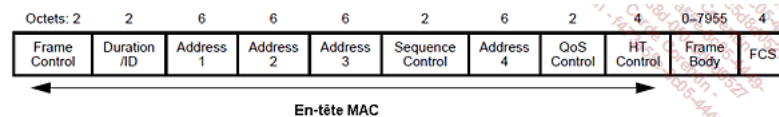


Figure 1.7: Header MAC

Bibliography

- [1] José DORDOIGNE, *Réseaux informatiques - Notions fondamentales*. ENI 6nd Edition, mars 2015.
- [2] Philippe MATHON, *Windows Server 2003 Les services réseaux TCP/IP*. ENI
- [3] Web site, *For additional information*.