LESSON E7_EN. TCP/IP FUNCTIONS AND PRACTICE.

Parent Entity: IPA SA, Bucharest, Romania, 167 bis, Calea Floreasca; Fax: + 40 21 316 16 20
Authors: Gheorghe Mincu Sandulescu, University Professor Dr., IPA SA, Bucharest, Romania, 167 bis, Calea Floreasca,
Mariana Bistran, Principal Researcher, IPA SA, Bucharest, Romania, 167 bis, Calea Floreasca, e-mail: san@ipa.ro. Consultations: Every working day between 9.00 a.m. and 12.00 p.m.

After studying this lesson, you will acquire the following knowledge:

- The functions of the Layers of TCP / IP Stack with Layers.
- The creation of the virtual, Pair to Pair, channels between Layers of the same rank,
- The functions of the TCP/IP Layers Application, Transport, Internet, Media Access.
- The manner of accomplishment of network / Internet reliability through the use of the connection oriented TCP protocol.
- The manner of creation of Headers and the creation of Segments, Datagram and Trams. Others.

CONTENT OF THE LESSON

1. THE MAIN FUNCTIONS OF THE TCP / IP LAYERS .
2. SENDING DATA PACKETS. THE LAYERS: 4-APPLICATION, 3-TCP, 2-INTERNET AND 1-MEDIA ACCESS. THE ESSENTIAL FUNCTIONS.
3. THE TCP/IP FUNCTIONING ON THE RECEIVING OF THE DATA PACKETS.
4. THE SUCCESSIVE ENCAPSULATION OF HEADERS AND DATA ON THE CREATION OF THE TCP / IP PACKETS.

LEARNING OBJECTIVES:

After learning this lesson you will acquire the ability to:

- Understand, explain and use the functions of the Layers of TCP / IP Stack with Layers.
- Understand, explain and use the Pair to Pair channels between the Layers of the same rank,
- Understand the features and the functioning of TCP/IP based on 4 Layers: Application, Transport, Internet, Media Access.
- Understand who and how is accomplished the reliability inside the Internet network reliability.
- The manner of creation and encapsulation of Headers and the creation of Segments, datagram and Trams. Others.
- Understand how the TCP/IP suite of protocols is applied.

1. THE MAIN FUNCTIONS OF THE TCP / IP LAYERS.

The TCP protocol and the IP protocol were the first protocols of the TCP/IP suite. These protocols constitute the basic elements which have been decisive for a reliable Internet functioning.
TCP /IP is based on 4 layers: **Application, Transport, Internet, Network Interface**.

In the process of sending Data, the main functions achieved by the TCP / IP protocols consist in:

- Cutting of the message into parts which will become the Data of the Data packets,
- Solving, step by step / layer by layer, of the multiple stages of encapsulation of Data. The completion of the Headers, on each layer.
- Monitoring the transfer of the Data Packet through multiple Layers,
- Preparation of the Data Packet to be sent in a serialized mode toward the physical media, and the assurance of monitoring of the interfacing processes achieved by the NIC- Network Interface Card.
- Assurance of the opening and closing of communication sessions with other hosts, in Peer to Peer mode.
- Assurance of the IP addressing needs. The placement in the header of the Data Packet of the IP Destination Address, the IP Source Address, and of other necessary information.
- Assurance and adaptation of the pace of sending the Data Packets, so as to diminish traffic congestion.
- Assurance of reliability of the digital communication, communication based on the **switching packets technology.** The error control: deteriorated, non-arriving and lost Data Packets, time to live (TTL) of the Data Packets.
- Assurance of the MAC (Media Access Control / Physical Address) addressing needs. The assurance of Data transfer from the Application layer to the network.
- Assurance of functioning of the Internet diagnosis tools.
- Other functions.

In the receiving of Data, the main functions achieved by the TCP / IP protocols are similar to the ones above, also including:

- The reception of Data (as Data packets named trams) from the network, the transfer of data towards the high rank Layers, the reconstruction of the message in Layer 3, and the offering of the reconstructed message to Layer 4, Application, which transfers the information to the machine programs.

The Layering principle:
Layer x of the destination Host or Server receives exactly the same object emitted by the correspondent layer x of the emitting Host or Server:
Layers 4 - Application to Application, exactly the same Message,
Layers 3- Transport to transport, exactly the same Data Packet,
Layers 2- Internet to internet, exactly the same Datagram,
Layers 1- Network Interface to Network Interface, exactly the same Frame, named Tram.

The type of software and the type of addresses used on each TCP /IP layer:
Layers 4 – Software not included inside the operating system. Virtual Ports for appealing the correspondent Protocol of Layer 4.
Layers 3- Software of OS (operating system).
Layers 2- Software of OS. IP Addresses.
Layers 1- Own Software. Physical Addresses.

2. THE DATA (TRAM) SENDING. LAYER 4 APPLICATION, LAYER 3 TCP, LAYER 2 INTERNET AND LAYER 1 MEDIA ACCESS.

1. **TCP / IP Layer 4: Application.**

The Application Service of TCP / IP Layer 4 implements the functions of all Layers 5, 6 and 7 of the ISO model.

The service of the TCP / IP Layer 4, Application, achieves:

- The formatting,
- The transfer and the reception, of the Data concerning the Application Layer.

The TCP / IP, Application Layer, generates a request of connection, corresponding to the opening of the communication session.
The process is achieved by sending [toward the chain: TCP / IP Layer 3 → 2 →1 (of the same machine)] the information. The process starts by sending the Message from Layer 4 toward Layer3.
The Message is a file, including Data and the correspondent specific indications generated by the Application Protocol.

TCP / IP Layer 4 hosts protocols such as : HTTP, DNS, SMTP, POP3, IMAP4, Telnet, FTP, NFS, NIS, LPD, Telnet, Remote login and other.

Protocols for e-mail transmission.
Among the e-mail services there are services described by the following protocols:

- SMTP- Simple Mail Transfer Protocol (described in the RFC 882), (The messages to be sent: binaries, audio and video, may be encoded with the UUENCODE programme and decoded, on reception, with the UUDECODE programme).
- POP3-Post Office Protocol, Version 3 (which requires the Server toward which the message is sent to be in function),
- IMAP4-Internet Message Protocol Version 4 (better than POP3, because the e-mail may be recovered, even in the cases in which the targeted Server was not in function at the time when it received the Data packets).

HTTP-Hypertext Transfer Protocol is the protocol which assures the transfer of web pages, from a host, inside the own machine.

FTP-File Transfer Protocol serves in the transfer of files, through the IP network, and between 2 machines:

- the server and
- the client.

NFS -Network File System, protocol serves in the exportation (transmission) of the File System from one machine toward another machine.

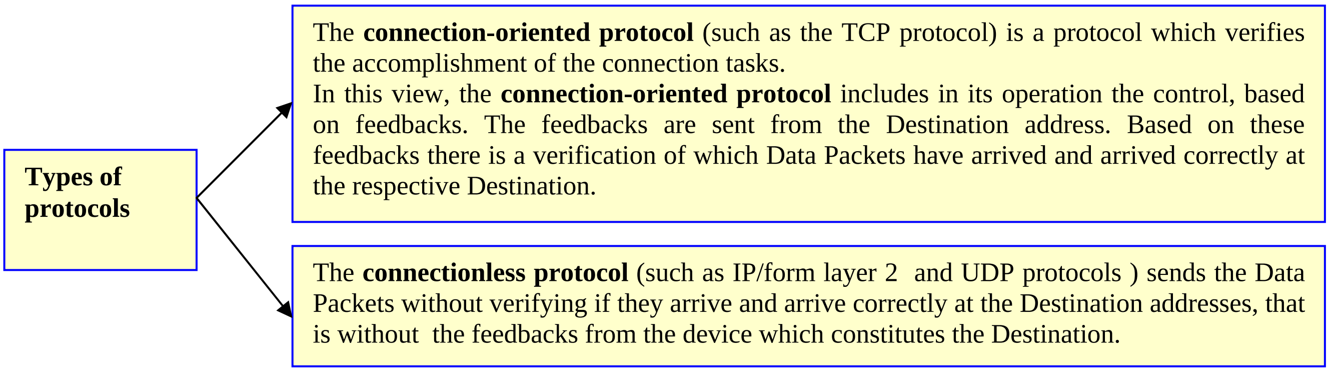
Other protocols are also hosted on Layer 4 application.

2. THE TCP / IP Layer 3. TRANSPORT.

The TCP / IP Layer 3 TCP, named Host to Host layer, is responsible **for flow control and connection reliability**, and it hosts primarily the protocols:

- TCP- Transmission Control Protocol and
- UDP-User Datagram protocol.

Generally speaking, the protocols are of 2 types: **connection-oriented protocol and connectionless protocol.**



Types of protocols

The **connection-oriented protocol** (such as the TCP protocol) is a protocol which verifies the accomplishment of the connection tasks.
In this view, the **connection-oriented protocol** includes in its operation the control, based on feedbacks. The feedbacks are sent from the Destination address. Based on these feedbacks there is a verification of which Data Packets have arrived and arrived correctly at the respective Destination.

The **connectionless protocol** (such as IP/form layer 2 and UDP protocols) sends the Data Packets without verifying if they arrive and arrive correctly at the Destination addresses, that is without the feedbacks from the device which constitutes the Destination.

The TCP is a **connection-oriented protocol** which guarantees the transmission of Data (and announces the impossibility of transfer).
The UDP protocol is a **connectionless protocol** which does not guarantee the transmission of Data.

2.1.) THE TCP / IP Layer 3. TRANSPORT. The TCP Protocol.

The TCP protocol (which is a **connection-oriented protocol**) assures, for the applications, services of guaranteed connection and delivery of the Data fluxes.
That means that the TCP protocol controls the execution of the transmission, the correct transmission and the flow.

The TCP protocol, placed on Layer 3, achieves:

- Cutting into segments of the Message received from Layer 4; the parts are named Segments. On the output of Layer 3, Data are segmented into Segments.
- Generation of the **connection-oriented** procedure for the achievement of a connection with the machine of interest (another host or work station or another network device),
- Addition of the TCP Header to each Data Packet.
- Multiplexing of the Data packets toward the protocols,
- Control of the Data flux.

  The control of the Data flux takes into consideration the number of the Data Packets not acknowledged by the Destination.

  In the case in which the Destination does not acknowledge the reception, within the time interval, of an approximate number of Data Packets, the Sender diminishes the rate of sending.

  The diminishment of the rate of sending is achieved through the use of **windows for the flux control** (the number of the bytes accepted for sending in the time window).

- The security and reliability controls.

  In view of accomplishing a high level of reliability, the reception of the Data Packets by the destination is acknowledged to the Sender.

  The non-received Data Packets are retransmitted (there is a pre-established number of retransmissions).

  The reliability is achieved through the procedure: **PAR-Positive Acknowledgement Retransmission**, which solves situations related to:

  - Data (Data Packet) received in an incorrect form,
  - Data lost,
  - Doubling of Data.

  In the case of the corruption of the Data, the TCP of the sender receives this information and resends the Data Packet.

- Transfer of Segments toward the inferior Layer, Layer 2 Internet.
- Others.

Features of the TCP protocol [10]:

- Stream orientation. Stream of bits grouped into octets (bytes, 1 bytes includes 8 bits).
- Virtual Circuit Connection, peer to peer, from software packages on the same layer 3, in fact through layers of inferior ranks.
- Buffered Transfer. The Data are passed through software packages.
- Unstructured stream. The stream service is the same for all cases.
- Full Duplex Connection. The connection is achieved in both directions.

The TCP / IP Layer 3, Transport, provides the software means for the achievement of the above tasks.

The **connection-oriented protocol**, TCP / Transport, establishes, before transmitting Data, a virtual **end-to-end connection**, between layers 3 of the 2 machines which communicate.

But this E**nd-to-End connection** is achieved based on the fact that the Data Packets are received, at each End, by the use of the **connectionless oriented protocol** hosted in Layer 2, the IP protocol (fig.2.1.).

The TCP protocol guarantees the reliable transmission of Data. Or it announces the impossibility of transmission

The applications of Layer 4 use the TCP protocol of Layer 3 for a reliable transmission of Data.

The TCP is the transport protocol which is most intensively used. It is used in Full Duplex, on virtual circuits (fig.2.1.) and with a high reliability level.

The TCP protocol assures the reliable connection and transmission of Data toward a long distance destination and for the data packets travelling through the intermediary Hops, fig. 2.1.

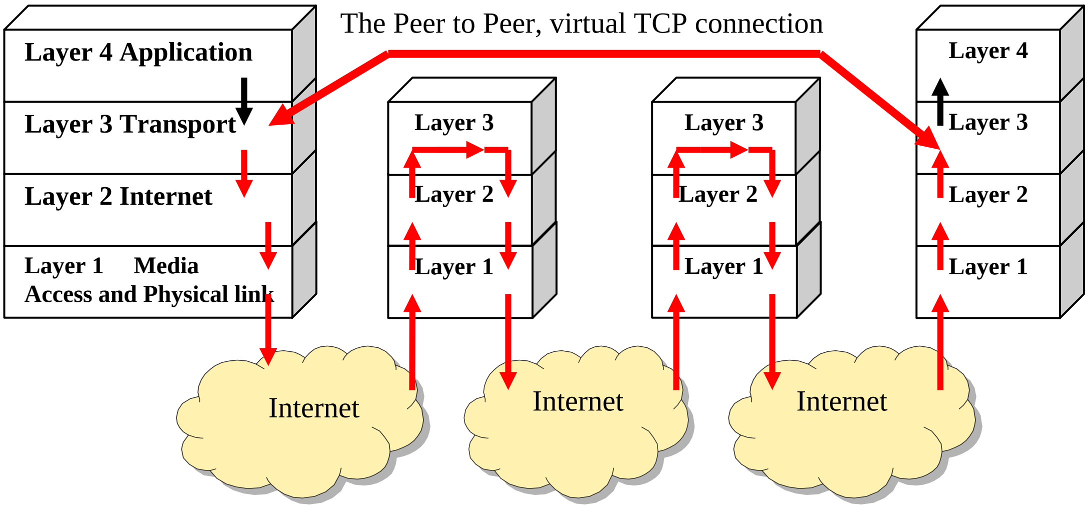


Fig. 2.1. Example: The TCP protocol assures the reliable, Peer to Peer, virtual connection, between the Layers 3 of the 2 machines, based on the practical, real connection through the chain of Layers of inferior rank and different Hops [5.].

As it results from the fig.2.1., the Data Packets use the path offered by different Hops (intermediary devices, such as routers, considered inside the clouds) and all the inferior Layers up to Layer 3. Based on this complex transmission, the virtual, Peer to Peer, connection between Layers 3 is achieved.

The configuration of the TCP Segment (Data Packet), including the Header and Data, is illustrated in fig.2.2.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">SOURCE PORT</td><td colspan="16">DESTINATION PORT</td></tr>
<tr><td colspan="32">SEQUENCE NUMBER</td></tr>
<tr><td colspan="32">ACKNOWLEDGEMENT NUMBER</td></tr>
<tr><td colspan="4">DATA
OFFSET</td><td colspan="6">RESERVED</td><td>U
R
G</td><td>A
C
K</td><td>P
S
H</td><td>R
S
T</td><td>S
Y
N</td><td>F
I
N</td><td colspan="16">WINDOW</td></tr>
<tr><td colspan="16">CHECKSUM</td><td colspan="16">URGENT POINTER</td></tr>
<tr><td colspan="25">OPTIONS</td><td colspan="7">PADDING</td></tr>
<tr><td colspan="32">DATA</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
</table>

Fig. 2.2. The Data Packet named Segment and elaborated by the TCP protocol on the Transport layer (layer 3).

The significations of the parameters from the Header of the TCP Data Packet are the following:

The TCP Header contains about 20 Bytes and includes, as it may be seen in figure 2.2.:

- **Source Port,**
- **Destination Port,**
- **Sequence Number,**
- **Acknowledgement Number,**
- Data Offset,
- Window (Window seize),
- Checksum,
- Urgent Pointer,
- Control Bits (Flags): U (URG); A (ACK); P (PUSH); R (RESET); S (SYN); F (FIN) End of Data.
- Other Information.

After the Header information follow the **Data** of the Data packet.

Please take into consideration that the TCP protocol does NOT place inside the TCP Header the IP Addresses.

The TCP Header contains the Source Port and the Destination Port, which are Ports Numbers (software virtual Ports of the protocols of Layer 4). These Ports are used for the de-multiplexing of the Data Packets sent by Layer 3 TCP toward the Protocols of Layer 4, Application.

The Port Number together with the Internet Address generate the **socket.**

The **Source Socket** is an identifier including both elements: IP Address of the Source and Source Port number.
The **Destination Socket** is an identifier including both elements: IP Address of the Destination and the Destination Port number.

Based on the **socket,** the respective Segment is correctly identified and directed inside the software packets which support the TCP protocol (at the Source and at the Destination).
Using sockets, the TCP protocol may process, in parallel, multiple segments.

The Sequence Number (fig. 2.2.).

The Number of Sequence presents importance in the reliability aspect and for the possibility to reconstruct the message from segments.
Each Segment, generated by Layer 3, TCP protocol, toward Layer 2, (and Peer to Peer, through virtual connection, toward Layer 3 of the interlocutor, respectively another Host) has its own Sequence Number.

At the reception, each Data Packet, under the form of a Segment, may be used, based on the Sequence Number, for the correct re-construction of the Message.

Also, through feedback from the Destination machine to the Sender machine and the manipulation of the Sequence Number, one may control the correct arrival of the respective Segment at the Destination machine.
In case of errors or loss of data packets, corrective means are used. One main corrective means consists in the re-sending of Data (through the sending of a new Data Packet).

Some remarks about the TCP Sequence Number:
Inside the TCP protocol, the definition of the sequence number is different from the definitions of other protocols.
Normally, inside **other** protocols, the Sequence Number is the number of the Data Packet.

Each TCP Segment has its own manner of formation of the Sequence Number, based on which, on reception, the Segment may be used in the correct re-construction of the Message.
The numbering of the TCP segments is based on the quantity (number) of bytes included.
If each Segment includes, for instance, 1000 Bytes , then the numbering of the Segments, based on the included quantity of Bytes, is the following [9.]:

- First Segment : Number 0
- Second Segment: Number 1000
- Third segment (of 1000 bytes): Number 2000
- …………….

Inside the TCP, the Sequence Number has a different formation manner and different significance (compared with the significance in other protocols).
Inside the TCP the Sequence Number corresponds to the total number of bytes sent, resulting from multiple Data Packets of one message.

Therefore:

- **when the Sequence Number belongs to the first (initial) Data Packet, this sequence number includes the respective number of Data bytes (of the correspondent Segment).**
- **when the Sequence Number belongs to a Data Packet in the string of Data Packets, then the Sequence Number contains the total number of bytes already sent (for the respective message) toward the Destination machine.**

The timing control.

At the start of the transmission of a Segment, the TCP/IP launches a timer.
If acknowledgment of the respective segment is returned by the Destination machine to the Sender (Source) machine within the pre-established time interval, then the segment is internally acknowledged by the initial Sender machine.
If acknowledgement does not return in time, then the Data Segment is re-emitted by the Sender machine.

The ACK- Acknowledgement Number.

For transmission reliability, the TCP protocol uses the acknowledgement of the received Packets of Data.

The acknowledgement is performed by the Destination machine by sending the feedback Data Packet toward the initial Source (Sender) Machine and the **PAR- Positive Acknowledgment Retransmission** procedure.

The **ACK – Acknowledgment Number** – represents a feedback indicator sent from the Destination machine to the initial Source machine (initial sender which has sent the Data packet), an indicator which informs about **the accumulated number of bytes achieved from multiple Data Packets received by the Destination machine**.

The **ACK – Acknowledgment Number** – is formed by summing the value of the number of bytes of the Sequence Number and the real number of received bytes (for one or more segments).

If the value of the ACK is for instance 2000, that means that 2000 bytes are received (in total, for the respective message divided into Segments).

The **ACK- Acknowledgment Number** is returned as feedback in the following form:

- The quantity of bytes received by the Destination machine, received through multiple Segments (multiple Data Packets) which are parts of a message.
- Therefore the Acknowledgment Number indicates the number of bytes which are already received by the Destination machine for one message (possibly through many Segments) and through one or multiple Data Packets.

- Since the Acknowledgment Number indicates:
    - the number of bytes which are received by the destination machine, and
    - because **this number of bytes represents the position of the next first byte to be sent**,

the Acknowledgment Number indicates the position of the next first Data byte to be sent.

This value corresponds to the number representing **the position** (number) of the first byte from the Data Packet which is expected by the Destination machine.
Therefore, in the TCP protocol, the Acknowledgement Number returned by the Destination to the Source represents the position (number) of the first byte from the packet of bytes which is expected by the Destination machine.

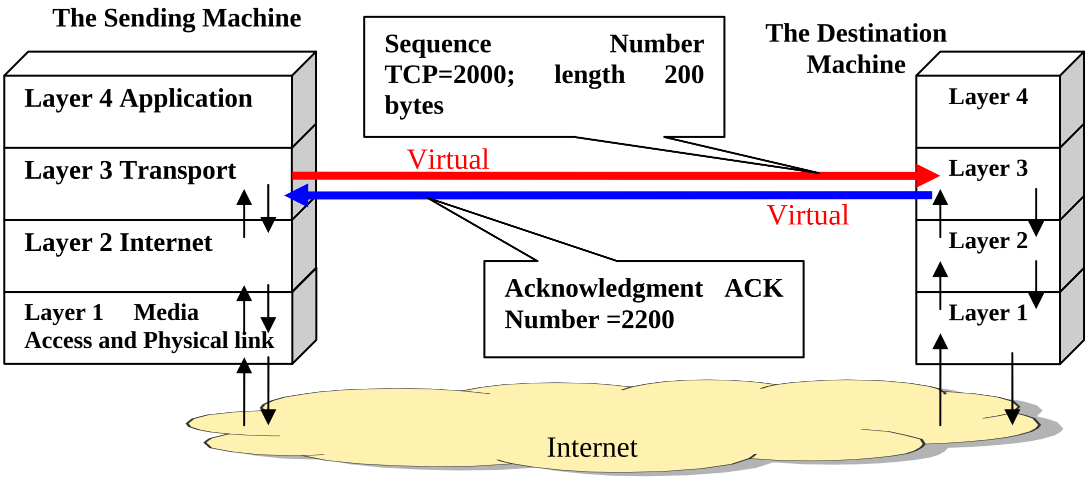


Fig. 2.3. The TCP sending of the Data Packet with the Sequence Number TCP=2000 (bytes) and with the length of 200 bytes. The Destination machine elaborates and sends one feedback consisting of the Acknowledgment Number ACK=2000+200= 2200 bytes.

Therefore the Destination machine informs the Sending machine which Data Packet's number is expected by the destination machine.

The important situation and the relation between:

- the Sequence Number and
- the Acknowledgement Number

is illustrated in the following fig. 2.3. (The channel is only virtual)

In this fig.2.3. the Sending machine sends the Segment having:

- the Sequence Number 2000 bytes, which signifies that the Source machine has previously sent, Data Packet by Data Packet, 2000 bytes toward the Destination machine and
- the length of the new sending (the Data Packet on the way) is of 200 bytes and

receives the TCP Acknowledgement Number 2200 which is the sum of the Sequence Number and the number of bytes of the last Data Packet.

The correctly received Segments (Data Packet) are acknowledged by the Source machine.

If the Source does not receive inside the precise time interval the Acknowledgment Segment, then the Source machine sends a new Data Packet, including the same Data and with a new Header.

The Data Offset.

The Data Offset indicates the number of words of 32 bits which compose the header of the TCP Data Segment.

The Flags have the following significance [5.]:

- U (URG) active indicates **Urgent Data**.
- A (ACK) active indicates that the Acknowledgement Number is valid,
- P (PUSH) active indicates the immediate transmission of Data toward the Layer of superior rank.
- R (RESET) active indicates the restart of one virtual circuit following an irreparable error.
- S (SYN) active indicates the opening of a virtual connection
- F (FIN) active indicates the closing of the connection.

The window (The window size).
The window size defines the number of bytes which are accepted by the Sender of the Data Packet.

The window size has an important role in traffic control, congestion avoidance and the adaptation to the speed accepted by the Destination machine.

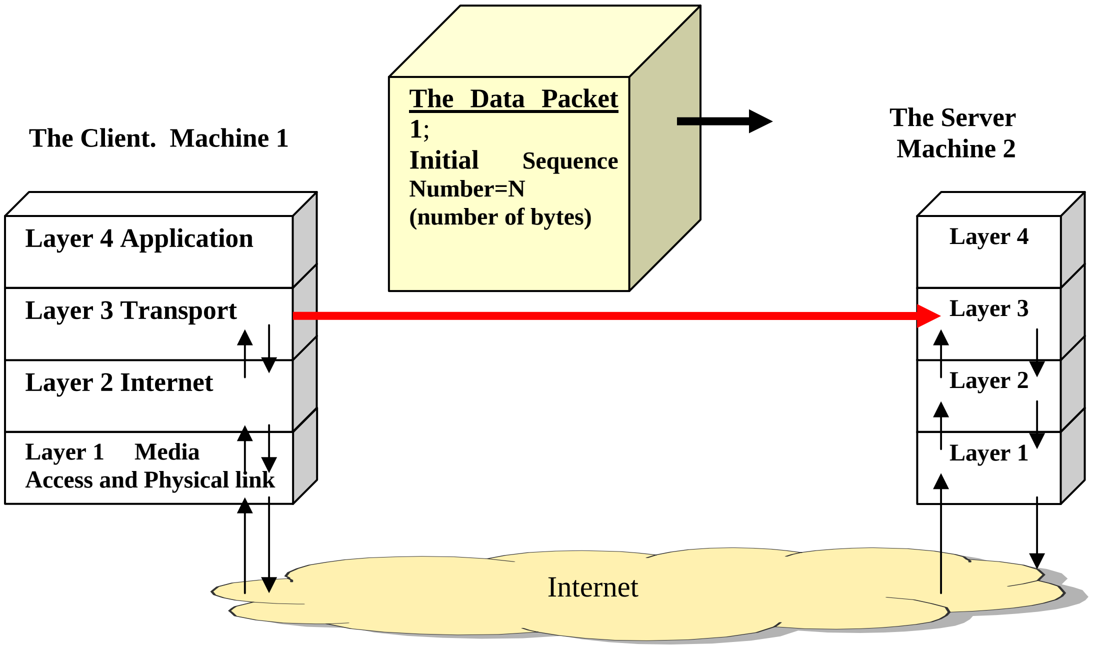


Fig. 2.4. **The Client sends a Data packet with the Sequence Number consisting in the number N of bytes (the number of bytes sent up to the respective moment)**.

If the number of the non-acknowledged segments is great, the TCP protocol diminishes the dimension of the windows and, as a consequence, it lowers the speed of sending the Data Packages.

<u>The Creation of a Connection between the Client and the Server. The Three Way Handshake procedure</u>

The Three Way Handshake procedure serves for the opening of a communication session, Peer to Peer, through virtual direct channel, between Layers 3 TCP of the 2 different machines.
The channel is only virtual and is, in reality, supported by the path including the Layers of inferior ranks of both machine and the intermediary Internet media.
The sequences of the **Three Way Handshake procedure** are the following:

A.) The TCP protocol (by the TCP protocol we understand the software package working based on the TCP protocol rules and inside Layer 3 Transport) of the Client sends to the Server a Segment named:
Open Flag, **Client Initial Sequence Number** (fig 2.4.).

By this he in fact asks (figuratively): “Is it possible to open the dialogue session with the Server?”

In the first sending the Client transfers the Data Packet 1 towards the Server (Machine 2).

The Sequence Number of this Packet is, for example: the number **N,** one number which represents the number of bytes already (previously) sent in this session.
On the first sending, the number of bytes sent initially (as a value considered in the number of bytes sent previously), is zero [the number of bytes already sent, previously, in this case is 0, because previously no bytes were sent. That is because this is the initial Data Segment (Data Packet)].

The Data Packet, named Data Packet 1, has (includes) Z bytes. They represent the code for the request of service from the Server.

B.) The Server, as it is illustrated in fig. 2.5., replies to Data Packet 1 through 2 Data Packets
Through this reply, the server said in fact (figuratively): “Yes, the opening of the dialogue session is possible”.
The 2 Data Packets by which the Server replies has the following details:

B.1.) the first Data Packet, named Data Packet 2, is a reply to the Machine’s Data Packet 1 and includes a

ACK Acknowledgment Number= (N+Z) number of bytes

where Z represents the number of bytes of received Data (from the Client’s machine) by the Server.

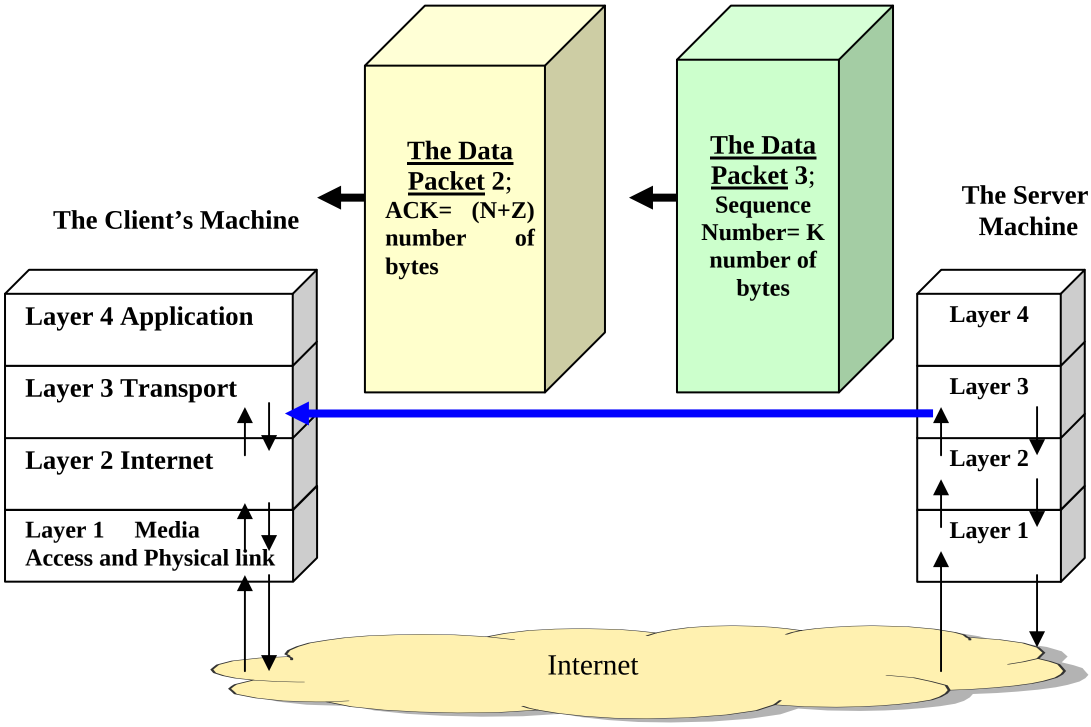


Fig. 2.5. **The Server replies with 2 Data Packets**.

B.2.) its own initialization (of the Server), Data Packet 3 having its own
Server Initial Sequence Number: K bytes (normally K=0), and including Y the total number of bytes.

C). The TCP protocol of the Client replies, as in fig. 2.6., to the Server Packet 3, with Packet 4, consisting in:
Acknowledgment Segment: **ACK= (K+Y) number of bytes.**

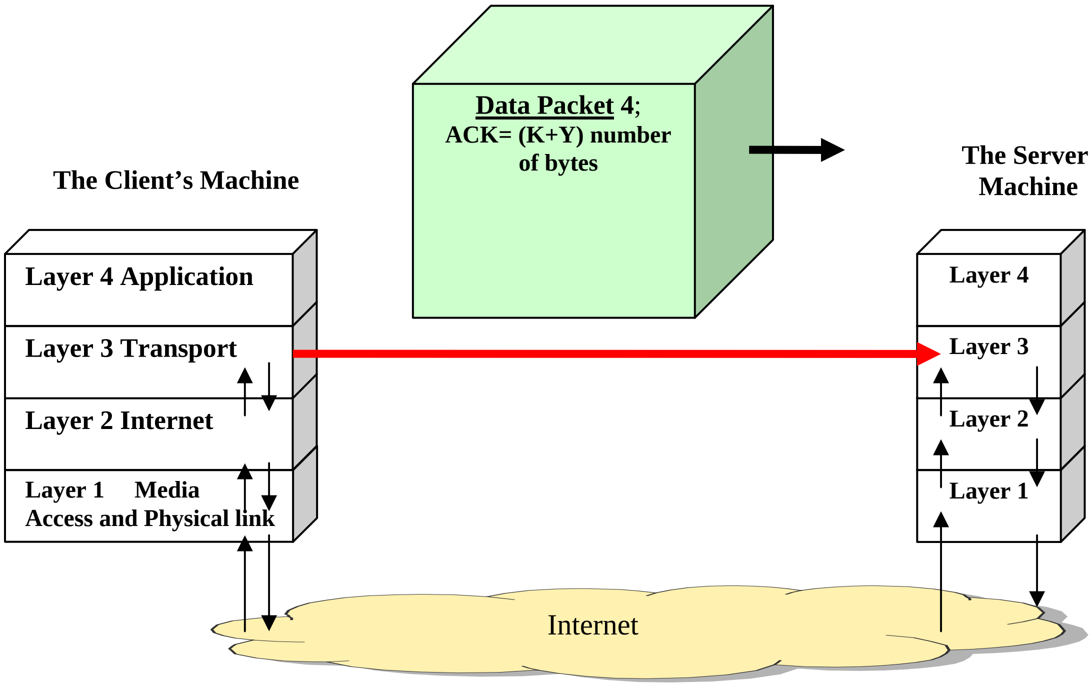


Fig. 2.6. **The Client sends a Data Packet (in response to Data Packet 3 from the Server) with the Sequence Number represented by the number of bytes (K+1)**.

Based on the **Three Way Handshake** procedure, the software package of the TCP protocol of the Client informs the TCP protocol (the software package inside the Server machine) of the Server about a possible communication between the Client and the Server. The Communication Session is open.
The basic idea of the **Three Way Handshake** consists in the opening and (after the convenient communication between the 2 machines) the closing of the virtual, peer to peer communication session.
The **Three Way Handshake** works by sending, by each of the 2 Peer to Peer partners, of feedback responses.

The Client and the Server respond one to the other, each by anew, personal **Sequence Numbers** and new **Acknowledgment Number** by processing the values of the respective arriving Data Packets.

The connection between the Client and the Server is open when, in the **Three Way Handshake**, each of the 2 partners receives the expected Sequence Numbers.

It is emphasized that this Peer to Peer conversation between the TCP levels (Layers 3) of the Client and the Server is, in reality, achieved by the direction and processing of the Data Packages through the layers of inferior ranks.

The Peer to Peer Exchange of the Data under the TCP monitoring.

After the establishment of the connection based on the ones described above, the **Three Way Handshake,** the virtual connection is open and prepared for exchanging Data.

If the Client's machine intends to send Data to the Server, based on the Data received by the Layer 3 Protocol TCP from the Application Layer 4, named Application, then the Client's machine, through the TCP protocol, creates new Segments. In these segments the above-mentioned rules are applied for the generation of new Sequence Numbers and new ACKs.

One example of running a numbering process between 2 machines is presented in the following Table:

Client's Machine	Server Machine
Sequence Number=0 (number of bytes) Length of sending (in number of bytes)=200 →	
←	ACK=200 in number of bytes
Sequence Number=200 (in number of bytes) Length of sending (in number of bytes)=200 →	
←	ACK=400 in number of bytes
Sequence Number=400 (in number of bytes) Length of sending (in number of bytes)=300 →	
Sequence Number=700 (in number of bytes) → Length of sending (in number of bytes)=200	
←	ACK= 900 in number of bytes
……………………………………..	

As it may be observed in the example above, an **ACK** responds to 2 **SN-Sequence Numbers**, respectively to 2 Data Packets. But, in this case, the ACK indicates the total number of bytes received and accumulated from all the received Data Packets, from the correspondent Client's machine.

The procedure allows the sender to transmit multiple packets before waiting for an acknowledgment.
In this way each TCP Segment is sent and received.

If a sent Data Segment (Data Packet) is not received in the established time interval, the segment is re-sent with the new Sequence Number and another Acknowledgement is expected.
After re-sending, with the established number of times, and non-reception of corresponding ACK, the system declares error or failure.

The repeated re-sending of Data Segments (Data Packets) improves the reliability of the Internet connections.

Closing of TCP connection.

The Application process (from Application Layer 4) of the Client closes the connection by giving the CLOSE information to TCP Layer 3 (Transport Layer).

Based on this information, the TCP Layer of the Client sends (through the inferior Layers of the Client's stack) to the TCP Layer 4 of the Server, a Data Segment (Data Packet) which informs about the closing of the connection.

The TCP Layer of the Server informs the Servers of the superior levels on the closing of the TCP connection and sends to the Client a Data Packet which informs the Client about the successful closing of the connection.
The TCP protocol: a protocol of the oriented-connection type.
The knowledge above illustrates the entire essential description of the functioning of the TCP protocol.
The TCP protocol is a **connection-oriented protocol** because it controls, through feedback, the correct arrival of the Data at each temporary Destinations.

2.2.) **THE TCP/IP Layer 3. TRANSPORT. The UDP Protocol**.

The TCP Protocol is **a connection oriented** Protocol.
That means that TCP Protocol supervises / controls and corrects the errors and the Data flux.

TCP offers the guarantee of the correct Data delivery.

But the efforts to guarantee the correct delivery of Data have led to time consumption (through more software instructions and time for software running in order to assure this control).

In contrast with the TCP Protocol, the UDP Protocol is faster, it has simplified error control and error treatment but **does not** offer the guarantee of delivery.
UDP is a Protocol also hosted by the Layer 3.
Because it does not supervise the correct arrival of data at the Destination, UDP is a protocol that is **not** oriented towards the connection **(connectionless oriented protocol).**

Following the elimination of the control of complex errors, the Header of the UDP protocol is very simple comparing to the header used by the TCP protocol.

The header of the UDP protocol contains only 4 fields, each of 16 bits and Data.

The UDP fields are the following:

- Source Port Number,
- Destination Port Number,
- The length in bytes of the UDP Data Packet.
- The Checksum.

3.) **The TCP / IP Layer 2. INTERNET . The IP Protocol**.

The IP protocol, described in RFC 791, performs:

- The preparation of the first level of virtualisation: the creation of the conditions of working with virtual addresses, the IP Addresses.
- In order to correspond with the IP protocol and IP Addressing, a logical, virtual representation of the Internet
- Network is created.
- The generation of the **connectionless procedure** of communication in which the Data Packets find the path from source to destination based on the cooperation between the Data Packet (which offers the IP Addresses) and the Routers, which direct based on the Tables of IP Addresses.
- The addition of the IP Header to each Data Packet, named, inside Layer 2, Datagram.

The IP protocol (which is a **connectionless-oriented protocol,** contrary to the TCP protocol which is a connection-oriented protocol) determines and facilitates the manner in which the Data Packets travel from the Source to the Destination, passing through different networks and Hops (Servers, Gateways etc).
The main tasks of this protocol are:

- to add to each Data Segment coming form Layer 3 above (TCP protocol or UDP protocol) the correspondent IP Header, including the IP Address of the Destination and IP Address of the Source and others, and
- to encapsulate:
  - the Segment provided by Layer 3, and
  - the IP Addresses of Destination and Source (and other Data) inside one new Data Packet named Datagram.

When the IP protocol, placed on Layer 2, receives from Layer 3 the Data Segment, it also receives the estimated, parameters of the QoS-Quality of Services, by Layer 3 TCP.

The IP protocol of Layer 2 functions based on the reliability assured by other protocols, respectively by the TCP protocol of Layer 3.

The IP protocol, being a connectionless protocol, does not assure the supervision and control of the arrival of the data packets at destination.

It is necessary to be understood that the word protocol signifies the viable software packages which process the Data.

The content of the IP Header is illustrated in fig. 2.6.
It is important to emphasise that the elements which are used by the Data Packet to find the path from Source to destination, respectively the IP Address of Destination and the IP Address of the Sender are present inside the Header of the IP based Data Packet.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="4">VERSION</td><td colspan="3">IHL</td><td colspan="10">TYPE OF SERVICE</td><td colspan="15">TOTAL LENGTH</td></tr>
<tr><td colspan="17">IDENTIFICATION</td><td>0</td><td>DF</td><td>MF</td><td colspan="12">FRAGMENT OFFSET</td></tr>
<tr><td colspan="8">TIME TO LIVE</td><td colspan="9">PROTOCOL</td><td colspan="15">HEADER CHECKSUM</td></tr>
<tr><td colspan="32">SOURCE ADDRESS</td></tr>
<tr><td colspan="32">DESTINATION ADDRESS</td></tr>
<tr><td colspan="26">OPTIONS</td><td colspan="6">PADDING</td></tr>
<tr><td colspan="26">……………………………………………………………………………………………………</td><td colspan="6">……………………...</td></tr>
<tr><td colspan="32">DATA
……………………………………………………………………………………</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
</table>

Fig. 2.6. **The IP Data Packet (datagram) including Data**.

The significance of the parameters of the Header of the IP datagram is the following [5.]:

- Version indicates the type of protocol, for instance:
  - IPv4 is indicated by 4
  - IPv6 is indicated by 6
  - Other possibilities.
- The IHL-Internet Header Length indicates the lengths of the header in words of 32 bits.
- The TOS, 8 bits, indicates the Type of Service to the network and to other entities [5.]:
  - A. Field of first 3 bits (Field precedence):
    - Routine, up to tomorrow, (value 000),
    - Priority, in the same day (value 001),
    - Immediate, in 4 hours (value 010),
    - Flash (value 011),
    - Flash override (value 100),
    - Critical (value 101),
    - Internet work control (110),
    - Network control (111).
  - B. Field TOS of TOS, 4 bits:
    - Minimum delay (value 1000),
    - Maximum debit (value 0100),
    - Maximum reliability (value 0010),
    - Minimum expenses (value 0001),
    - Normal service (value 0000).

  - C. MBZ for future developments.

- The Data Packet's entire length includes two main parts:
  - the Header,
  - the Data,

and the length may have a maximum of 16 bits, that is, the maximum value of 65,535. This value represents the maximum value acceptable from the point of view of the parameter Total Length.

Other supplementary constraints limit the MTU - Maximum Transfer Unit of the IP Data Packet:

Ethernet	to 1500 bytes,
IEEE 802.3	to 1492 bytes.

The normal dimension of the Datagram is of 16 Kbytes.

The **minimal** length of the Datagram is of (512 Bytes for Data + 64 Bytes for Header) =576 Bytes.

- The identification field: includes the Number of the IP Datagram (for instance, in a communication, from the Client to Server: 5,6,7,8, etc; from Server to Client: 501,502,503, 504 etc).

- DF signifies: DO NOT FRAGMENT THE DATAGRAM.
- MF signifies: MORE FRAGMENTS.

- The Fragment Offset indicates the offset of the fragments (position of Data in relation to the starting point of the original Datagram) in order to reconstruct the datagram from fragments (after the fragmentation processes, where necessary).

- TTL –Time to live: the lifetime allowed for the Datagram, normally in seconds and with the standard values 32 seconds or 64 seconds.

Normally each Hop extracts one unit from the TTL. Following this aspect the TTL is also one counter of HOPs.

- The field protocol: indicates the type of the protocol used in the layer of the superior rank, for instance:
  - for TCP, value 6,
  - for UDP, value 17.
  - Other hundreds of values for other protocols or significations.

- The field Header Checksum: indicate the sum of control of the header and is applied to the IP protocol.
- Since, in each Hop, the TTL is diminished by the value 1, the header Checksum must be recalculated.

- The IP Source and Destination Addresses.

- The field OPTIONS includes the options:
  - **Security**, with the possible taking into consideration of:
    - Basic security, such as:
      - Confidential,
      - Non-classified,
      - Secret,
      - Others
    - Other supplementary security
  - **Record Route**, it offers the possibility for the Data Packet to register the IP addresses of the routers of the path traversed by the Data Packet from the Source to the Destination.
  - **Strict Source Routing**, it offers the IP Addresses of the routers on the pre-established path from Source to Destination. Routers which are not in the list are not accepted.
  - **Loose Source Routing** works in a similar manner as the Strict Source Routing presented above, with the difference that between 2 imposed Routers, the Data packets may travel through other, non-nominated Routers.
  - **Internet Timestamp** registers the time of the reception of Datagram by each Router.

With the addition of this IP header, the Data Packet receives the IP addresses of the Source and of the Destination and other information.

Having the IP address of the Destination the Data Packet under the name Datagram is passed to Layer 1.

The IP protocol, a **connectionless** protocol (in contrast with the **connection-oriented protocol** achieved in Layer 3 by the TCP protocol), does not achieve an **end-to-end connection** before the time of transmission of Data.

The Data Packet will find the path toward the destination by itself, based on the virtual IP Address and on the cooperation with the tables of addresses and directions placed in the Routers.

The TCP / IP Layer 2 Internet provides the software means for the achievement of the above tasks.

4.) The TCP / IP Layer 1. NETWORK ACCESS.

The TCP/IP Layer 1 works for and with the physical network and **with the physical addresses**.
The TCP /IP Layer 1 works inside the basic, local network, normally the basic LAN (for the great majority of the Ethernet type).

The Data Packets processed inside the protocols of Layer 1, and placed in serial form (serialised) on the physical transmission media (for instance cables) are named Trams.

At the TCP/IP Layer 1, the Protocols of this Layer perform at the sending of the Data Packets toward the network:

- The reception of the Data Packets, each under the form of Datagram, from Layer 3 above.
- The processing of the received Datagram, in order to be delivered, serialized, to the physical media, as Trams.
- Other functions.

Many physical networks and digital communications are based on the use of the Ethernet Protocol.
The Ethernet Protocol is a protocol hosted and used in Layer 1, Network Access.

The protocol of Layer1, Ethernet 802.3 protocol, adds the Ethernet Header to the Data Packet.
This new, supplementary Header includes the Ethernet address (Physical address) of the Destination and the Ethernet address (Physical address) of the Source / Sender.

These Ethernet addresses are **the physical** (MAC – Media Address Control) addresses of Destination and respectively of the Source.

The TCP / IP Layer 1, Network Access, provides the software means for the achievement of the above and other tasks.

The Network Access protocols of the TCP / IP Layer 1 are improved and adapted in accordance with the appearance of new types of interfaces or new hardware technologies, so that the TCP/IP is compatible with all types of interfaces and communication media.

The TCP / IP Layer 1, Network Access is defined in RFCs (requests for Comments), for instance in:

- RFC 826: *Address Resolution Protocol (ARP).* The RFC 826 specifies the mode and the procedure of the accomplishment of the Ethernet, physical and existent addresses, when the IP addresses of the devices of interest are known.

Where IP are virtual addresses which allow the finding of the path toward the destination, at the passing of the serialized Tram through multiple, different networks and Hops, the physical address allows the transmission of the serialized Tram between the devices connected to the same network LAN-Local Area Network.

Somebody must perform the correspondence between the IP Addresses and the Physical addresses.
Following this correspondence it is possible to access the NICs from the Ethernet LAN. Definitions in RFC 826.

- RFC 894: *A Standard for the Transmission of IP Datagrams over the Ethernet Networks.* The RFC 894 specifies the mode of encapsulation (formation) of the Data Packet in order to be transmitted through the Ethernet Networks.

The detailed and practical presentation of the Ethernet is achieved in the following lessons dedicated to the LANs.

3. THE SUCCESSIVE ENCAPSULATION OF HEADERS AND DATA IN THE CREATION OF THE TCP / IP PACKETS.

Fig. 3.1. illustrates the manner of formation of the Tram starting from the Message / File transferred from the TCP / IP Layer 4 Application to the TCP / IP Layer 3 Transport.

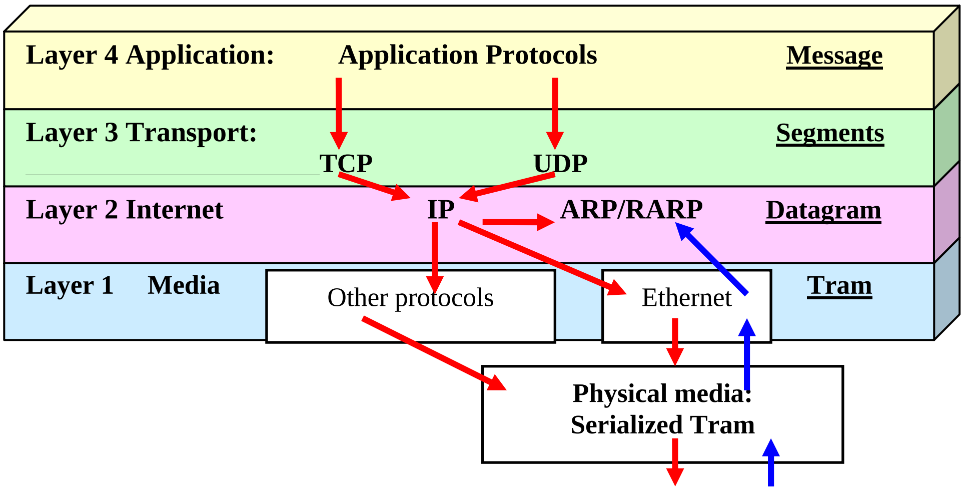


Fig. 3.1. The conversion of the Data Packets

The Data is converted in the following forms:

- Message, received from the machine programs,
- Segments, representing the parts in which the message is cut, in Layer 3, with the TCP corresponding Header,
- Datagram, representing the result of processing by the IP protocol of Layer 2, and the addition of the IP Header.
- Tram as the result of the processing of the protocol from Layer 1.

The Message. The Message (file) is sent by Application Layer 4 to Layer 3 Transport.
The Segments. In the TCP / IP Layer 3 Transport the Segments are generated under the TCP protocol, as part of message. The correct transmission of these segments is under the control of TCP, a connection oriented protocol.
The Datagram. The Segments are transferred to the TCP / IP Layer 2 Internet, where a Datagram is generated from each Segment. In Layer 2 Internet each Datagram receives the IP header including IP virtual Addresses (of the Destination and of the Source) and other parameters.

The Tram. The Datagrams are transferred, each, to TCP / IP Layer 1 Network Access. From each Datagram one Tram is generated, in correspondence, with the inclusion of the physical network header (for instance Ethernet Header if the Ethernet network is used).
The Tram includes information about the Physical address of the Local Destination. This Local Destination represents the Physical address of one partner of the same LAN. If the Internet is targeted, the Tram includes the Physical address of the Gateway by which the Data Packets are transferred toward the Internet network.

If the machine (TCP /IP suite of protocols) knows only the IP Address then the Physical address is accomplished through the ARP – protocol (Address Resolution Protocol). The Physical Address is necessary for layer 1 but it is accomplished by the ARP protocol placed in Layer 2 (fig.3.1.).

The Tram, under serialized form, is sent to the physical media.

The preparation of the Data Packets, Layer by Layer, under the TCP / IP protocols, is edited and illustrated in fig.3.1.

Also in fig. 3.1. the following aspects are emphasised:

- The Layer 4 Application sends the Data (according to the process / commands needs) towards one port which represents the entry to either of the protocols TCP or UDP placed on Layer 3 – transport.
- The Segments of the TCP or UDP protocols are sent to the IP protocol from Layer 2 Internet.
- The Layer 2 Internet also includes other important protocols: ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol) which offers the equivalence between IP Address and the Physical Address and vice-versa.
- The layer 1 includes the protocols for working with the physical level, with the MAC / Physical Addresses.

4. THE TCP/IP FUNCTIONING AT THE RECEPTION OF THE DATA PACKETS.

The process of the step by step, layer by layer processing and sending of Data Packets is illustrated in fig. 4.1.

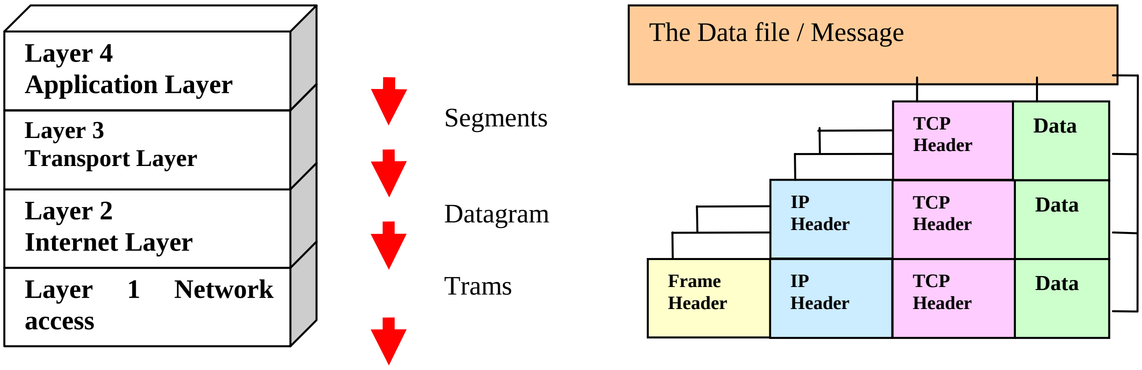


Fig. 4.1. The formation step by step of the Segments, Datagram and Trams and of the related Headers at the Source, in order to send the Data packets.

In comparison with the sending process, at the receiving of the Data Packets the processes are reverse:

The Data Packets, named trams and including corresponding Physical address arrive at the entry of the NIC of the machine

The Data Packets, under the form of the serialized Trams, generate the correspondent packets inside the TCP / IP Layer 1.
The Trams are transferred, one by one, to the TCP / IP Layer 2 Internet, where the multiple Datagrams are formed (from each Tram one Datagram).
The Datagrams are transferred, one by one, to the TCP / IP Layer 3 Transport, where each Datagram generates one Segment.
From the Segments the Message is re-constructed and is offered to TCP / IP Layer 4 Application.

Fig. 4.2. illustrates the reverse process by which the message is reconstructed, step by step, passing through the phases: Trams, Datagram, Segments, Message.

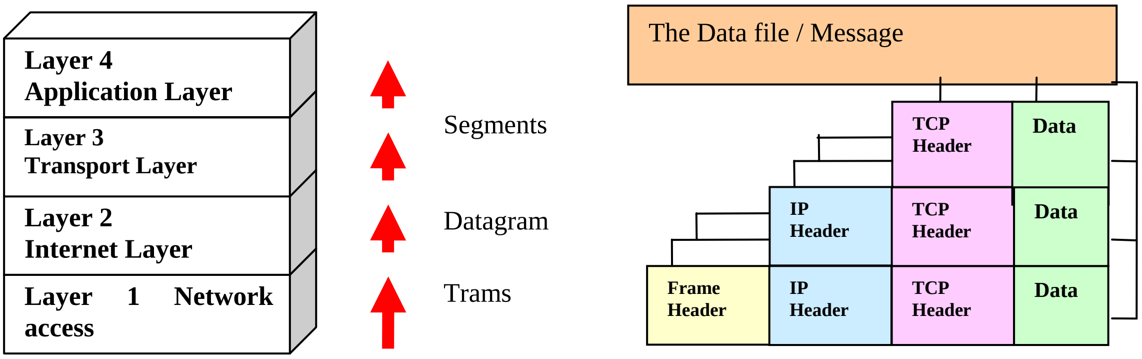


Fig. 4.2. The re-formation of the message, step by step at the Destination.

The entire process, send-receive, between 2 TCP / IP implementations, and the correspondent multiple encapsulation / de-encapsulation of the data is illustrated in the following fig. 4.3.

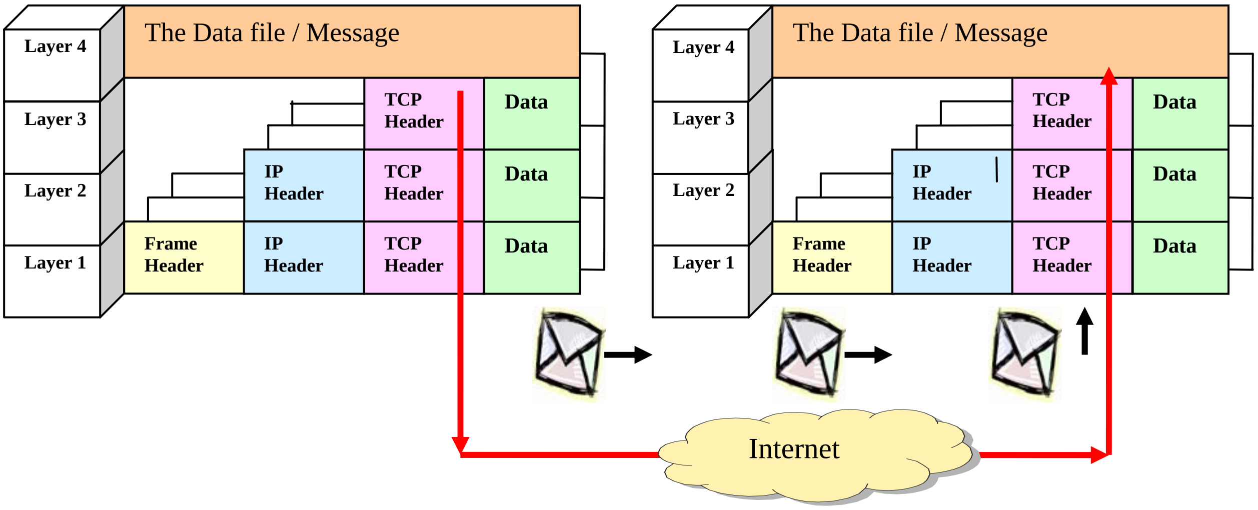


Fig. 4.3. The entire process of generation of the Segments, Datagram and Trams and of related Headers at the Source and the re-conversion Trams, datagram Segments, Message at the destination.

The Data Packets do not arrive synchronously, nor in the sending order.
It is possible that the first Data Packets arrive after the Data Packets which are sent later.
Part of the Data Packets may be lost or altered in content, so that the TCP/IP protocols require a new sending of Data etc.

Therefore, the reconstruction of the Message is not a simple task. The reconstruction of the Message includes multiple “try again“processes. In the “try again“processes, the system may request the retransmission, as illustrated above.

Key Point Summary Conclusions and Recommendations

- The Internet functions following the clear TCP/IP division of the functions, on 4 Layers and on protocols placed on these Layers.
- The functions are allocated to the protocols placed on the Layers. The functions achieved at the level of each layer are focused on the specific fields.
- The reliability of Internet is accomplished through the use of multiple controls, “try again” and error correction.
- The reliable arrival of the Data Packets at the destination is accomplished through the use of the connection-oriented protocol, TCP which uses the specific feedback from the destination machine.
- The encapsulation of the Data Packets and of the specific header of the Segments, Datagram and Trams leads to the construction of the complete and complex Data Packets which join:
  - the work with the Physical Addresses (in the local network),
  - the work with the Virtual IP Addresses for the creation of the conditions so that the Data Packet is directed toward the Destination,

- the construction of reliable communications, switching packets technology, through the use of adequate feedbacks and corrections.

Study Guide

ESSENTIAL QUESTIONS TO EVALUATE THE ACQUIRED KNOWLEDGE

1. Which are the TCP/IP essential Layers and which are the most important protocols placed on each Layer?
2. Which are the essential features and the functioning of the TCP/IP Application protocol?
3. Which are the essential features and the functioning of the TCP Transport protocol?
4. What is the one protocol of the connexion-oriented type protocol?
5. The UDP, TCP and IP protocols are connection oriented or connectionless protocols?
6. Which are the essential features and the functioning of the TCP/IP IP protocol?
7. Which are the essential features and the functioning of the protocols of the Layer1?
8. How is it achieved the reliability of Internet related to the confirmation of the arrived Data packets at the Destination machine?
9. What is the Three Way Handshake procedure?
10. At the sending of the data Packets between one Client and one Server, at the Server arrives one data packet having the Sequence Number 1500 bytes and the length 5000 bytes. Which will be the value of the ACK-Acknowledgement Number?

BIBLIOGRAPHY. REFERENCES.

[1.] Ron Gilster: *Cisco Networking for Dummies*, 2nd Edition, Wiley Publishing, Inc, 2002, 0-7645-1668-X.
[2.] Joe Casad: *TCP / IP*, Campus Press, Paris, 2002, 2-7440-1501-6.
[3.] Tim Parker, Mark Sportack: *TCP / IP* , Teora, Bucharest, 2002, 973-20-0243-3.
[4.] Candace Leiden , Marshall Wilensky: *TCP /IP for DUMMIES*, 5-th Edition, Wiley Publishing, Inc, 2003, 0-7645-1760-0.
[5.] Karanjit S. Siyan: *TCP/IP* CampusPress, Paris, 2002, 2-7440-1562-8 ,
[6.] Lukas T. Gorys: *TCP/IP Arbeitsbuch*, Huthig Buch Verlag Heidelberg, 1989, ISBN 3-7785-18884-4.
[7.] Andrew S. Tanenbaum: *Computer Networks*, 4th ed., Pearson Education, Inc, Prentice Hall PTR , Upper Saddle River, New Jersey 07458,2002, translated in Romanian and edited by BYBLOS s.r.l., Bucharest,2003, under the ISBN 973-0-03000-6.
[8.] Gilbert Held: *Ethernet Networks*, John Wiley and Sons Ltd, England, 2003, ISBN 0-470-844476-0
[9.] Lukas T.Gorys: *TCP /IP Arbgeitsbuch. Komminkatiosprotocolle zur Datenübertagung*, Hüthig Buch Verlag Gmbh, Heidelberg, 1989, 3-775-1884-4.
[10.] Douglas E. Commer: *Internetworking with TCP/IP* , Fifthy edition, Pearson, Prentice Hall, 2006, 0-13-187671-6.
[11.] Joe Habraken: *Absolute Beginners's Guide to Networking*, QUE, Indianapolis, Indiana, 2004, 0-7897-2911-3.

IMPORTANT SUPPLEMENTARY BIBLIOGRAPHY. REFERENCES. (www)

[Supplem. 1.] http://www.prenhall.com/tanenbaum, Prentice Hall, Andrew S. Tanenbaum
[Supplem. 2.] www.cisco.com/univercd/cc/td/doc/cisintwk/idg4
[Supplem. 2.] www.cramsession.com

SUPPLEMENTARY INDICATIONS ABOUT THE CONTENTS OF THE LESSON

It is recommendable to be consulted also the documentations from: www.cisco.com; www.cramsession.com; RFC: www.ietf.org ; www.rfc-editor.org.

ANSWERS TO QUESTIONS

1. The TCP/IP Layers are: 4.- application, 3.- transport, 2.- Internet, 1.- media access. The important protocols are, for instance; on the Layer 4: HTTP, FTP, Telnet, SMTP, POP3, ICMAP4 and other, on the Layer 3 TCP and UDP, on the Layer 2 IP and ARP, and on the Layer 1 Ethernet and other.
2. The Application protocol includes functions of the high rank such as the achievement of the navigation, sending of e-mails, and other.
3. The TCP/IP Transport protocol is one connection oriented protocol. It achieve the dividing of the Message, coming form the Layer 4, in Segments, create the encapsulated segments including the TCP header, achieves the supervising of arriving of the Data Packets at the destination, accomplishes the reliability of the Internet transmission, based on the feedbacks packets, open and close the sessions of communication between Client and Server.
4. One protocol which is not indifferent at the mode in which the packets arrive at the destination and consequently achieves the control of the arriving of the packets at destination, based on the using of the feedback information.
5. The UDP and IP are connectionless protocol and the TCP is connection oriented protocol.
6. The IP protocol prepares the conditions for the travel of the Data Packets through the Internet networks, through the creation of the new data Packet named datagram, and introducing of the IP header including the IP Address of Destination and of Source.
7. It assures the sending and receiving of the data packets at the level of the physical network..
8. The reliability is achieved through feedbacks. At each or at multiple arrived packets, the destination machine sent one Confirmation Packet toward the source including the own (of the Destination machine) Sequence Number and the ACK-Acknowledge number which inform the source about the number of bytes which have received by the Destination machine. If the ACK do not arrives, in the pre-established time interval, at the Source, then the Source sends one new Packet with Data.

Based on this procedure the number of bytes arrived, in good conditions, at the Destination are continuously supervised.

9. It is one procedure, by which the Client requires, opens, solves and close, in cooperation with the Server, one session of dialogue with the Server.

The procedure is based on the exchange of data packets between the client and Server.

10. 6500.

WORDS TO THE LEARNER: ***"… it is not required that you have the collective intelligence of all the network pioneers to be a network administrator"*** [11.].