Network & Operation Systems Essentials

Dr Nikos Ntarmos

Joao Almeida-Domingues[*]

University of Glasgow

September 24th, 2018 – December 4th, 2019

Contents

These lecture notes were collated by me from a mixture of sources , the two main sources being the lecture notes provided by the lecturer and the content presented in-lecture. All other referenced material (if used) can be found in the *Bibliography* and *References* sections.

The primary goal of these notes is to function as a succinct but comprehensive revision aid, hence if you came by them via a search engine , please note that they're not intended to be a reflection of the quality of the materials referenced or the content lectured.

Lastly, with regards to formatting, the pdf doc was typeset in LaTeX, using a modified version of Stefano Maggiolo's class

[*] 2334590D@student.gla.ac.uk

1 Networks

1.1 *Introduction - Networked Systems*

1.1 definition. Networked System a collection of autonomous computing devices that exchange data to perform some goal

In this first part of the course we'll focus on 3 key aspects of these systems (1) how information is exchanged between the different devices involved ; (2) how we can build larger networks by linking devices ; (3) how systems communicate amongst themselves

1.2 definition. Signal a function which conveys information

1.3 definition. Communication Channel component of a a data transfer system responsible for carrying the signal

1.4 definition. Information Entrophy how much useful information a message is *expected* to contain

Claude Shannon the father of *Information Theory* showed that the amount of information that can be coded into a message could be quantified, and is known as *Information Enthropy*. Shannon stated that a data transfer system is composed of three parts: a source, a communication channel and a receiver. He identified the main problem within the system was to make sure that the information passed over the channel could be successuflly *recreated* by the source.

This encoding and decoding of messages can be done in several ways, some introduce more noise than others, but they all follow the same process of taking some form of physical signal (e.g. a wave) and converting it into some sort of simplied form of itself and then recreating it at the source end

Extra Information Enthropy Formal Definition

If we take X as the set of messages $\{x_1, \dots, x_n\}$

1.5 definition. Analogue Signal a smooth continuum of values

1.6 definition. Digital Signal a discrete sequence of values

The simplest analogue signal is when information is encoded directly using amplitude (e.g. AM radio), however of particular interest to us is the process of converting analogue signals to digital, which can be done for any analogue signal. (see Physical Layer)

1.7 remark. the the rate at which the signal must be sampled for accurate reconstruction is given by the sampling theorem

Switching

1.8 definition. Codign the act of mapping information to symbols

1.9 definition. Link the combination of a signal with a channel

1.10 definition. Hosts receivers and sources

1.11 definition. Network a collection of connected links

Within a networked system, information flows via channels forming links which connect hosts. The devices connecting the links are called *switches* or *routers* depending on the type of network. This *network switching* is responsible for determining how the information flows through the network and can be setup so that there are dedicated connections between hosts - *circuit switching* - or by splitting the messages into smaller packets before transmission allowing several hosts to share the same channell - *packet switching*

1.12 definition. Circuit Switching a dedicated circuit between hosts

1.13 definition. Packet Switching a shared link where messages are split into packets before transmission

The main trade-off here is between capacity and availability. For example, traditional phone networks are circuit switched (the very first ones had actual humans switching the channels and connecting hosts) which means that the two hosts requested a channel and they had guaranteed capacity over that channel while the connection was active, but it also meant that if some other hosts needed to use any part of the same link then their connection would be refused.

The internet on the other hand, is packet switched, by breaking the messages apart into smalled chunks hosts can share links the catch here being that though connectivity is guaranteed the capacity/speed is dependent on how many users are using the same channel.

1.2 *Protocols*

The different building blocks of a network presented above allow for the transportation of information, but is is the use of protocols which provide the semantics. For a message to be decoded the parties involved must agree on some sort of well-defined syntax, so that noise can be separated from meaningul information, this is precisely the role of the various network protocols existing at all levels within a network.

1.14 definition. PDU stands for protocol data unit, and is the basic unit of information for any given protocol

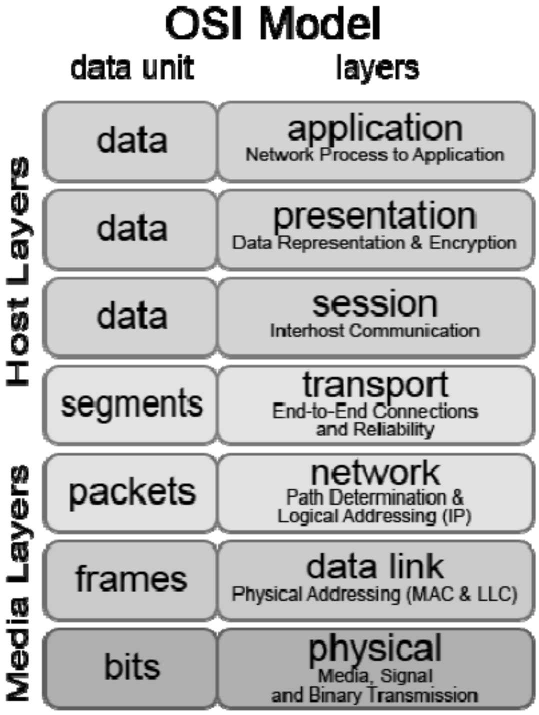
PDUs can be textual where rules of syntax and grammar are used to implement behaviour (e.g. HTTP), or binary where similar appropriate rules are used (e.g. TCP/IP). It is the role of PDUs to define what messages are legal to send, but is up to protocol semantics to define when to send them and what should be expected in response

Layers

Communication systems are tipically organised into layers, which reduces complexity at each layer's level. Peers on the same layer, use that layer's protocol to communicate using services provided by the well-defined interfaces of the lower layers

1.15 definition. OSI Model stands for *Open Systems Interconnection Model* and is a conceptual model that characterises and standardises the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.

A design tool used widely to model layered communication channels is the *OSI model*. It is merely a design tool, real implementations are more complex and usually the boundaries between layers are not so well defined.


OSI Model
data unit
layers
Host Layers
Media Layers
data
application
Network Process to Application
data
presentation
Data Representation & Encryption
data
session
Interhost Communication
segments
transport
End-to-End Connections and Reliability
packets
network
Path Determination & Logical Addressing (IP)
frames
data link
Physical Addressing (MAC & LLC)
bits
physical
Media, Signal and Binary Transmission

1.3 *OSI - Physical Layer*

The physical layer is concernerd with the transmission of raw data bits. In order for this to be possbile, the information needs to be transformed and encoded and a decision on the best medium for the job (e.g. cables, fibre optic etc.) and their phyiscal properties needs to be taken.

Transmission Channels - Enconding & Modulation

1.16 definition. Wired Data Trasmission the signal is transmited over a cable and is *directly* enconded onto the channel, by varying the voltage/light intensity

1.17 definition. Wireless Data Transmssion the signal is transmitted without the aid of an electrical conductor, most commonly using radio waves and some kind of modulation

A signal can travel with or without the aid of an electrical condutor, if it is directly encoded into a cable, then one of several *enconding schemes* can be used in order to change the signal into discrete pieces of data (e.g. bits).

High $\approx [3,5]v$ *, and Low* $\approx [0,3)$
NRZ : Non-Return to Zero

- **NRZ :** 1 – High ; 0 – Low

- **NRZ Inverted :** 1 – Change ; 0 – Constant
- **Manchester :** 1 – High-Low ; 0 – Low-High

To do (1)

Alternatively one can encode information onto a channel by varying the properties of the carrier signal via a modulating signal, a process know as *modulation* which allows the same channel to be shared by different signals

To do (2)

Bandwith, Capacity & Noise

1.18 definition. Bandwith determines the frequency range it can transport

1.19 definition. Sampling Theorem states that to accurately digitise an analogue signal, $2H$ samples per second are needed, where H is the bandwith in Hz

1.20 definition. Signal-to-Noise Ratio the ration between signal power and noise floor, typically quoten in $\text{dB} = 10\log(\frac{S}{N})$

The bandwidth of a channel is determined by physicial limitations of the channel, and given the existence of noise in the real worl, the *Signal-to-Noise* ratio and the bandwidth represent the fundamental limits for the rate at which information can be transmitted

1.21 remark. The maximum transmission rate of a channel grows lograithmically to the SNR

Extra Theoretical Maximum Transmission Rate

$$R_{max} = 2H\log_2 V$$

where:

R_{max} = max trasmission rate in bits/s

H = bandwith in Hz

V = # of discrete values per symbol

Extra Shannon's Theorem

$$R_{max} = H \log_2(1 + SNR)$$

Summary

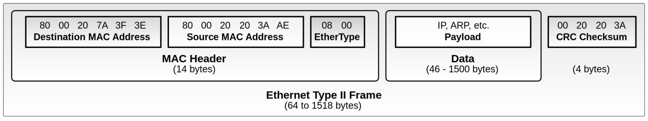
- **PDU :** bits
- **Function :** transmit a sequence of bits over an analogue channel
- Information can be encoded directly into the channel or the signal can be modulated
- Physicial limitations cap the transfer rate

1.4 *OSI - Data Link Layer*

The main purpose of the data link layer is to arbitrate access to the physical layer and turn the raw bit stream of data into a structured communications channel with the goal of transferring data between nodes attached to the same physical cable. There are several services provided by the DDL, the main ones being: *Media Access Control (MAC addressing) , Error detection and/or correction, Framing*

Framing

Frames are essentially fenced packets, which signal to the next layer the significant part of the data , i.e the *payload* and often whether that data was corrupted via some sort of error code or *checksum*. The DLL add the final tail and header to the payload and is therefore responsible for the last bit of data *encapsulation*



Error Detection & Correction

Though rare in wired systems, it is quite common for noise to cause bit errors in the data being transmitted. If the DLL implements error detection then it must add a *error detection code* as an header of the frame, the simplest one being the *parity code*. When the receiver gets the packet it uses the same function/rule to recalculate the code, if it doesn't match the frame is either discarded or corrected

1.22 definition. Parity Code an error detection code which is able to detect single bit errors. It works by adding all the bits, and checking the parity of their sum

1.23 definition. Checksum works similarly to the parity code, but is able to handle some multiple bit errors by using a 16-bit one's complement checksum

1.24 definition. Cyclic Redundancy Code a more advanced algorithm, commonly used in the DDL which can check if the bits are out of order. It relies on the remainder of a polynomial division of the data being sent

MAC

MAC is needed to determine which machine gets access to the channel when multiple hosts try to access it simultaneously. Because if that happens then the signals are said to *collide* and will overlap, resulting in an unreadable/garbage message.

1.25 definition. Contention-Based MAC a system is contention-based if multiple hosts share a channel in a way that can lead to collisions

CB MAC deals with collision in one of two ways:

1. **ALOHA** is the simplest protocol developed at the University of Hawaii in 1970. It tries to transmit whenever data is available, and if a collision occurs the frames are destroyed and the node will wait for a random amount of time before retransmitting, repeating until successful.
2. **CSMA** listens to the channel before sending, if it hears no traffic then it starts transmitting. Note however, that if the message takes time to reach the node , i.e. if there's a high *propagation delay* then there is an increased probability of a collision occurring mid-transit, an improved algorithm is **CSMA/CD** where the sending node keeps listening even during sending, if a collision occurs then both stations cease transmission immediately. This is an improvement because even though the frames are still corrupted, it saves time and bandwidth by reducing the time the channel is blocked due to collision.

The back-of interval between retransmissions is also random, but should increase with the number of collisions to reduce congestion

Summary

- **PDU :** series of bits - *frame*

- **Function :** Physical addressing , Framing, Error Detection
- Last encapsulation of data step ; adds an error detection code and some other meta data for framing in the trail of the packet
- Simpler error detection codes rely on summing up the bits of data and either checking their parity or sum
- Contention-Based MAC handle collisions by listening to the channel before sending the data and/or during

1.5 *OSI - Network Layer*

1.26 definition. End-to-End Principle is a network design principle whereby application-specific features reside in the end nodes, rather than being distributed across the network

The Network layer is responsible for end-to-end delivery of data and is therefore the first end-to-end layer in the OSI. This is important because networks can be of enourmous sizes, and since implementing a function always has a cost, if that function is implemented across the whole of the network that cost quickly multiplies. If instead the system is concerned with achieving reliability of communication above a certain threshold, it is more efficient to implement processes for checking for correctness and completeness at the end hosts rather than at the intermediary nodes, since end-to-end reliability is not perfectly aligned with the reliability of intermediary processes

1.27 definition. Internet set of interconnect networks

1.28 definition. Autonomous System a network within a larger network which is administered separately by a single organisation who is responsible for making independent policy and technology choices

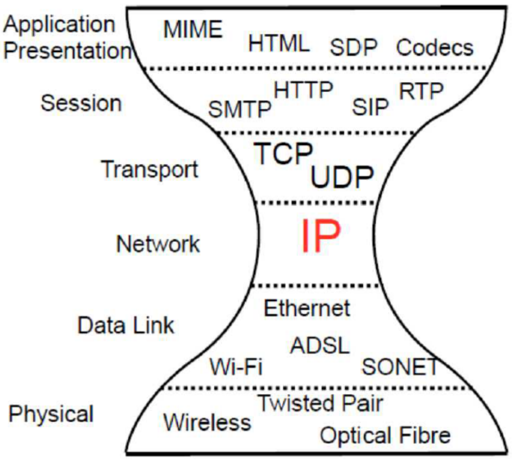
The basic components of an internet are:

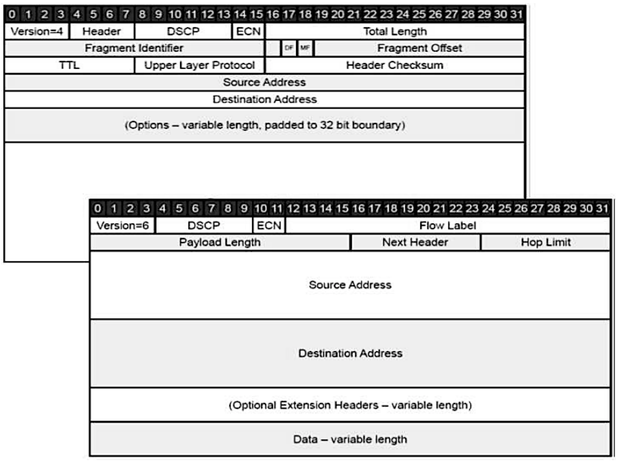
1. The existence of a common end-to-end protocol, which provides a single seamless service to the transport layer
2. A set of intermediate gateway devices, i.e routers, which implement the protocol and hide differences in link layer technologies by performing the usual services provide by that layer

1.6 *Network Layer - Internet Protocol*

The IP provides an abstraction layer, including a *simple, best effort, connectionless* packet delivery service. Which means, that it does not guarantee correctness or delivery, but it allows for addressing, routing, fragmentation and reassembly of packets.

The IP service model does not require a connection to be setup first, instead it just sends the available packets and anything which cannot be delivered is discarded. This means that it favours simplicity over assurance and correctness, leaving that for the layers above.





<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="4">Version=4</td><td colspan="4">Header</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="16">Total Length</td></tr>
<tr><td colspan="16">Fragment Identifier</td><td></td><td>DF</td><td>MF</td><td colspan="13">Fragment Offset</td></tr>
<tr><td colspan="8">TTL</td><td colspan="8">Upper Layer Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td colspan="32">Source Address</td></tr>
<tr><td colspan="32">Destination Address</td></tr>
<tr><td colspan="32">(Options – variable length, padded to 32 bit boundary)</td></tr>
</table>

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="4">Version=6</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="20">Flow Label</td></tr>
<tr><td colspan="16">Payload Length</td><td colspan="8">Next Header</td><td colspan="8">Hop Limit</td></tr>
<tr><td colspan="32">Source Address</td></tr>
<tr><td colspan="32">Destination Address</td></tr>
<tr><td colspan="32">(Optional Extension Headers – variable length)</td></tr>
<tr><td colspan="32">Data – variable length</td></tr>
</table>

Addressing

IPv4 addresses are 32 bits (4 × 8), while IPv6 are 128 bits (16 × 8), one part of the address identifies the network while the other identifies the host (which part is which may vary across different networks). Each network interface must have an unique address, however virtual IP addresses are sometimes used to give the illusion of privacy

1.29 remark. IPv4 addresses are deemed insufficient for the near future, so IPv6 was created. It has been slowly deployed since 2000 given the costs of replacing hardware and updating current software

1.30 definition. netmask describes the number of bits reserved for the network part of the address

1.31 definition. network address the host part of the address is set to 0

1.32 definition. broadcast address the host bits are set to 1

IP address: 130.209.241.197 ⇒ 11010001 11110001 11000101
Netmask: 255.255.240.0 ⇒ 11111111 1111111 11110000 00000000
Network: 130.209.240.0/20 ⇒ 10000010 11010001 11110000 00000000
Broadcast: 130.209.255.255 ⇒ 10000010 11010001 11111111 11111111

1.33 remark. a host with several network interfaces will have one IP address per interface (e.g Ethernet and WiFi interfaces in a single machine)

Fragmentation

1.34 definition. Fragmentation process which breaks packets into smaller fragments so that a layer with a smaller maximum transmission unit can receive them

The link layer has a MTU, hence before sending the packets to it, the IP breaks the packets apart into smaller frames. The process is reversed when receiving, and this can be achieved by including metadata with each frame - the *fragment identifier* , the *DF, MF flags* and the *fragment offset*. The DF flag is set if the packet is not to be fragmented, the MF flag lets the node know that it should expect more fragments part of the same packet.

1.35 remark. Note that both the last fragment of a packet as well as an unfragmented packet have MF set to true. These two cases are differentiated by setting the offset to a non-zero value in the first case

Loop Protection

In order to ward against loops, packets include a value which sets the maximum number of hops allowed in the network. With each hop this value de-

IPv4 - TTL ; IPv6 - Hop Limit

creases and if 0 is reached the packet is discarded

Transport Layer Protocol Identifier

IPv4 - Upper Layer Protocol ; IPv6 - Next Header

The TLPI is responsible for identifying the protocol used by the Transport layer above, in order to pass the data to the correct one.

To do...

□ 1 (p. 6): Insert image from anki card

□ 2 (p. 6): Insert image from anki card