XC Primer Parcial

Unit 1: Introduction

1.1 ISO Open Systems Interconnection (OSI)

We use a layer based system to know what type of connection, device or protocol we are working with, that order of layers is the following:

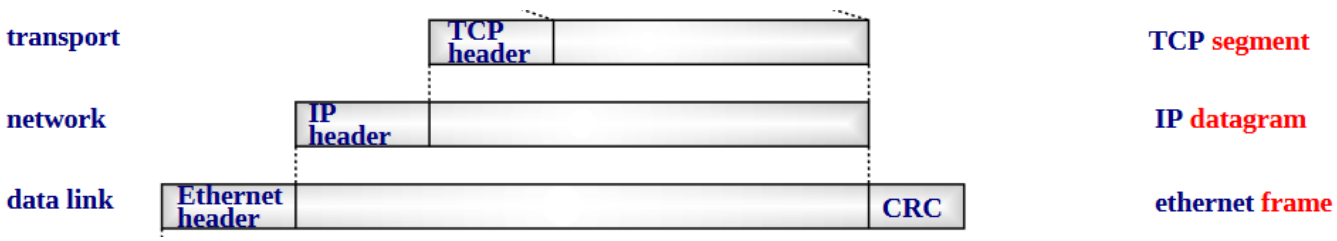
Number of the Layer	Name of the layer	Brief description
1	Physical	Electric and mechanical
2	Data link	Structured transport of bits
3	Networking	Routing
4	Transport	End to end data transport
5	Session	"Login" type service
6	Presentation	Encoding of text, numbers
7	Application	Processes using network services
8	*The User*	*This one is not oficial, but is used*

> Sometimes is used the expression **Physical network** to describe all the network that transports datagrams, but has NO relation with the layer 1 (L1)

1.2 TCP/IP Architecture

1.2.1 Encapsulation

Each layer adds/remove a PDU header



1.2.2 TCP/IP Implementation

- TCP/IP **networking code** is part of the OS
- OS use **sockets** to comunicate in/out with TCP/IP
- The creation of sockets is similar to the inodes of a file

1.3 Client Server Paradigm

1.3.1 The Internet Transport Layer

Two protocols are used in TCP/IP transport layer:

- **UDP**: offers a non reliable datagram service. It's connectionless.
- **TCP**: offers a reliable (segments are acknowledged if correct or retransmited if lost) It's connection oriented. Uses Three way handshaking. (More in Unit 3).

1.3.2 The Client Server Paradigm

- The client **always** initiates the connection.
- Parts of a datagram:
    - IP header: Has the known IP of the target.
    - TCP/UDP header: Has the known port of the target (< 1024).
- The server is a **daemon** waiting for client requests.

Unit 2: IP Networks

2.1 IP Layer Service

- The **main goal** of Internet Protocol (IP) is **routing datagrams**.
- The **main design goal** of IP is to interconnect hosts to LANs/Wan/s that use different technologies.
- The IP characteristics are:
    - Connectionless
    - Stateless
    - Best effort

2.2 IP Addresses

- IPv4 addresses are **32 bit long** and noted as Dotted point notation, e.g: 192.186.1.1
- We can divide them in **two parts**:
  - **netid**: identifies the network
  - **hostid**: identifies the host within the network
- IP adresses identifies an **interface** which are attachment points to the network
- All ip adresses in the Internet **must be different**: The **IANA** distributes it using RIRs
  - **RIR assign addresses to ISPs** and the **ISPs to the customers**.

2.2.1 Classes

- The **highest bits identify the class**, the number of IP bits of netid/hostid varies
- D Class is for multicast addresses and E Class are reserved addresses.

Classe	netid (bytes)	hostid (bytes)	Codificaton	Range
A	1	3	0xxxx...x	0.0.0.0 ~ 127.255.255.255
B	2	2	10xxx...x	128.0.0.0 ~ 191.255.255.255
C	3	1	110xx...x	192.0.0.0 ~ 223.255.255.255
D	-	-	1110x...x	224.0.0.0 ~ 239.255.255.255
E	-	-	1111x...x	240.0.0.0 ~ 255.255.255.255

2.2.2 Special Addresses

netid	hostid	Meaning
xxxx	all '0'	Identifies a network. It is used in routing tables.
xxxx	all '1'	Brodcast in the net xxxx.
all '0'	all '0'	Identifies "this host in this net". Used in DHCP.
all '1'	all '1'	brodcast in "this net" Used in DHCP.
127	xxxx	host loopback: interprocess communication using TCP/IP

> Each network has two special addresses: network and broadcast addresses.

2.2.3 Private addresses

Private addresses are used to communicate devices "outside" the internet.

There are the following:

Number of Addresses	Network type	Addresses
1	A	10.0.0.0
16	B	172.16.0.0 ~ 172.31.0.0
256	C	192.168.0.0 ~ 192.168.255.0

2.3 DNS

- Uses the client server paradigm
- Short messages, uses **UDP**
- Uses the port **53**

2.4 Subnetting

We use subnetting because it allows us to split up a huge pool of addresses into more small ones. For that we use **masks**:

- Masks can be written as: 255.255.255.192 or as /26 as in 210.50.30.0/26
- To compute avaliable addresses of a certain subnet we use $2^{32-mask} - 2 - routers$
- There is a variaton called **VLSM** that simply are subnets of different sizes.

2.5 Classless Inter-Domain Routing CIDR

It's a **rational geographical-based distribution** for IPs that:

- Used masks instead of classes in order to **aggregate routes**
- Allows using **summarization**: $\begin{matrix}200.1.10.0/24\\200.1.11.0/24\end{matrix} \rightarrow 200.1.10.0/23$

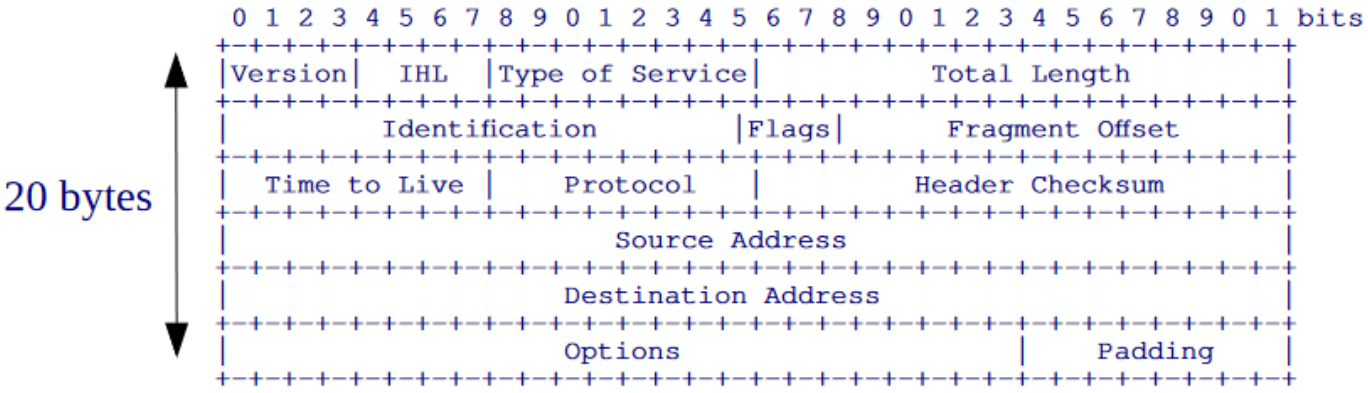
2.6 Routing tables

- Routing can be:
    - **Direct**: The destination is directly connected to an interface.
    - **Indirect**: Otherwise. In this case, the datagram is sent to a router.
- **Default Route**: Is an aentry where to send all datagrams with a destination not present in the routing table, by default is 0.0.0.0/0.

2.7 Address Resolution Protocol ARP

- Main goals:
    - Detect **duplicated** IP addresses
    - Update MAC addresses in **ARP tables** after an IP or NIC change.
- To send packages u need the **physical address**, we use ARP to **translate** IP to MAC
- When IP calls ARP:
    1. If ARP table has the requested address, it is returned
    2. Else:
        1. IP stores the datagram in a **temporal buffer**, and starts the resolution.
        2. IP initiates a **timeout** and starts forwarding the next datagram.
        3. Can happen the following scenarios:
            - The timeout triggers before resolution, the datagram is removed.
            - If ARP return the requested address, IP calls the driver with it.
- ARP resolution in an ethernet network
    1. A **broadcast** "**ARP Request**" message is sent indicating the IP address.
    2. The requested IP address sends a **unicast** "**ARP Reply**" and stores the requesting address in the ARP table.
    3. Upon receiving the "ARP Reply", the requesting station return the IP call.
    4. ARP entries have a timeout **refreshed** each time a match occurs.

2.8 IP Header



- Version: 4
- IP Header Lenght (IHL): Header size in 32 bit words
- Type of Service: (ToS) xxxdtrc0
- Total Length: Datagram size in bytes
- Identificacion/Flags/Fragment Offset: used in fragmentation
- **Time to Live (TTL)**: if (--TTL == 0) discard;
- **Protocol**
- Header Checksum: Header error detection
- **Source and Destination addresses**: En nodes addresses.
- Options: Rcord Route, Loose Source Routing, Strict Source Routing.

2.9 IP Fragment

Fragmentation can occur when:

- **Router**: Fragmentation is needed if networks with different MTU are connected.
- **Host**: Fragmentation may be needed using **UDP**. TCP segments are <= MTU.

Datagrams are recronstucted at the destiantion using the following fields:

- **Identificacion** (16 bits): identify fragments from the same datagram.
- **Flags** (3 bits):
    - **D**, don't fragment. Is used in MTU path discovery.

    - **M**. More fragments: Set to 0 only in the last fragment.
- **Offset** (13 bits): Position of the fragment first byte in the original datagram.

2.10 MTU Path Discovery

- Used in modern TCP implementations.
- By default TCP chooses the maximum segment size.
- Goal: avoid fragmentation, sends packets each time with less segment size untill one dosn't gets returned.

Unit 3: IP Networks

3.1 Internet Control Message Protocol ICMP

- It's a protocol used for **attention and error messages**
- Can be generated by **IP, TCP/UDP** and application layers
- Are encapsulated into an IP datagram
- There are two types:
    - Query: Have an **identifier field** for request-reply correspondence.
    - Error: The first 8 bytes of the payload causing the error are copied. These bytes are captured by the TCP/UDP ports.
- An ICMP **cannot** generate another ICMP

> Exaples of common ICMP messages are: echo reply, network unreachable, host unreachable, echo request and time exceeded.

3.2 Dynamic Host Configuration Protocol DHCP

- Used for **automating the following network configuration tasks**:
    - Assign IP address and mask
    - Default route
    - Hostname

    - DNS domain
    - etc
- DHCP has the following modes:
    - Dynamic: During a leasing time
    - Automatic: Unlimited leasing time
    - Manual: IP addresses are assigned to specific MAC addresses

> Examples of common DHCP protocol messages are: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACK.

A typical server-client interaction is somthing of the sort:

- Client -> Server: DHCPDISCOVER (port 67) using UDP
- Server -> Client: DHCPOFFER (port 68) using UDP (can be unicast or broadcast)
- Client -> Server: DHCPREQUEST (port 67) using UDP
- Server -> Client: DHCPACK (port 68) using UDP (can be unicast or broadcast)

> If previously a DHCP connection has allocated a network address to a client, that client can reactivate it using only DHCPREQUEST.

3.3 Network Address Translation NAT

- NAT's are often used to **save public addresses** because translate private addresses to fewer (usually 1) public address.
- NAT's also provide improvements in security

Basic NAT:

- Pretty useles, u need as many external addresses as internal ones.

Port and Address Translation PAT:

- Different private addresses can use an **unique public address**.
- Each connection requires one NAT table entry.

The NAT entries can be:

- Static: Manually added.
- Dynamic:
    - Entries are automatically added when an internal connection is initiated
    - External addresses are **chosen from a pool** (or an unique one).
    - Table entries have a **timeout**.

DNAT:

- The address translation is exacly as the NAT but **connections come from outside**.
- Static configuration is needed.

3.4 Routing algorithms

Routing algoithms main objective is adding entries to routing tables, they can be:

- **Static**: Manual, scripts, DHCP
- **Dynamic**: Automatically update table enties when a topology change occurs.

Internet is an **Autonomous Systems** (AS), routing algorithms are classified as:

- Interior Gateway Protocols (**IGPs**): Inside the same AS
    - RFC standards: RIP, OSPF
    - Propietay: CISCO IGRP
- Exterior Gateway Protocols (**EGPs**): Between different Ass
    - Currently BGPv4

> AS are identified by the IANA with 16 bits numbers (ASN)

3.4.1 Routing Information Protocol RIP

Important Concepts:

- **Metric**: Is the distance (in hops) betwwen 2 hosts, if it's directly connected is "1". If the metric is unreachable (infinite) then is 16.
- **RIP updates**: Come every **30 seconds to the neighbors**, if in more than **180 seconds no update** comes from a neighbor is **considered down**.

- **RIP v2**: Allows variable masks and multicast addresses.

Depending on the route **convergence problems** may arise (**count to infinity**). This normally happens when a router of a network goes down and the neighnbour routers cannot find another path to the "other side".

Solutions:

- **Split horizon**: When a router sends the update, removes the entries having a gateway in the interface where the update is sent. **¡Very important!**
- Split horizon with **Poisoned Reverse**: Consists in sending the update before the 30 seconds timer expires when a metric change in the routing table.
- **Hold dowm timer** (CISCO): When a router becomes unreachable the entry is placed in holdowm during 280 seconds. During that time the enrty is not updated.

3.4.2 Open Shortest Path First OSPC

- Is a **high performance IGP routing protocol**.
- **Link state** protocol: Routers monitor neighbor reouters and networks and send that information to all OSPF routers. They use the *hello protocol*.
- To find the shortest path they use the **Dijkstra algorithm**.
- The metric is computed taking into account delays, link bitrates... etc... The infinite metric is the maximum metric value.
- There is no **convergence** problems

3.5 Security in IP

Main goals:

- **Confidentiality**: Who can access
- **Integrity**: Who can modify the data
- **Availability**: Access guarantee

> Typical vulerabilities are: **Technological** ones (Protocls and networking devices), **Configuration** ones (Servers, paswords...) and **Missing security policies** (Secure servers, encryption, firewalls...).

Attacks:

- **Reconnaissance** (Previous to an attack):
    - Avaliable IP addresses, servers and ports
    - Types of OSs, versions, devices...
    - Eavesdropping
- **Acces**: Unauthorized acces to an account or service.
- **Denial of Service**: Disables or corrupts networks, systems or devices.
- **Viruses, worms, trojans**: Malicious software that replicate itself.

Basic solutions:

- **Firewalls**: System or group of systems that enforces an access control to a net.
    - NAT
    - Access control List, ACL
- Virtual Private Networks (**VPN**):
    - Authentication
    - Cryptography
    - Tunneling:
        - Sends the datagrams encrypted and encapsuled to the destination and in the wway the VPN server will remeove it.

Tunneling Problems:

- Fragmentation: The exit router may have to reassemble fragmented datagrams.
- ICMP datagrams are addressed to the entry of the tunnel.
- MTU path discovery may fail.

Solutions:

- Routers in a tunnel enter the **tunnel state**, that allows to use ICMP and MTU and fragmenting before entering.

Types of tunnels:

- **IP over IP**: Basic encapsulation
- Generic Routing Encapsulation **GRE**: Allows encapsulating other protocols.
- Point to Point Tunneling Protocol **PPTP**: Add the ppp funcionalities.
- **IPsec**: Standards to introduce authentication and encryption and tunneling to IP.