Computer Networks and Distributed Systems

Reference Solutions to Questionnaire no. 2 on the Foundation Chapter of CN

Context

- paloalto.unileon.es/cn under the heading "*Chapter 1: Foundation*"
- paloalto.unileon.es/cn under the heading *"Chapter 1: Brief notes on basic network performance and solved exercises*" which points to http://paloalto.unileon.es/cn/ComplNotesCN.Ch1.pdf

1. Depict a diagram that establishes the correspondence between the layers of the OSI and the Internet (TCP/IP) Architectures

```
OSI architecture        TCP/IP architecture
================        ===================

-----------------       -------------------
7 – Application
6 – Presentation        4 - Application
5 - Session
-----------------       -------------------
4 – Transport           3 – TCP or UDP
-----------------       -------------------
3 – Network             2 - IP
-----------------       -------------------
2 – Datalink
                        1 - Subnetwork
1 – Physical
-----------------       -------------------
```

2. Beyond the fact that the OSI and TCP/IP architectures have different numbers of layers, what do you think is the most important difference between them?

   A notable difference between the two architectures is that the OSI architecture enforces strict layering and TCP/IP doesn't. There are other differences.

3. Execute ping against an Internet host that does respond to ICMP echo messages (For example, www.cisco.com), then, start a Wireshark trace of the messages interchanged by your host and the remote host. You may want to display the ICMP messages only by specifying the following protocol name within the textbox: "icmp". After capturing a few frames, stop the trace and select any one of them and, according to the results you see on the screen, depict a protocol graph containing all the protocols involved. You have an example of a protocol graph in fig. 1.14 on the textbook.

   Fig. 1 contains a screen dump where you can identify the shell where I executed ping against www.unileon.es on the left and, on the right is the Wireshark capture of the interchanged frames. Identify the following relevant facts about it:

   - The "icmp" display filter specification was entered into the green-colored textbox, thus,

Wireshark will only display frames containing ICMP messages as the application payload

- Frame number 522 was selected, which causes its information to be displayed on the lower, white-colored pane
- Physical frame 522 (Layer 1) is 98 bytes long and contains an Ethernet II frame
- The Ethernet II frame is sent by MAC 70:56:81:… and it is received by MAC 14:10:9f:… (These MACs correspond to hosts belonging to the same local network). This Ethernet II frame contains an IP packet
- The IP packet was sent by 193.146.99.17 and it was received by 192.168.2.107 (These IPs correspond to the host that sent the IP packet and the host it was sent to; both hosts are reachable in the Internet). The IP packet contains an ICMP protocol message
- The ICMP message is an echo reply message

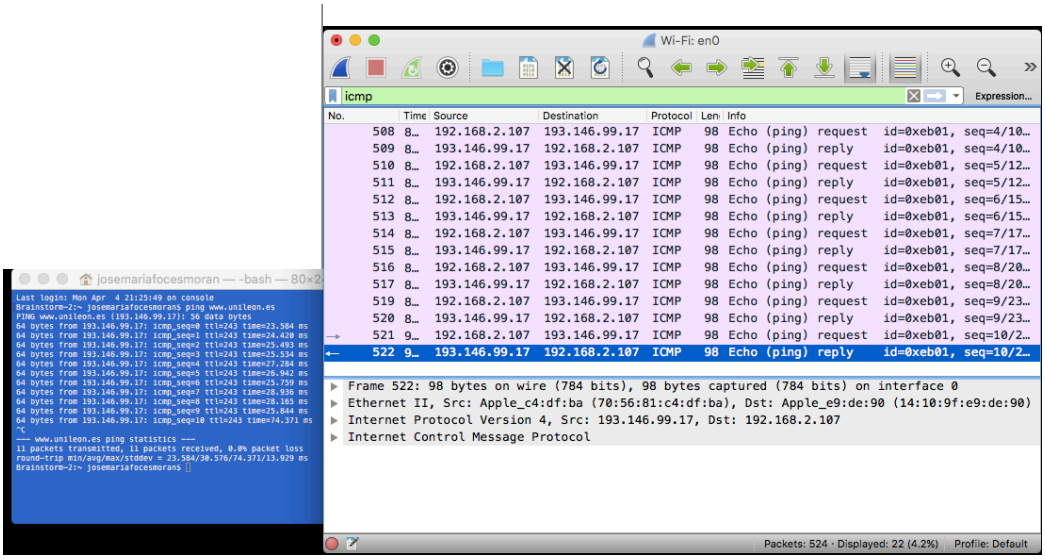


Fig. 1. Wireshark capture of a few pings

Using the information in the bullet list above, we derive the following protocol graph:

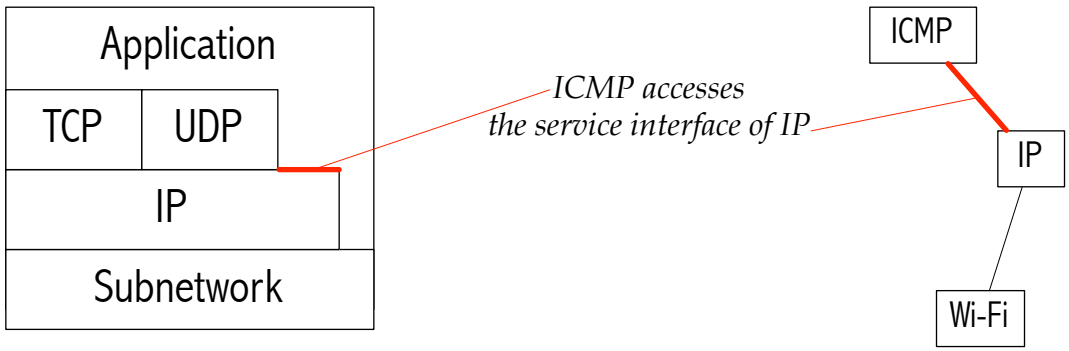


Fig. 2. The ICMP protocol graph

The ICMP protocol uses no transport protocol for encapsulating the messages sent, it simply composes a new message and submits it directly to IP for transmission over the internetwork, bypassing any transport protocol altogether. This is acceptable of the Internet Architecture where an application can select the service interface of any layer below; by contrast, in the OSI architecture, an application can only access the service interface of the presentation/session layers since layering is strict there.

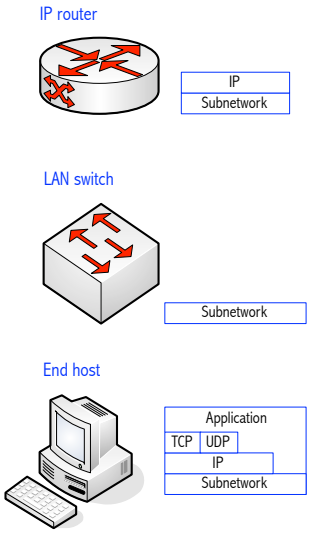
ICMP is an application protocol complementary to IP, which implements its own particular kind of transport, other than TCP or UDP. We will see this in more detail in the lectures in chapter 3, soon. For the time being, it suffices that we observe some application protocols use none of the established transport protocols, though this not the norm. Nevertheless, we must emphasize that ICMP is a required protocol for the correct operation of the TCP/IP architecture. Observe that the Wireshark representation of the physical frame (Frame 522: 98 bytes on wire …) and its representation of the datalink frame (Ethernet II, Src: Apple_....) are collapsed into the single subnetwork layer protocol named Wi-Fi on the protocol graph.

4. Consider the TCP/IP architecture for this question; in TCP/IP, any layer exports two interfaces, one to its upper layer and the other to its remote counterpart, what are the technical names of these two interfaces?

The interface between a layer and its local layer right below is known as *service interface.* At any layer n considered, the interface between the two layer-n protocols, one at the transmitter and the other at the receiver, is known as *peer-to-peer interface.* This interface is comprised basically of the set of the legitimate messages interchanged between the transmitter and the receiver.

5. Which TCP/IP layers are implemented in a host? And, which are implemented by a LAN switch and by an IP router?

A host needs all the four layers for communicating with another host in the Internet. An application running in a host sends messages by using a transport protocol, which subsequently calls IP so the messages are added the source and the destination IP addresses, last, each IP packet is sent from the host to its first IP router by means of a LAN. The LAN is made up of a number of switches, therefore, the travel from the host to the router will be composed of a sequence of switch-to-switch links; the addresses that identify the host and the router within the LAN are known as MAC addresses and they constitute a basic aspect of the subnetwork layer. All in all, a host must implement all the four layers.



Switches only implement the subnetwork layer since their mission consists of forwarding a frame from switch to switch as the frame travels from the host to the router within a LAN.

The mission of an IP router consists of forwarding IP packets between networks connected to it, to that purpose, a router must handle IP addresses which are meaningful in the internet, therefore, a router implements the subnetwork and network layers.

6. Explain what is multiplexing and encapsulation and what role each concept plays in network architecture

The Internet may be contemplated as a resource shared amongst all the hosts connected to it, thus, the packets of information sent by any host must include addresses that identify the sender and the receiver. A host *multiplexes* packets over the internet by using Ip addresses.

Also, notably, when a packet reaches its destination host, its payload is delivered to a specific process running in the receiver host's operating system, *i.e.*, it is *demultiplexed*, in this case by using port numbers which are *multiplexing keys* at the transport layer.
In summary, IP addresses constitute a *multiplexing key* that allows an IP packet to use the internet

(A shared communication resource) for reaching a destination host. Port numbers constitute a *multiplexing key* used for delivering the application message contained in an IP packet to one of the many running processes in the IP packet's receiving host.

A client application C generates some message M directed towards a server application S running at a host in the internet. C uses a transport protocol, UDP for example, which will add some control information to M, specifically, it will add two port numbers (Source port number and destination port number) used for identifying the sending process and the receiving process in the destination host. The resulting UDP datagram *encapsulates* M. UDP now calls IP for having the datagram sent, *i.e.,* IP *encapsulates* the datagram into an IP packet by appending the source and destination addresses to the datagram.

7. What international institution is responsible for the TCP/IP architecture?

   IETF (Internet Engineering Task Force) is responsible for the development of the TCP/IP architecture.

8. Did you already study ch.1 ex. 4.a and 4.b? If so, now we request you to calculate the throughput attained in each case. **Throughput** means the effective performance attained, that is, considering only real user data transferred from end to end (From host to host).

   Throughput is a performance metric, in general it means a number of operations completed per unit time. The operations, for example, could be the mean number of instructions executed by a microprocessor per unit time. In the case of this exercise, *throughput* represents the mean number of bits transferred from host A to B. In ex. 4.a, the throughput is roughly equal to the transmission bandwidth, due to the initial handshake, which consumes two Rtt. In the present case, ex. 4.b, since the transmitter is inserting a wait time of 1 Rtt after transmitting each packet, it's easy to see that the throughput will be much smaller than in 4.a. since the amount of effective, user information is the same (1.5MB) but the transfer time is substantially larger:

   ```
   Throughput    = Number of bits transferred / Total transfer time
                 = 1.5·8·2^20 bits/ 124.258 s
                 = 101.26 Kbps
   ```

9. Check the pdf document mentioned above about Network Performance (http://paloalto.unileon.es/cn/ComplNotesCN.Ch1.pdf) and study all the exercises solved in it. We already worked 4.a and 4.b in the exercises sessions of 17/3 and 18/3. In the case of ex. 4.b, please, note that the explanation I provided you in the lab is easier to grasp than that included in the pdf document.

The adjoining figure further explains the solution to this exercise included in the textbook (P&D, pg. 801). This strategy results more intuitive and easier to grasp than the one developed in the pdf document mentioned above. In this case, for computing the total time it takes to transfer the 1.5MB file we focus on the timeline of the transmitting host A. We first obtain the formula that represents the total file transfer time:

$$T_{total} = \text{Initial Handshake} + (T_{TransmPack} + Rtt)\cdot(Npack - 1) + T_{TransmPack} + T_p$$

The meaning of each of the variables is the following:

- Initial Handshake. Per the exercise statement we know this term takes a time equal to 2 x R_{tt}
- $T_{TransmPack}$. This is the time it takes to transmit
- N_{pack}. The total number of packets comprising the file
- T_p. The propagation time of the link used for directly connecting A and B

The first term is the initial handshake, after which we repeatedly transmit one packet and next we wait a full R_{tt}; this pattern is repeated (N_{pack}-1) times since no wait is needed after the last packet. Lastly, we transmit the last packet, which consumes a time equal to $T_{TransmPack}$. Finally, we should observe that, when the last packet has been transmitted (Observe the figure at label Packet Npack transmitted), the last bit still has to propagate from A to B, which takes T_p seconds. Label Packet Npack fully transferred represents the time point where all the file bits have been successfully transferred to host B.

I suggest you perform the arithmetic calculations and check the result against the textbook. Proceeding all the way through the correct final result is a nice check of your understanding of this exercise. Please, recall I performed all the arithmetic calculations on the chalkboard.