8/10/2020

A TELECOMUNICATIONS NETWORK MODEL (Slide 0)

- 5 basic components
  - TERMIALS (any output-input) → software
  - TELECOMUNICATION PROCESSORS → software
  - TELECOMUNICATIONS CHANNELS → not software
  - COMPUTER
  -

The networks are divident into tree areas:

WAN (Wide area network)
large size in covers, big geographic area (decine → migliaia km)

LAN (Local area network)
smaller extention (10 - centinaia km)

MAN (Metropolitan Area Networks)
class of network, cover an area of a few km

A network could be private or public.

- PRIVATE → **VPN** (Virtual private Network)
  (if it can be used only by few users, that are authenticated by credentials)
  Public network and private user's owner.

Local area → intranet (which is private) → INTRANET: use of internet in the privat area
(is a logical concept)

↳ then we go in public area.

Not all the netw. elements have the same role

- CLIENT / SERVER Networks (server applications can be very difficult)
  - end user PCs
  - ↳ helps with application processing and also manages the network.

My smartphone operates as a server when we use it as an hotspot

There are LINKS connection devices

- WIRED: different kind of media → ethernet cables, telephon cables, TV cables, telephone cables
  - COPPER BASED
  - FIBER BASED (AI) — the material is glass

  } have very different characteristics: the material used is different and this changes the performance.

- WIRELESS: there are a huge amount of possibilities
  - LONG RANGE: terrestrial area in order of several kms
    - TERRESTRIAL MICROWAVE (40 km apart) using Antennas
    - COMMUNICATIONS SATELLITES using satellites and antennas (we can cover more area)
  - MEDIUM RANGE
    - CELLULAR SYSTEM: Each cell is typically from 1 to several squares miles in area. There is an Antenna, connecting different devices. → BASES STATION
  - SHORT RANGE
    - WI-FI (Medium - short range) which is an infrastructure. There are access points that are wired connected

STANDARS IN CELLULAR NETWORKS

2G → 3G → 4G → 5G

Technical name 2G = GSM → mainly circuit switched

3G → GPRS → packet switching and an architecture based only on internet protocol.

4G → LTE (long term evolution) → operate in IP domain

5G → (5G) → the standard has the same name of the generation

PAN (personal AREA network) there are several connection methods:

IEEE 802. ... → is the standard in local area

(ex) IEEE 802.11 → Network. WI-FI (personal network)

IEEE 802.15 → Bluetooth.

DICEMBRE

WIRELESS: if the communication uses low power or

-LOW POWER Area Network.

is used to interconnect small devices with different roles in the network, IOT (internet of things)

It means during communication it uses low power only to keep alive small devices.

There are a lot of standars in IOT, they are divided into costs, use...

LOW POWER AREA NETWORKS

RFID operates in VERY SHORT RANGE

WI-FI operates in SHORT - MEDIUM RANGE

CELLULAR SYSTEM has the highest hosts.

LORA → low power solution. Provides services for IOT and it belongs to wide Area network

9/10/2020

TELECOMMUNICATION PROCESSORS

- Internetwork processors
  - Switches: Make connections between telecomm. circuits so a message can reach its intended destination. (is an evolution of hub. Transfers infos from an input port to a specific output port)
  - Router: Interconnects networks based on different rules or protocols (The info is routed from an input port to an outp. in the network in accordance to routing rules (based on protocols))
  - Hub: Port switching communications processors (it is used in LAN and transfers infos to a multiple number of ports from a single port)
  - Gateway: devices part of the network but implement tasks to process data (for example a firewall)
    → devices of the network that implement tasks in order to process network data. (also a modem can be seen as a gateway)

TELECOMM. SOFTWARE

provides many communic. support services including connecting & disconnecting, communication links & establishing comm. parameters such as transmission speed, mode and direction

- Network Management (capacity planning)
  - traffic manag. → we do have to control packages on a network and so on
  - Security → can be implemented in a specific network element
  - Network monitoring → control all operations on network.
  - capacity planning.

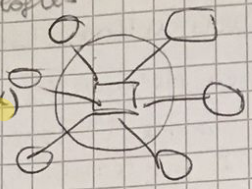
advantages of using softwares: SCALABILITY, CHEAPER

↳ easier to update when technology updates

other differentiation is that by topologies

NETWORK TOPOLOGIES

- **STAR** → is used in corner network (not in core network)
  - Ties and user computers to a central computer
  - Considered the less reliable

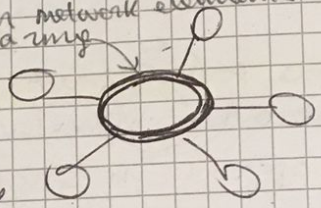


devices are connected to a same device called access point.

ADVANTAGE: if you have a new user and you have space in the port, you can add it
simple to substitute a broken node?

DISVANTAGE: If the central broken, nothing will work. stops
Single point of failure. (if there is an error the network
different user, not other network elements but only
the media shaped in a ring

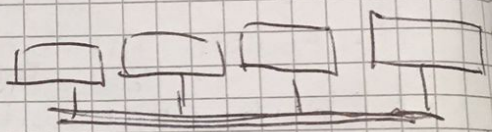
- **RING** (TOKEN RING)
  - Ties local computer processors together in a ring on a more equal basis.
  - Considered more reliable and less costly



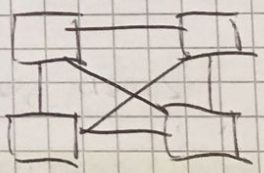
ADVANTAGE: if something is broken, I can run the ring on the other direction to reach all points connected

DIS: complicated to substitute because every device is directly connected with the media

- **BUS**: → no other network elements and the media interconnect every device
  - Local processors share the same bus, or communications channel
  - TREE is a variation which ties several bus networks together



- **MASH TOPOLOGY**
  - every user is interconnected to all other users are more expensive but very robust.
  - Are used in the core network thanks to their reliability.



TECHNOLOGY IS A UNION OF PROTOCOLS

Protocol is a standard set of rules and procedure for the control in communications in a network

OSI MODEL 7 layers. In a network we operate in different layers and any layer implement a set of tasks. The protocols are the way to implement these tasks

TCP/IP MODEL Can match OSI MODEL but it has 5 layers

ACCESS NETWORK

is a part of comm. network which connects subscribers to their immediate service provider.

It is contrasted with the core network

The access network may be further divided between feeder plant or distribution network, and drop plant or edge network

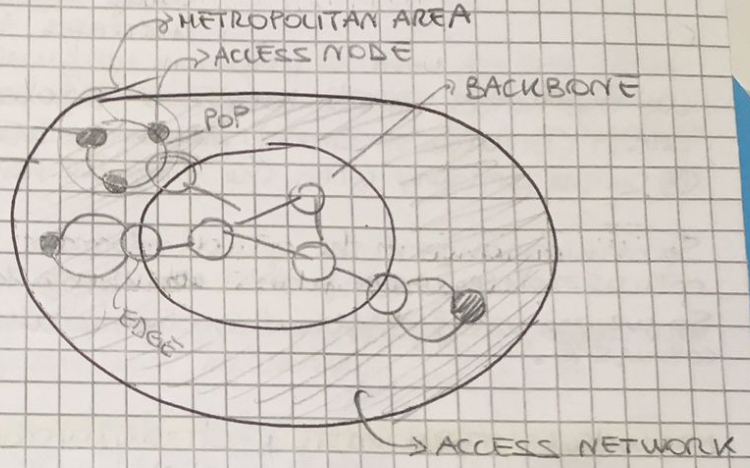
We use very different technologies for the access: ~~which the core evolved by the ISPs~~ communication carriers have used ~~COPPER LINES~~ COPPER LINES.

Carriers are also investing heavily in optical fiber.

The METROPOLITAN AREA between access network and core is also called EDGE NETWORK.

we can perform control to the information that cross the network.

~~Edge~~ EDGE COMPUTING.
(used for intrusion detection system)



Examples of access network

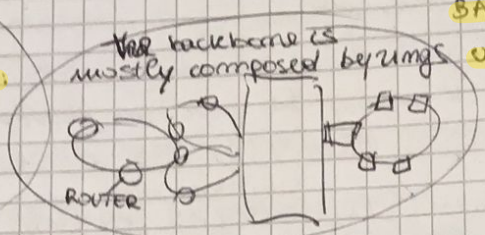
- FIXED WIRELESS ACCESS: systems are connected to the core through wireless communication
  wireless
  medium range
  - an example is LINKEM (is an operator providing fixed wireless access)
- COPPER BASED: copper is the material used for telephon network and it is used for all ADSL family.
  wired
  short range
  Provide access from the perferal area network and the core
- FIBER ACCESS: is the same but using fiber
  wired
  longer range
- CELLULAR ACCESS: mobile by using cellular infrastructure to access core.
  wireless
  medium range

There are other differences for example security, cost, coverage, data rate.
The ~~wire~~ wired ones are faster than wireless, but cellular access is faster than copper (especially the 5G)
Wired is more stable than mobile (unless damage in wire)

EXEMPLE OF TELECOM ITALIA

ACCESS NETWORK
cellular access
we use different medias:
cellular and copper

BACKBONE NETWORK



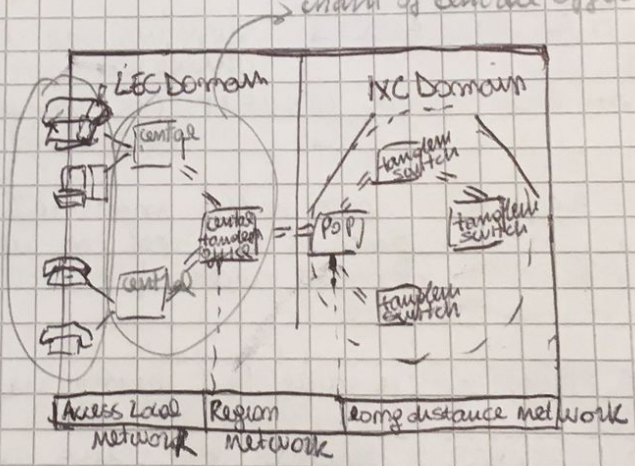
FIBER WORKS EXCHANGING LIGHT, so the router are able to transfer different colours. So different colours represent different subcarrier
Using different colours at the same time increases the capacity of the fiber

We use RINGS in the backbone because is cheaper than implement SMASH (Because in smash all devices are interconnected with each other) ☹ On the contrary with the ring we have only one cable

Spectrum range in the optical domain is different when we will use optical routers on fibers ~~etc~~ using different colours.
So we are using different spectrum range for producing different colours 😊.

NETWORKS TERM IN TELEFON NETWORK

In the local area, the operator is called
LOCAL EXCHANGE CARRIER (LEC)
(in telephone terminology a corner is an operator)



- Incumbent LEC (ILEC)
  is the starting ~~owner~~ carries of the network
  (ex) TIM
- Competitive LEC (CLEC)
  are operators that allowed to provide a service in the local area
  (ex) VODAPHONE, TISCALI, WIND, TELEDUE, TRE, ILIAD

There are ~~owners~~ carries in the local area that are Incumbent. ~~etc~~ That is an operator that owns the infrastructure where the information is exchanged (TELECOM ITALIA)

The competitive is allowed by law to have in the access network other network operators

15/10/2020

LOCAL LOOP (the last mile) (circuit between user and network) (circuit ?)
interconnects in the local area some users (connects the home to the network)

WIRED LOCAL LOOP : • PLC (power line communications)
• FIBER OPTICS SERVICES
• CABLE LOCAL LOOP

WIRELESS LOCAL LOOP : • satellite local loop (communications satellite and cosmos internet connections of satellite television
• LMDS
• WiMAX
• GPRS

ex EOLO
LINKEM

UNBUNDLING FRAMEWORK

To prevent the owner from using the monopoly to monopolize other fields of trade, some ~~countries~~ jurisdictions require utilities to UNBUNDLE the local loop : that is make the local loop available to their competitors.

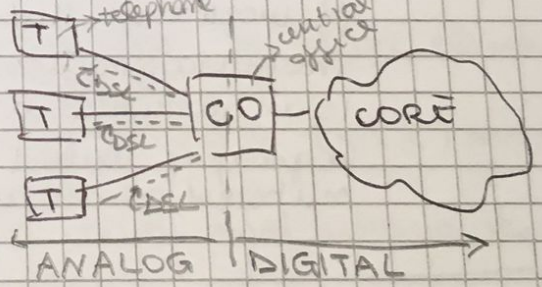
COST ANALYSIS

Thanks to the pre-existent copper-based system of tv and telephone, ~~we~~ we are able to provide the next generation network.

So it is possible to upgrade the copper-based access networks to carry high-speed services through the use of xDSL technologies;
DSL → digital subscriber line.

At the very beginning (till 30 years ago), the telephone network was done in this way

The analog was a continuous signal, while the second part was digital.
So it is called digital subscriber line because when they ~~put~~ added DSL to connect telephone to CO they try to transform the communication into a digital number



so xDLS stands for all types of DSL

So xDSL is the most widespread access

TYPES OF ACCESSES

There are still local loops based on copper (telecable) and local loops that use fiber (real time fiber)

- **OPTICAL ACCESS**

the fiber is a media that allows faster and more reliable communications.
The cost is high not for the material perse, but for the fact that you need to work on the road (to position cables, you have to stop the traffic and so on. (digging))

FTTx = Fiber to the - x

FTTH : Home
FTTC : Curb
FTTP : Premise
FTTB : Building or Business
FTTU : User
FTTZ : Zone
FTTO : Office
FTTD: Desk

FTTN : Node or Neighborhood

Sito per vedere cose sulla rete

https://fibermap.it (putting region/area/address you can check the cover of fiber.)

https://www.garr.it (you can see the interconnection of Italy using Fiber).

NAMEX : internet exchange point where different network operators are interconnected (PEERING)
It works in Mediterranean area.
The interconnection is based on AUTONOMOUS SYSTEM which is an administrative system that is a sort of supernetwork. (a group of routers belonging to the same entity are numbered as an autonomous system).

FTTx : reference architectures

OLT : (Optical line terminal) is in correspondence of the curb or the cabinet or the central office

ONU : (Optical Network Unit) is in correspondence of the user side (between OLT and ONU we have fibers)

ONT : (optical network termination)

ODN :

AON : Active optical network

N.B copper cable is represented by ∞∞∞ because it is based on a twisted pare of cables

Fiber to the Exchange : the optical fiber terminates to the central office CO and the CO is connected with the user via a copper based line

When you reduce the amount of twisted pair that you have in the last mile, you increase the bit rate.
So the potentiality of the local loop depends also on the lenght of the fiber with respect to the copper.

RETRO LINK:
COVERAGE FIBER BY TELECOM ITALIA: https://rete.gruppotim.it

2G and 3G architecture

16/10/2020

We can provide wireless access in accordance to cellular network area.
We have to provide mobility (and mobile connectivity)

Cellular networks are organized in cells and in every cell we have a macro cell and small cells.
In every cell we have a network device called BASE STATION (BS) which is controlled by a network element in cellular 2 and 3 generation architecture called BASE STATION CONTROLLER (BSC)

There is an upper level element called RADAR NETWORK CONTROLLER (RNC) - RNC interconnects different BS

These network elements are interconnected to other elements like the Mobile switcher center (MSC).
MSC is interconnected to Home location register (HLR) and to Visitor location register (VLR)
A user is registered in a database in HLR and when a user moves it is registered in VLR

GGSN and SGSN provide the IP (the data interconnection) of the network

---

- Another kind of wireless access that was designed to support local area network is the one based on Wi-Fi.
(standard named IEEE 802.X)
Starting from the standard we have several evolutions in two area directions: one in the personal area (PAN) (an example is Wimedia - IEEE 802.15 & bluetooth)
the other is to the wider area (Metropolitan and Local area MAN and LAN) 802.16 and to Region area (RAN) 802.22)

TECHNOLOGIES and BANDWIDTHS

Is always true that in the wired solutions the data rates is increasing and in the wired solution are higher than the wireless one.

---

links connect one continent to another using submarine cables

BACKBONE

The access for the backbone is provided by using wired links that are implemented by using ~~fibre~~ optical fiber / (fiber optics)

In Italy we have 32 PoP (points of presence) equivalent to cities where these PoPs are.

~~There are~~ Among these 32 there are 4 called INNER CORE (2 in Rome and 2 in Milan) and the others are Outer CORES

in
- Inner core : 10 Gbit/s
- Outer core : 10 Gbit/s or 2,5 Gbit/s or 155 Mbit/s
- ~~other~~

The amount of traffic set on the link is 50% of the capacity of the link. This is in order to add redundancy - so in case of failure on the network, the traffic can be directed to another part.

PHYSICAL TOPOLOGY

is made using optical routers and they are interconnected by links with optical fiber.

TECHNOLOGY AND PROTOCOLS

We have different protocols at different layers.
In the backbone we have protocols at the lower layers and it is mostly implemented with multiplex traffic with fiber optics.

~~by~~ On layer 2 we have an asymmetrous Transfer mode (ATM) and gigabit Ethernet (GbE)
On layer 3 we implement multiprotocol Label Switching.

~~INTERNATIONAL INTERNET~~

22/10/2020

XDSL

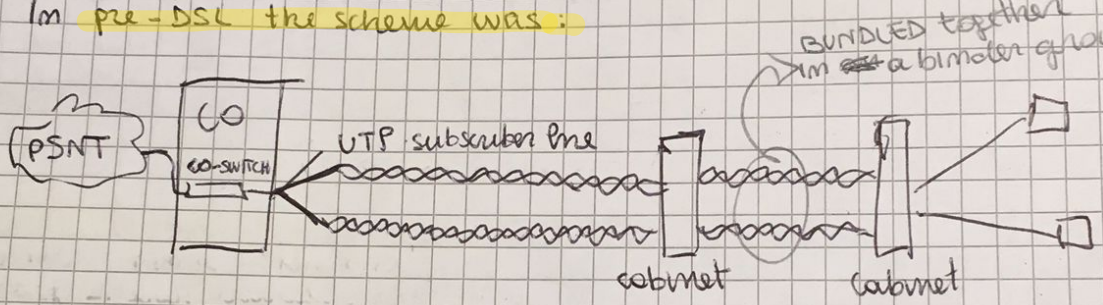
XDSL is a family of technologies that provide digital data transmission over the wires of a local telephone network.

DSL originally stood for digital subscriber loop

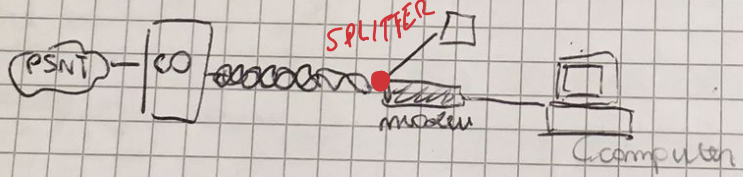
- IDNS: this solutions used the same copper line of telephone network but provided 2 copper wires because

(Before the signal from telephone to CO was analog, so to trasport the voice into an analog form the copper wire was set up to transfer in frequence a bandwidth contained in a range from 0 to 4 KHz.
~~So the wires to be transformed into an analog form;~~ (4H bandwidth)
So 4 KHz was enought to transform voice into an analog form
So initially IDNS used voice in path of copper wire

In pre-DSL the scheme was:



ANALOG modems: VOICE BAND MODEM



SHANNON CAPACITY OF TELEPHONE CHANNEL → bandwidth (in B)

~~C = W log2(1 + channel ratio)~~ $C = W \log_2(1 + SNR)$ = bits/sec.

SNR is in db (SIGNAL TO NOISE RATIO) → data rate or channel capacity

In the next years there were other solutions (xDSL)

- X stand for the different options that we have for DSL, for instance ~~ADSL~~ ADSL → asymmetrical digital subscriber line
VDSL → very high dig. sub. line

The speed we can achieve on the DSL made of copper wire, depends on the distance that we cross with this digital line.

Ex for a category 3 UTP (unshielded twisted pair) the data rate decreases as a function of the distance. This is always true for all communication system.

- ADSL (asymmetric DLS)

what is the winning point?

- the fact that it is asymmetric. It is almost random result because when the DSL happens the interest of having digital services at home was driven by the video on the main services. So at that time people didn't use so much computers at home to navigate the internet and so on. So this is the reason why they decided that DSL should have worked in an asymmetrical way (a lot of data in one direction and less data in the other) This structure is used also for surfing the internet. There are more data in the download than upload

ADSL uses two separate frequency bands referred to as the upstream and downstream

0 - 4 KHz PSTN (voice) telephone network)

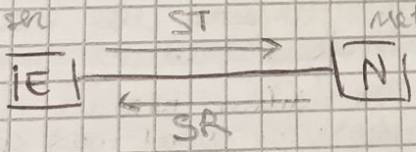
25.875 KHz - 133 KHz Upstream

138 KHz - 1104 KHz Downstream (bandwidth wider than upstream) so data rate here is faster than upstream

N.B → there are gaps between different frequences to avoid interference (which is contemporary transmission of signals in the same frequency band).

ADSL also provides an overlapping of up and downstream. We can trasmit contemporary data in up and downstream through the operation called ECO CANCELLATION

ex



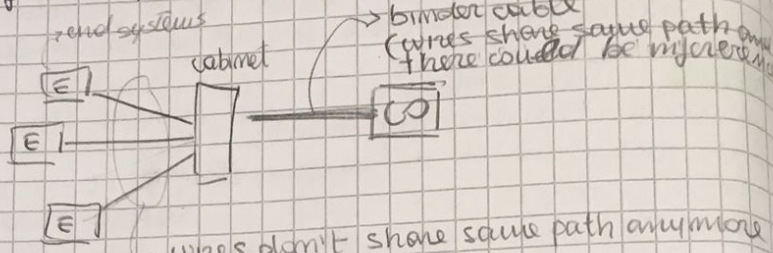
this communication is intrinsically bidirectional (same bandwidth, same time). How can I control that the two do not interfere? There is no way. But I can do ECO CANCELLATION

if I transmit the signal (ST) and there is another signal that is received (SR), when I receive the signal, I can cancel from what I received, what I have trasmitted. (So in this way I cancel interference)

ADSL also provides overlapping of voice received and transmitted in the telephone network. (we can receive and transmit at the same time.

CROSS-TALKS

wires sharing the same cable interfere one each other.
In the BINDER GROUP there are wires used only for telephone networks, wires used for DSL other used for VDSL / ADSL / ISDN and so on (depends on the original deployment of these wires)

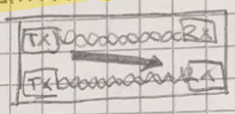


This interference has two names: FEXT or NEXT

FEXT (Far-end cross-talks)

It is the cross-talk between a transmitter and a receiver placed on opposite sides of the cable

NEXT

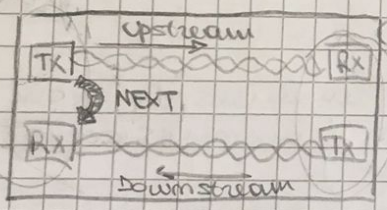


NEXT

It is the cross-talk between a transmitter and a receiver placed on the same side of the cable

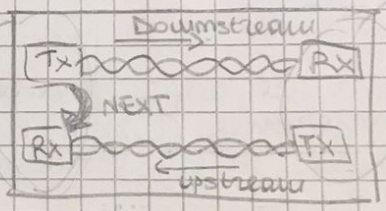
Consider the case where I want to use more bandwidth in the downstr. and use the band. of the upstream: I'll have 2 configurations:

① users / end systems



In this configuration, we consider two different users on the left and the CO on the right.
However This configuration does not exist in fact I can't have interference NEXT among ~~beta~~ different users that use different cables.
So this means that NEXT must be in CO, so downstream and upstream are inverted

② CO / end systems



So the right configuration is this one, where NEXT interference is in the CO

This is the ~~case~~ right case.
To avoid interference I avoid to use the ~~all~~ full bandwidth in downstream

The solution is that the the CO, knowing what was sent in downstr, could remove what was sent and isolate what is receiving from upstream (avoiding interference)

- So the solutions for interference are:
  - ECO CANCELLATION
  - not overlap the bandwidths (keep them separated) of upstream and downstream

DICEMBRE

The real data rates depend on:
- the length of the cable
- the distance from the CO or the cabinet
- how many cables share the same binder group
- what is the quality of the cable
- what technology was used for cables

23/10/2020

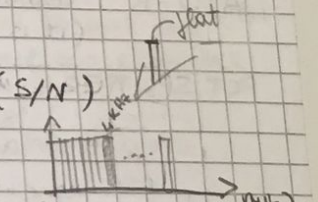
MODULATION
is a way to create a shape of the signal that is going to transport the bits. (We are talking about digital comunication)
There are different schemes:

★ **CAP** (Carrier-less Amplitude/Phase)
It provides a signal that once is modulated, it occupies the whole bandwidth.
In general there is a frequency carrier to transport these signals.

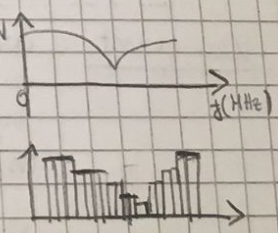
Problem) Since the bandwidth we are going to put ~~on a~~ this signal is quite large, the frequency behaviour in the spectrum is not ideal.

Which is an ideal behaviour in a spectrum band? It is when you have an attenuation (as a function of the frequency) ~~flat~~ flat, that is all the frequences are attenuated in the same manner.
So while it is quite easy to assume that the channel is flat, when the bandwidth is large it is compex to have flat attenuation

The idea of ADSL: let mesure the attenuation (S/N)
The attenuation is not flat (but there are some frequences that are suppressed by the channel)



★ **DMT** (Discrete modulation multi tone)
Divide the channel in several subchannels, each one very short (4 KHz).
The advantage of this splitting is that if we look on one subchannel, we can observe that it is flat.
So in each ~~subchannel the~~ subband the channel becomes flat and for the frequences in that subband you can ~~characterize~~ characterize the attenuation with a value which is the same for the whole subband.
~~This multi tone modulation~~ So it is called discrete because you divide it in subparts. Multi tone because you have different bands and each band has a different tone.

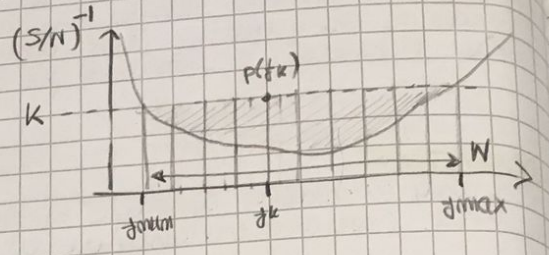


Once we divide in subbands, we can provide modulation different modulation for each subband.
General Rule for modulation: you can put more bits (effuent modulation) when you have low attenuation.
On the contrary, you have to put less bits (less effuent modulation) when you have an higher attenuation.
This concept is represented by WATER FILLING

WATER FILLING

Let us assume that our channel is represented as the inverse of its signal to noise ratio $(S/N)^{-1}$ so it represents the behaviour of S/N

This can be considered as a pool in which the water is the band you dedicate to each modulation. (the amount of bits that you put in your modulation)
And you put the bits in a way that is inversally proportional to the depth of this pool.



Whereas this is $(S/N)^{-1}$, the bottom of the pool corresponds to a better value because I can put more bits in it (so the power of the modulation is higher where $(S/N)^{-1}$ is deeper.)

So there will be some empty bands that correspond to unused tones where the attenuation is the worst.

We have a theoretical maximum upstream and downstream bandwidth:
number of channels X bit/channel X width of subband.

In ADSL we have modems:

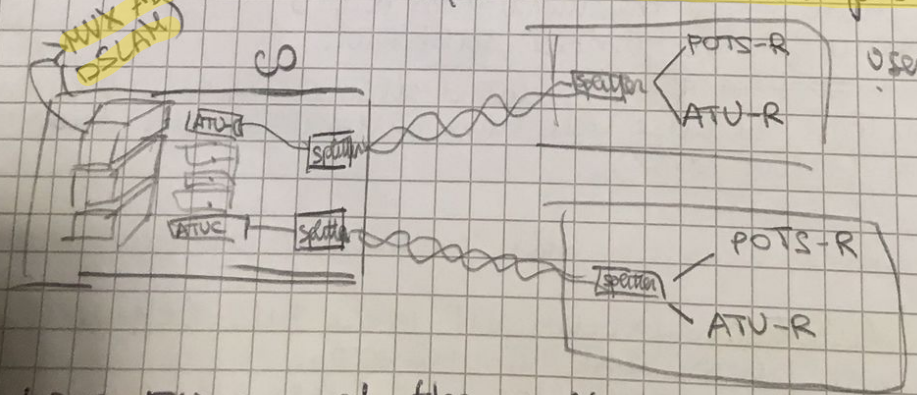
ATU-R: ~~terminal~~ ADSL termination unit - Remote side
(it is at the user side)

POT SPLITTER: it is a filter in the frequency band filtering on one side the frequency band dedicated to the telephone, and on the other side the up and downstream

ATU-R → POTS-R

Key point: what is present in pot splitter { POTS-R, ATU-R } is replicated in identical manner at the CO side. So in the CO ~~side~~ we have the splitter and the modem (DSLAM / ATU-C)

We have a splitter and a modem for every twisted pair



We have ATU-C and the result is multiplexed in an element that is called multiplexed DSLAM (DSL Access Multiplexer)

SPLITTER

- close to
- splitte
- you d
you h
ADSL
(it

N.B No
cab
w
S
co

VDSL

It evo
So wh
the V
cabin
In the
pair,
There
is no
optic
cabi

1 t

SPLITTER 3 types

- close to the modem (SPLITTERED)
- splitter distributed in the house (DISTRIBUTED SPLITTERS)
- you don't have the splitter (SPLITTERLESS) and this means that you have more interference from the telephone To the frequency of ADSL and vice versa.
  (It was used at the very beginning.)

N.B Now telephone companies include in buying DSL free telephone calls because the telephone calls, instead of being transmitted in the telephone band, are transmitted as bits. So they become bits that are included in your data, so the communication happens in the digital part of the DSL.

- VDSL (Very high digital subscriber line)

It evolves in this way: it reduces the size of the copper wire. So while until now the classical ADSL uses FTTE (exchange); the VDSL brings the fiber to the cabinet (FTTC) and from the cabinet we have twisted pair.
In this way we have reduced the distance crossed by a twisted pair, so we improve the bit rate.
There are two main costs here: ① we need more fiber (and the cost is not of the fiber itself) ② of the fact that we have to put an optical device (ONU optical network unit) so you need space in the cabinet.

① the cost of the fiber depends on the fact that you have to do works on the road to insert cables.

29/10/2018

IPV6 INTERNET PROTOCOL VERSION 6

It is a new version of Internet protocol (IP)

- the changes from IPV4 to IPV6 fall into the following categories:

  - expanded addressing capability

    in IPV4 addresses are 32 bits long. So we can write at most 2^{32} addresses (4 billion)

    Initially the main scope of an IP address was to uniquely identify an host on the internet. So we could have only 4 billion devices connected on the internet) It was enough when the internet was born, but not now.

    Now all devices need to be connected to the internet (for example sensors) so now we have to use many more addresses.

    In the '90 there was NETWORK ADDRESS TRANSLATION (NAT)

    It is still used.

    It takes the IPV4 addressing space and it divides it in 2 parts not necessarily equal. So we have the set of private and the set of public. The idea is that all those hosts that are required to be reachable from everywhere are assigned to a public address (servers) and they need to be global unique (I can't have 2 identical public addresses).

    The private addresses are designed to be used in private networks (such as LAN, home networks, enterprise networks). Inside the single private network we assign unique addresses but I have 2 different private networks I can use the same prefix. (With this solution I can reuse addresses)

    THIS IS A MIDTERM SOLUTION because there are some problems:

    - requires to play with layers that are upper with respect to the layer 3

    So as long TERM SOLUTION WAS DESIGNED IPV6

    In IPV6 the address space is so big that we will never have problems with the limited size of the address space

    In IPV6 addresses are 128 bits long so we can write 2^{128} different addresses.

    So there is no more need to divide addresses in private and public.

  - header format simplification

    reduce processing that is required to perform in each packet

    IPV4 in the header there were many fields and mandatory fields. But there were fields that were not used (like fragmentation & that I only use when I encounter a link whose is smaller than the packet length. So most of the time bits related to this field are set to 0. But you have to process them anyway

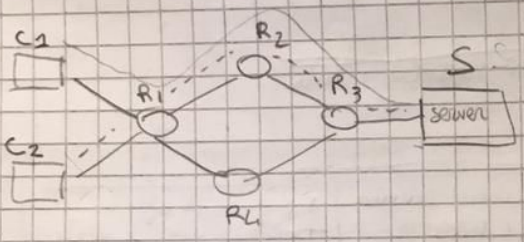
    So in IPV6 we create a basic header where only fundamental fields appear (destination, source addresses & etc).

All optional fields are remove. So header now has a fixed length and there are a lot of routers to do the processing, so they reduce the processing overhead of routers and it also determines a reduction of the delay of the processing.
This benefit is achieved in all the packets that generally only require basic services.

So in IPv6 we have the basic header with only mandatory fields plus an extension header that contains optional fields (I can add multiple extention header depending on the service that I need). • improved support for extensions and options

- flow labeling capability
add a label to each packet so the router knows that the packet belongs to a specific flow

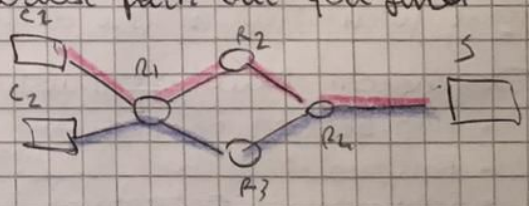
(ex) consider a network infrastructure



assume that this use IPv4.
So routers have to run a routing protocol and that will determine the port to go to deliver packets to the servers.

Assume that C1 wants to communicate with S and C2 wants to communicate with S.

They can go to the same path R1, R2, R3, S
But in this case there is a part in the net that is overloaded and the others not, so there is a possible congestion in one part and a waste of capacity in the other.
The solution could be to balance the load on the network. So with IPV4 you don't find a single shortest path but you find multiple shortest path.

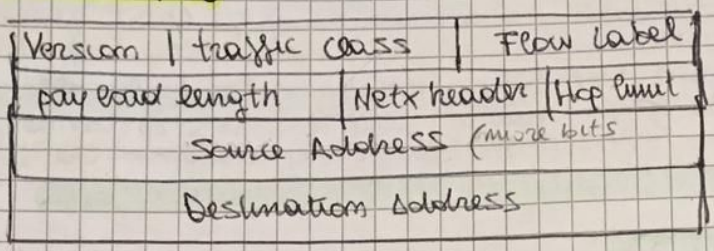


PROBLEM: The way flow balancing can be performed in this architecture is as follows:
R1 receives a packet, no matters which flow belongs to, It sends it to the upper port. R1 receives the second packet I decide to send to the down port. R1 receives the third packet and it sends it to the upper port. (So for each packet R1 sends it one up and one down)
Not a good way because at layer 4 there is TCP protocol which is sensible to out of order. (So if I deliver a packet on a flow out of sequence, TCP has to do a lot of work to reorder the packets and it will ask for retransmission.

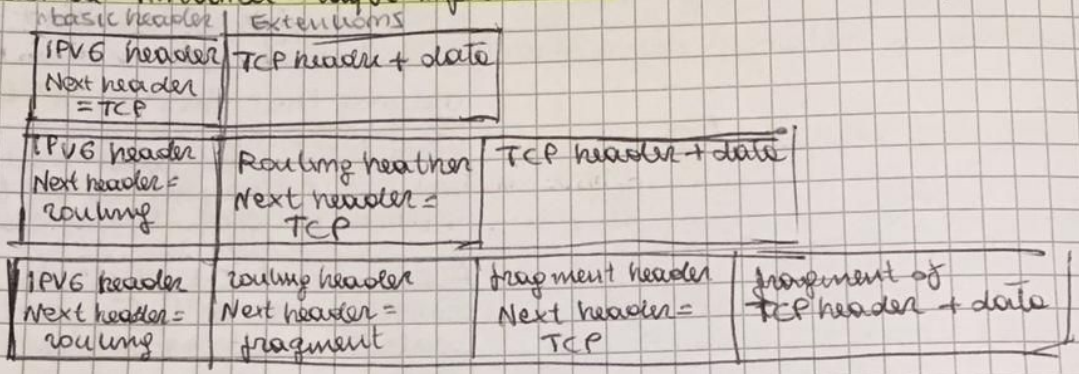
in IPv6 we can avoid this problem through labeling capability So R1 can understand from which client arrives the packet and then sends it on the right flow.

- authentication and privacy capability

BASIC HEADER IPV6



Optional internet-layer information is encoded in separate headers



PROCESSING AN IPV6 PACKET

Extension headers are not processed, inserted or deleted by any node along a packet's delivery path, until the packet reaches the node identified in the destination address field of IPV6 header

Extension headers must ~~appear only once~~ be of different types:

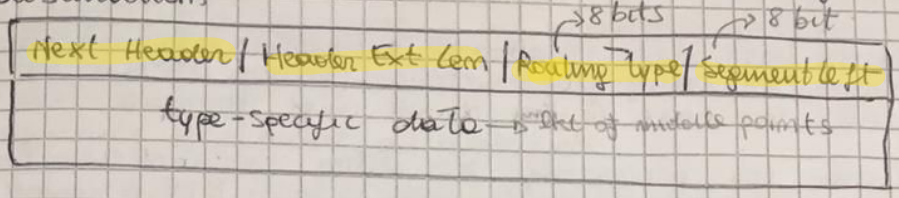
- Hop-by-hop options → it is allowed to be processed by intermidiate node. (it uses protocols)
- Fragment
- Destination options
- Routing
- Authentication
- Encapsulating Security Payload

The order is foundamental for headers:

1) IPV6 header
2) hop-by-hop options
3) Destination
4) Routing
5) Fragmentation
6) Authentication
7) Encapsulating Security Payload
8) Destination options
9) Upper-layer

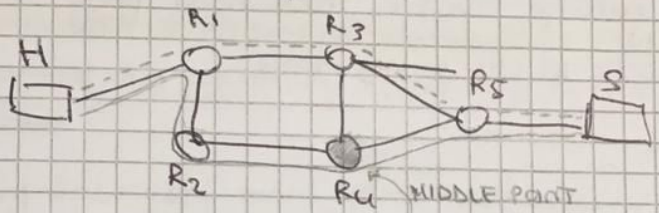
ROUTING HEADER

Allows the source node to specify a list of intermediate points that the packet has to go through before being delivered to the destination



It specifies a list of intermediate nodes that the packet has to go through before being delivered to the destination

ex



If it doesn't specify anything the packet will take this path

for example it could choose one router to be the middle point (ex: router R_4) this means that the packet must go through it

TYPE 0 ROUTING HEADER

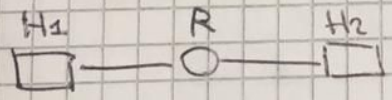
It has been deprecated because it creates problems about network security. It was used to create the (DoS) service attack in the network. It tried to create a congestion such that you have a lot of ~~packet~~ lost packets.

The vulnerability is that in type 0 routing headers the middle point is allowed to appear in a list of middle points as many times as we want. So this fact can be exploited by attackers

ex Attacker generate a packet that wants to reach the destination but the list of middle points to go through is always the same (for example A B A B A B). This makes the ~~pkt~~ packet to go back and forward as many times as he wants.
So it can create traffic in A-B link, and if we have a lot of packet, they can congest the link.

FRAGMENT HEADER

fragmentation in IPV4:



each link is caracterized by a parameter MTU (maximum transmission unit). It specifies what is the longest packet allowed to be transmitted over that link.

If the packet is longer than the MTU then the packet must be dropped
In IPV4 we have a service (FRAGMENTATION) which allows to send big packets over a link: it divides the packets too long in fragments short enough to be sent.
In IPV4 there are 3 field in the header to do fragmentation and reassembly: (~~FLAGS~~ IDENTIFIER (that is the same for all the fragments that are generated from the same packet →

FRAGMENT OFFSET: points at the first unit of the payload that is carried by the fragment. So we can reorder packages in the destination.
MFLAG: it is set to 0 only if the fragment is the last of the packet.

In IPV6 only the first node is allowed to perform fragmentation. It tries to reduce the use of fragmentation (because it is a waste of time & whereas you have to divide and recompose the packets).
So the pros are: less processing, less delay, overhead reduction
the cons are: security threats, need of path MTU discovery procedure

So in IPV6 in order to discover the capacity of each link during flow, before sending traffic each host performs a procedure called PLATEAU ALGORITHM to find the smallest MTU on the path and to divide the packets in the source node.

REASSEMBLY

An original packet is reassembled only from fragment packets that have the same source address, dest. address and fragment identification.

I want to receive all fragments and then using the fragment offset I determine the sequence fragments and step by step build the original packet.
Once I put together the fragments, I still haven't got the original packet because there are two different fields in the basic header that have a different value with respect to the original one:

- in the basic header there is the payload length that in the fragmentation needs to be reconstructed
- In the original packet, the next extension header is not the fragment one. So I have to go into the pre-fragment header (where I find the basic header + some extension headers) and take the last extension header that appear in it and in the next header field update the value (which now is pointing at fragment header) And I have to update it to the actual next extension header.

To find the length of original packet is obtained using this formula:

$$PL_{orig} = PL.first - FL.first - 8 + (8 * FO.last) + FL.last$$

- PL.first: payload length of 1° fragment
- FL.first: fragment length of 1° fragment
- 8: length of fragment header (8 byte = 64 bits)
- FO.last: fragment offset of last fragment (8 byte)
- FL.last: fragment length of the last fragment

30/20/2000

ERRORS IN REASSEMBLY

- Insufficient fragments are received (reassembly must be abandoned and all received fragments are discarded)
- the length of a fragment is not a multiple of 8 octets and the M flag is 1 (packet solo e ultimo pacchetto può avere num8 ottetti (discard the frame and send an ICMP Parameter problem to the source)
- Fragments of a packet are overlapped (reassembly of the packet must be abandoned, all received ~~packet~~ fragments are discarded and no ICMP ~~err~~ error msgs should be sent)

SECURITY THREATS RELATED TO FRAGMENTATION

each end device can decide by itself how to end a service

~~fragmentation~~

PACKET SIZE ISSUE

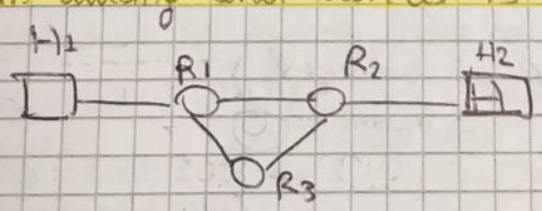
while in IPV4, every single node is allowed to do fragmentation, in IPV6 only the source node can. (it reduce the overhead)

The problem is that the source node is asked to create fragments that are ~~minimo~~ smaller or equal to the smallest MTU on the links in the flow.
The size of the smallest packet in a IPV6 should be 1280 octets

To know what is the minimum MTU among all links you do PATH MTU DISCOVERY: initially you know only the MTU of the first link, then on every node you see the MTU of the next link and you return it to the sorce node that update the new value of MTU. In the end the source node fragments the packets at the minimum MTU found.

PTMTDV and Black Holes

black holes occur when the network infrastructure is UP but connection among end devices is down



$H_1 \rightarrow R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_1$
black hole

possible causes: the routers are not sending PTB msgs
when the packet enters the loop it doesn't go out. So after an amount of Time the packet is considered ~~lost~~ missed.

Loop is easier to be detected

IPv6 SECURITY CONSIDERATIONS

IPv6 has security properties that are similar to IPv4
There are some problems:

- EAVESDROPPING
- PACKET INSERTION
- PACKET MODIFICATION
- MAN-IN-THE-MIDDLE
- DENIAL OF SERVICE

IPV6 ADDRESSING

IPv6 addresses are 128-bit long.
There are three types of addresses depending on the type of communication:

- UNICAST: used for client-server applications
- ANYCAST: the source node wants to send a msg to a device in a given set of devices (not really interested of which one will receive the msg.)
- MULTICAST: is for multicast communication (live streamings, web radio, web TV). There is a source node which is sending traffic to a set of users.

N.B. We don't have broadcast in IPv6

TEXT REPRESENTATION OF ADDRESSES

The general form for IPv6 is x:x:x:x:x:x:x:x (128-bit, 16-bit)
we use the four hexadecimal digits of the eight 16-bit pieces of the address.

ex ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
2001:DB8:0:0:8:800:200C:417A

It is not necessary to write the leading zeros in an individual field. There must be at least one numeral in every field. You can not omit the final zeros

The use of "::" indicates one or more groups of 16 bits of zeros (it can appear only once in an address).

ex 2001:DB8:0:0:8:800:200C:417 → 2001:DB8::8:800:200C:417 (UNICAST ADDRESS)
(in general unicast starts with number 2)

FF01:0:0:0:0:0:0:101 → FF01::101 (MULTICAST ADDRESS)

0:0:0:0:0:0:0:1 → ::1 (LOOPBACK ADDRESS)

0:0:0:0:0:0:0:0 → :: (UNSPECIFIED ADDRESS)

ex FF01::80:0:1 => FF01:0:0:0:8:0:0:1
FF01:0:0:8::1 => FF01:0:0:8:0:0:0:1
(so they are not the same address)

IPV6 ADDRESS PREFIX

an IPV6 prefix is represented by the notation ipV6-address/prefix-length

- ipV6-address is an ipV6 address
- prefix-length is a decimal value specifying how many of the left most contiguous bits of the address comprise the prefix

ex 2001 (exadecimal) : 0DB8:0000:CD30:0000:0000:0000:0000 / 60 (number of bits)

↳ each group represents 16 bits
whereas the prefix-length is 60 it means that I have to consider only the first 64 bits → 2001:0DB1:0000:CD3 (PREFIX IDENTIFIER)
all the other numbers belong to interface identifier.

I can also write it in the abbreviation way:
2001:0DB8::CD30:0:0:0:0/60
2001:0DB8:0:CD30::/60

I CAN'T WRITE:
2001:0DB8:0:CD3/60 → because CD3 = 0CD3 ≠ CD30
(if I have only 3 numbers in one group, it means that the missing 0 is the leading one)

2001:0DB8::CD30/60 => 2001:0DB8:0000:0000:0000:0000:0000:CD30
(quando non è lo stesso indirizzo di partenza)

2001:0DB8::CD3/60 => 2001:0DB8:0000:0000:0000:0000:0CD3:0030
(quando non va bene mettere questo)

Address type	Binary prefix	IPV6 notation
Unspecified	0.0...0 (128 bits)	::/128
Loop back	0.0...1 (128 bits)	::1/128
Multicast	1.1.1.1.1.1.1.1	FF00::/8
Link-local unicast	1.1.1.1.1.1.1.0.1.0	FE80::/10
Global unicast	(everything else)	

Anycast addresses are taken from the unicast address spaces

ADDRESS SCOPE

How these addresses will be used?

The global unicast addresses and public IPV4 addresses are similar. Global unicast are required to have connectivity. Every server must have the global address. The main difference between global unicast in IPV6 and IPV4 is that while in IPV4 public addresses are assigned only at servers, global unic. addr. are assigned also to host's.

Global unic. addr. ask for public addres. and can be routable over the internet

If we are in the subnet of a network we can use Link local address instead of the global one.

If we want to allow the communication with other subnet works we can use SITE addresses

INTERFACE IDENTIFIER

Interface identifiers in IPV6 unicast addresses are used to identify interfaces on a link.

They are unique within a subnet prefix

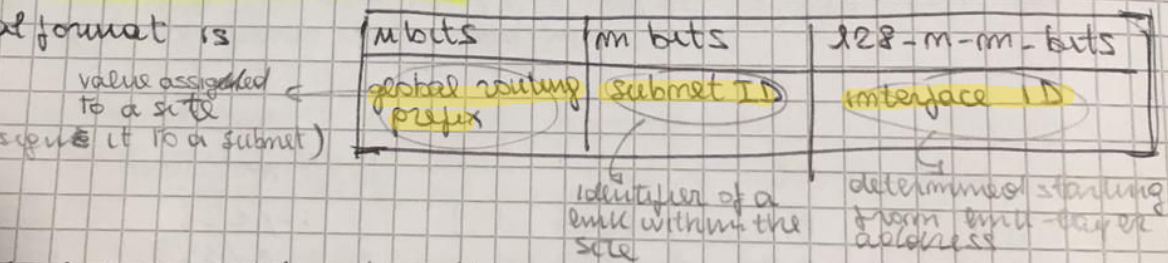
An II can be derived directly from that interface's link-layer address:

- Split the MAC addr. in 2 strings 24-bit long
- insert the hexadecimal string FFFE in between the two obtained parts
- flip the 7th most significant bit

II=I is considered for multicast addr's. except those starting with 000

GLOBAL UNICAST ADDRESSES

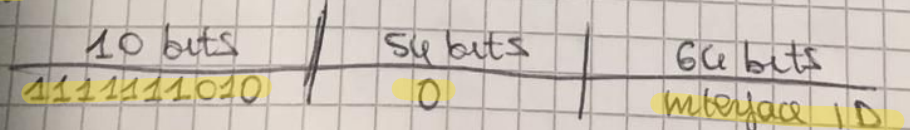
general format is



All global unic. addr. other than those that start with 000 have a 64-bit interface ID field (i.e. n+m=64)

LINK-LOCAL IPV6 UNICAST ADDRESSES

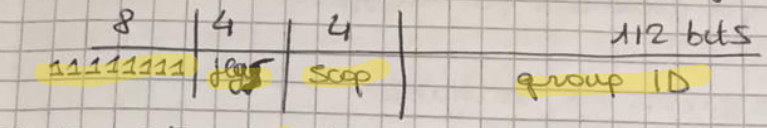
are designed to be used for addressing on a single link for automatic address configuration, neighbor discovery, when no routers are present



Routers must not forward any packets with link-local source or destination addr. to other links.

MULTICAST ADDRESSES

An IPV6 multicast address is an identifier for a group of interfaces
An interface may belong to any number of multicast groups



- flgs is a set of 4 flags : 0/R/P/T
  T=0 permanent address (well-known) used for configuration
  T=1 non permanent address (running an application)
  R, P → used for special purpose

- scop is a 4-bit multicast scope value used to limit the scope of the multicast group
  1 : interface local scope
  2 : link local scope
  ⋮

ex let's consider "NTP servers group" and we want to assign a permanent multicast address with a group ID of 101

FF02:0:0:0:0:0:0:101
↳ reach all NTP servers that are in the same link as the sender

FF05:-----
↳ in the same site

FF0E
↳ all NTP servers in the internet (so I use the global one)

WELL-KNOWN MULTICAST ADDRESSES

- All nodes addresses (depending on the scope you send the msg to a different range of nodes)
  FF01:0:0:0:0:0:0:1 (interface local)
  FF02:0:0:0:0:0:0:1 (link-local)

- All routers addresses
  FF01:0:0:0:0:0:0:2 (interface local)
  FF02:0:0:0:0:0:0:2 (link-local)
  FF05:0:0:0:0:0:0:2 (site-local)

IPV6 Subnetting -

NEIGHBOR DISCOVERY

nodest use it to
- determine the link-layer addresses for neighbors
- purge cached values
- find neighbor routers
- keep track of which neighbors are reachable.
- detect changed link-layer address

the procedure is based on the following IPV6 addresses:
- all nodes multicast addresses
- solicited nodes multicast addr.
- link-local addr.
- unspecified addr.

MESSAGES

Router solicitation
(prompt routers to generate router Advertisements quickly)

Router Advertisement
(routers send out rout. Adv. msgs periodically, or in response to Router solicitations).

Neighbor solicitation
from a host to another host (generates an answer)

Neighbor advertisement

Redirect

~~HOST CON~~
SENDING ALGORITHM

ROUTER DISCOVERY

- it is used to locate neighbor routers
  it uses a link_local addr and a multicast to all other routers
  there is a periodic advertisement sent.
  So the host can have information ~~on~~ of all routers on the network.
- it is also used to do duplicate address detection (DAD)
- Another one is NS spoofing.
- Unsolicited NA

HOST CONFIGURATION

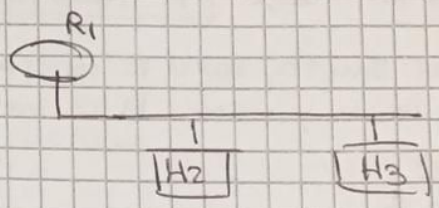
There are three ways a host can get an IPV6 address:

- manual configuration
- stateless configuration (created automatically) (SLAAC)
- stateful config. (DHCPv6)
  - the host can get the IP address and directly from DHCP server
  - the address is automatically computed by the host while the other parameters are given by the DHCP server when we generate an addr AUTOM. the addr. has a time validity.

stateless configuration

SLAAC

H3 connects to the subnet and generates an IPv6 link local addr.
It uses Duplicate address detection to verify the uniqueness of the generated address.



4/11/2020

IKE / IPSec

Network security services:

- confidentiality: only sender and intended receiver can understand msg contents (encryption and decryption)
- authentication: sender and receiver want to confirm identity of each other
- msg integrity: sender and receiver want to ensure msg not altered without detection
- access and availability: service must be accessible and available.

A and B want to communicate "securely" but an intruder T may intercept, delete or other on msgs.

ATTACKS:

- eavesdrop: intercept msgs.
- insert msg into connection
- impersonation: can fake source addr in packet
- hijacking: ongoing connection by removing sender or receiver inserting himself in place
- denial of service (DoS) prevent service from being used by others

m = plaintext msg.
$K_A(m)$ = ciphertext, encrypted with key K_A
$m = K_B(K_A(m))$

SYMMETRIC CRYPTOGRAPHY: A e B share same (symmetric) key: K_S
PUBLIC KEY CRYPTOGRAPHY: B has 2 keys (K^- private and K^+ public)
A encrypts with B public key and B decrypt with his private key

MESSAGE DIGESTS

large msg m ⟹ [H: hash function] → $H(m)$

goal: fixed-length, easy to compute digital "fingerprint"
- apply hash function H to m, get fixed size msg digest $H(m)$

Hash funct
- many to 1
- produces fixed-size msg digest (fingerprint)
- given msg digest x, computationally infeasible to find m such that $x = H(m)$

(I can easily encrypt m but I can't decrypt it)
Hash function is a one direction function

DIGITAL SIGNATURES

we want to replace the service (to be sure that no one modified the msg)
- B signed m
- no one else signed m
- B signed m and not m'

B) long msg m → Hash function → $H(m)$ → digital signature
encrypted msg digest $K_B^-(H(m))$

A) take signature and decrypt → decryption → m
A → H function → m ⟷ Equal ? ⇒ OK

CERTIFICATION AUTHORITIES → is encrypted in the signature. The certif. Auth. certifies that the sender is bob

CA binds public key to particular entity E.
E (person, router) registers its public key with CA.
- E provides proof of identity to CA
- CA creates certificate binding E to its public key
- certificate contains E's public key digitally signed by CA-CA says: "this is E's public key".

↳ IPSECURITY sopra servizi applicativi livello alto

12/11/2020

IP SECURITY SCENARIOS

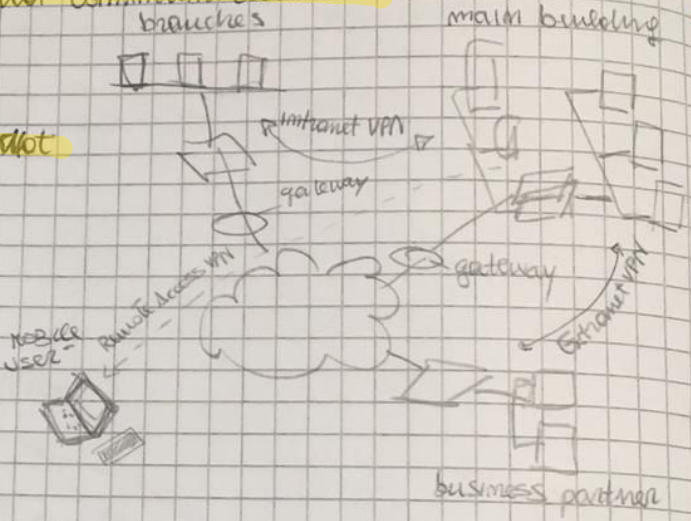
IPsec provides the capability to secure communications across LAN, private and public WANs, internet

There is a big company with a main building and in other parts of the country there are offices (different branches). ~~The offices~~ These branches are connected to the main ~~building~~ building through public Intranet.
(so I can communicate between branches and main building with private addresses)

- Can we protect only gateway-gateway communication By using IP-SEC or we can protect end-to-end communication?
(We can do both)

In the second case we want to communicate securely over the internet using a business partner
(we use EXTRANET)

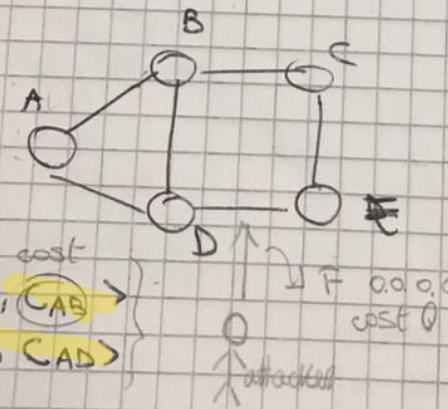
The third case is when we want to communicate securely through mobile users
(REMOTE ACCESS VPN)



ROUTING APPLICATIONS

GLOBAL ROUTING ~~APP~~ PROTOCOL: In order to ~~~~ fulfil the routing table each router needs to know the network topology entirely. Since a router is a machine attached to the network, it doesn't know nothing of the network where it is working, it has to run a protocol and exchange msg with the neighbors to discover how the network is made.

ex



LSA A { <(A,B), CAB> <(A,D), CAD> ...
link
cost

starts from A, at the end we know all routers and links in the network

The routers are discovered using LSA (link state advertisement)
It also contains the cost of each link. (in this way I can find the shortest path).

Once that the LSA is created, it is sent to all neighbors of A and this is the so-called FLOODING

/11/2020

FLOODING: the router B receives the LSA from A and it finds out the link between A and B and its cost.
~~The~~ the same for D.
Then B and D send their LSA to C and E (not to ~~the~~ A because we have already explored this link).

in this way we build the network topology.

- The problem is that ~~when~~ when a router receives the LSA, it ~~has~~ Thrust the content of the LSA.
So if one attacker tries to ~~create~~ create incorrect information in LSA the router will take them as correct (SPOOFING)

For example: an attacker creates an LSA where a node F with address 0.0.0.0/0 has cost 0
(that means that you can reach the internet with cost 0).
In this case the routers ~~that~~ in the network thrust this LSA and every router sends information and packets to this node F that doesn't exists.
This lead to a huge congestion on link DE and all the packets will never reach the destination.

- An attacker could also take a real LSA and change some information in it

The services that we need to have are: authentication of the source and the msg integrity. ~~In this way~~

IPSEC SERVICES

- It is used by two different protocols
  - authentication protocol designed by the header of the protocol (AH)
  - encryption/decryption protocol designed ~~from~~ by the format of the packet for the protocol (ESP).

- The services are:
  - access control
  - connection integrity
  - Data origination authentication
  - Rejection of replied packets
  - confidentiality
  - Limited traffic flow confidentiality.

- IpSEC provides security services.

AH = authentication header (doesn't provides confidentiality and limited traffic flow)
ESP (encryption only) (doesn't provide connection-less integrity and data origin auth...)
ESP (encryption and authentication) (provides everything)
ESP = encapsulating security payload.

IP SECURITY ARCHITECTURE

SECURITY ASSOCIATIONS

- In general two peers in an Ip sec communication need to create the security association to get security services.
A security association is a ~~one~~ one way relationship between a sender and a receiver. ~~It~~ The configuration file has to be negotiated with the other peer.
The protection is only in one direction sender → receiver or rec → send
If we want in both directions (inbound and outbound) we have to create another pair of security associations.
The association specifies a set of parameters:
  - spi: ~~identifier~~ identifier for security associations.
    the spi of a certain association is the same in both peers
  - transform: algorithm used for encryption is esp-des.
  - in use setting: tunnel mode
  - sa timing: time assigned to every security association.
  - replay detection support: N
- Associations on the same peer but for different directions (inbound and outbound) have different spi. (because they are different entities).

SPI (SECURITY PARAMETERS INDEX)

It has a local meaning (this means that could exist another device using the same SPI).
It is like a key to distinguish different security associations.
It enables the receiving system to select the SA for processing the current packet

IP DESTINATION ADDRESS

the destination depends on the direction of the association
It cannot be a multicast address because only unicast addresses are allowed

SECURITY PROTOCOL IDENTIFIER

AH authentication header
ESP encapsulating security payload.) AH or ESP.
We cannot use both in a single security association

A security association (SA) is defined by these parameters:

- sequence number counter: number that the sender includes in every super packet (different for every different packet)
- Anti-replay Window:
- AH information or ESP information
- Lifetime of the SA
- IPSec Protocol Mode (tunnel, transport)
- PATH MTU (for fragmentation)

Every SA in a gateway will be installed in the security association database (SAD)

SA SELECTORS

We want to give the gateways the possibility ~~where~~ whether a packet has to be processed according to IPsec or not and in case the packet must to be protected, what type of association I have to use.

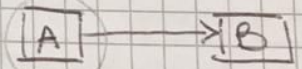
We use SECURITY POLICY DATABASE (SPD) that sets traffic filters for SA. (We can consider a traffic filter like a routering rule where we also specify the source and destination address, the port number of source and destination, the type of protocol and so on.

So we have 2 different databases for security gateways: Association database (SAD) and security policy database (SPD)

> tratta il traffico

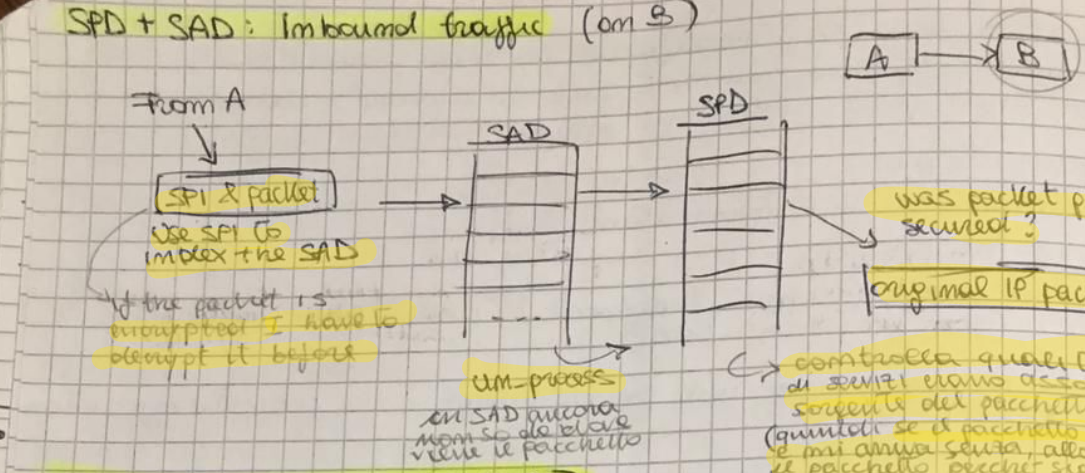
SPD + SAD: Outbound traffic (on A)

When the traffic leaves the device we referred to as IPSec traffic. (But before B becoming IPSec it is only IP packet)



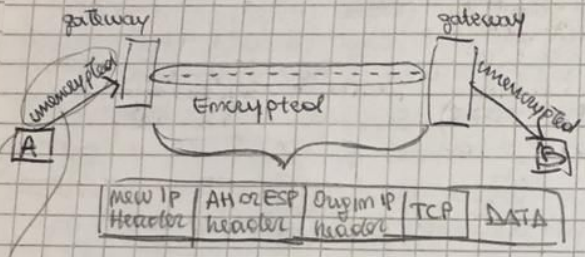
SPD contains entries which define a subset of IP traffic and point to an SA for that traffic.

SPD + SAD: Inbound traffic (on B)



TUNNEL VS TRANSPORT MODE

TUNNEL MODE



here msgs are sent like plain text

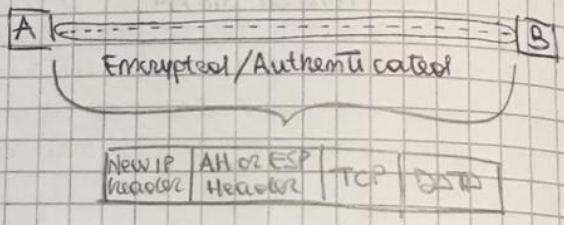
In the Tunnel mode the packet is encapsulated into another IP packet
In this IP packet the source address is that of the first gateway and the destination address is the second gateway.

CONS: bigger overhead because we are increasing the packet length because we put the origin IP gateway IP header

PRO: but with a single security association we can protect many more traffic flows

But we can't be sure if the first and the last part (from A to gateway and from gateway 2 to B) are secure channels

TRANSPORT MODE



in the transport mode the original packet is directly sent by including the IPSec header

PRO: reduces the overhead provides end to end service

In this case we are protecting a single communication

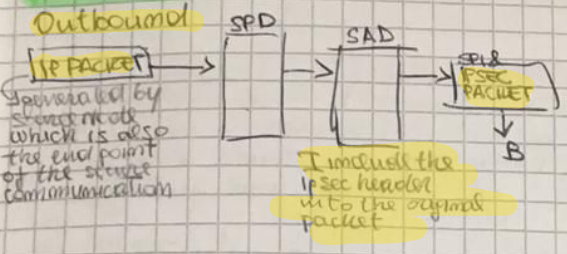
N.B. While for host-host communication we can decide to use either transport or tunnel mode, in case of gateway to gateway communication we must use tunnel mode

Si usa la tunnel per sfruttare la struttura IPV4 per IPV6 senza rifare tutto

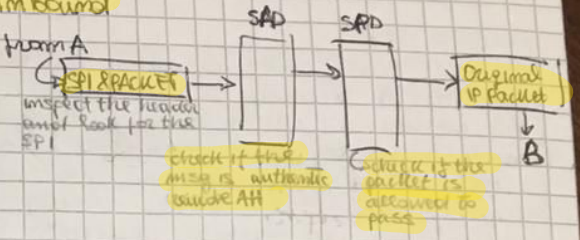
Apply transport or tunnel mode to Outbound traffic.

TRANSPORT

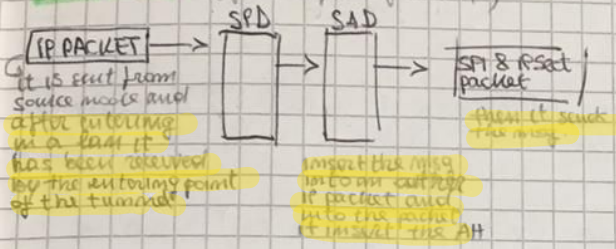
Outbound

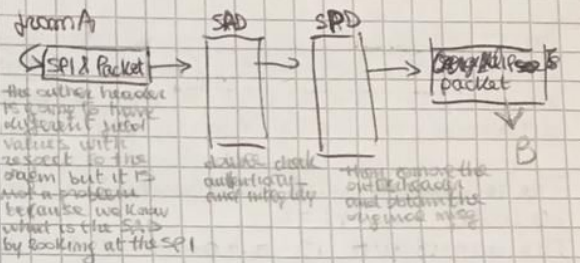


Inbound



TUNNEL (gateway to gateway)





~~In transport c'è bisogno di meno security and not tunnel mode~~

(AH) In transport mode is going to protect (by authentication and integrity) the full IP payload plus some header fields in the original header
~~Tunnel mode tutto header e tutto il pacchetto (che non è encrypted)~~

(ESP) In transport mode encryption of the payload of the packet
~~Tunnel encrypt l'intero intero pacchetto~~

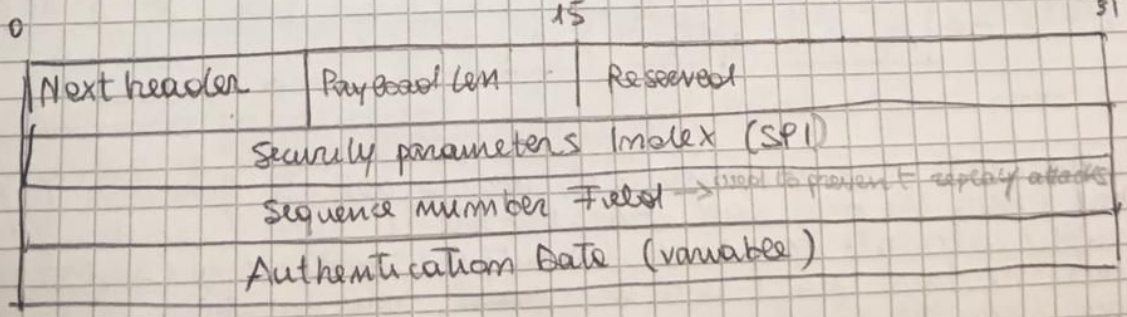
(ESP with authentication) In transport is going to protect only the payload (so is weaker than AH). We encrypt IP payload and authenticate it (but not the header).

If we want to get all the services in the entire original packet we have to use Tunnel mode

AUTHENTICATION HEADER (AH)

It provides support for data integrity and authentication of IP packets
It prevents and protects against address spoofing attacks and replay attack

IPV6



ANTI-REPLAY SERVICE

A replay attack is one in which the attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.

SENDER SIDE

the first time two security gateway communicate, they have to negotiate a security association. In that moment, the source (the outbound with respect to the traffic) initializes a variable (which is the sequence number) to 0. Everytime it sends a new packet using that SA it increments the counter and includes the number into the sequence number field of the AH.
In case the seq. numb. reaches the value $2^{32}-1$, it should go back to 0, so it terminates the SA and negotiates a new SA with a new key.

per mantenere elevato livello di sicurezza

RECEIVER SIDE

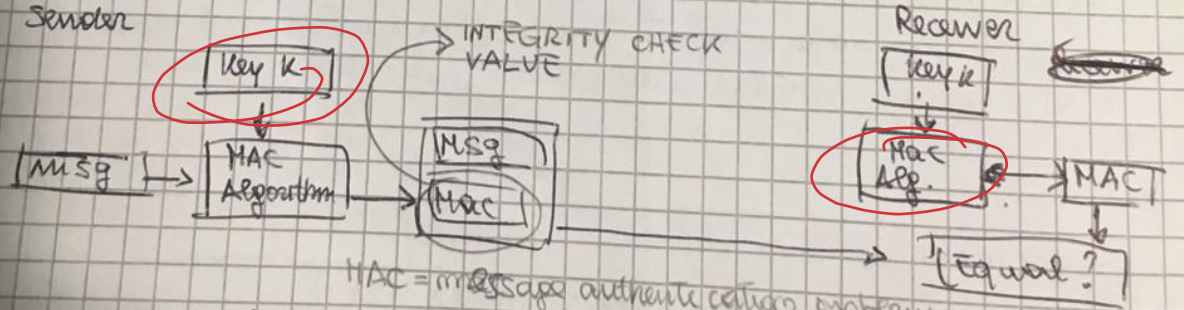
IP is connectionless, (main difference with respect to TCP), unreliable service, so there will be no guarantee that packets will be delivered in order (or simply delivered)

The receiver should implement a buffer (window of size W) with a default of W = 64.
The window is a range of sequence numbers that the receiver is allowed to receive and it has a fixed length.
In case we receive packets with a sequence number smaller than the smallest sequence numb. in the window, we have to drop them.
When I receive a valid packet, the window slides on, however ~~if one of the segues~~ when the windows slides, if I haven't received a packet with a certain seq. num yet, I lose it. (the packet is considered lost) Quando i pacchetti arrivano sulla parte a DX invece la finestra scorre per far entrare 10 (i pacchetti che non sono arrivati prima del 10 vengono eliminati)
(Non vengono accettati pacchetti con sequence number troppo basso e che sono più vecchi di un tot tempo)

INTEGRITY CHECK VALUE (it is authentication only)

(the msg non è stato cambiato)

An authenticator is a small string that provides the receiver a proof of the identity of the sender. The idea is that we want to verify wheather the sender knows a secret only key is supposed to know.



MAC = message authentication problem

To calculate the authenticator we use a hash function (MAC Algorithm) that takes the msg and concatenate it with a secret and it simply calculate the hash. → output: small string (DIGEST)
Since the hash funct is a long ~~short~~ way function, nobody else apart from the source can generate a MAC. MAC (which is the integrity check value) is inserted in the authentication data of the AH.

At the receiver side, the receiver knows the secret key because it has been negotiated before with the sender.
It applies the same MAC Alg used by the sender and if it finds a MAC which is equal to the one carried in the packet (integrity check value), then the sender knows the secret;
And in case the msg was generated by the sender but it has been modified, the two MACs will not be equal so the packets will fail.

Non tutti i campi servono per calcolare l'HAC (non ci sono quelli che variano da sorgente a destinazione ex. time to live del pacchetto)

The ICV is a msg authentication code produced by a MAC alg. at it can be HMAC-MD5-96 or HMAC-SHA-1-96
(takes only the first 96 bits)

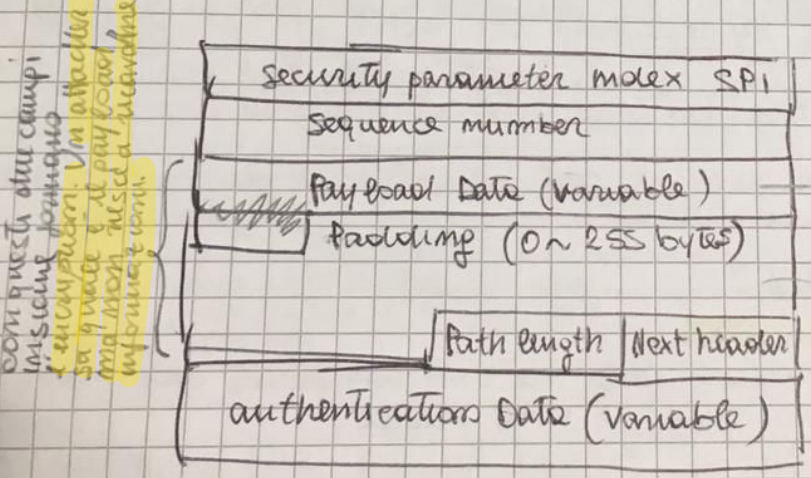
Not all IP-header fields are going to be authenticated because some of the header fields change value while transiting from the source to the destination

ex Destination address (is a mutable field but it is predictable)
in IPV6 we have the routing header in which we change every time from a router to another the destination address.

confidentiality
encryption and authentication)

ENCAPSULATING SECURITY PAYLOAD (ESP)

it provides confidentiality services (and it can also provide an authentication service)



To encrypt the payload we can use different algs.
in IPV4 we encrypt only the payload of the original msg (TCP+DATA+ESP)

In IPV6 tunnel mode we can protect (encrypt) the entire original packet plus the authentication of external ESP header.

PASSIVE OPTICAL NETWORK (PON)

13/11/2020

We use optical network ~~Becau~~ because of the performance of the fiber. (it can provide 10 Gbits of speed and it is able to reach long distances)
This is done by replacing part of the infrastructure that was built by using copper cables with fibers.

fibers have specific characteristics:

- When we talk about fiber we talk about trasmission at some specific wavelength (nm).

- la fibra (it is a range of values): 1310 nm, 1550 nm (nanometers) } perché qui l'attenuazione è bassa e costante

(fibra viene usata dove c'è banda costante e attenuazione bassa)

In these two windows we have important caracteristics:

- ATTENUATION: the attenuation is almost flat in our channel frequency band (The attenuation is the behaviour in the channel)

quando attenuazione è bassa e costante allora la fibra si può definire bene

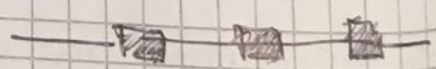
- FLAT CHANNEL: we can see from the picture that the bands are flat.

So through attenuation and flat channel we can have very good performances for fiber. (And these good perform. are related to fiber bitrate)

How the trasmission in the fiber is done?
It is done by sending a signal of light at a given wavelength (Tipically the fiber operates by reflecting the light at the endend)
This can cause some dispersion (riflessione) of our light power but in fiber the dispersion is very low so the performance at the end are very good.
There are no ways to lose signal out of the fiber so this is way they are very competitive as a media.

How is the light trasmitted?
It is transmitted by using LASERS. → sono dei rigeneratori, quindi ripristinano il segnale
Lasers provide good performances in the two windows we have presented and as you know they are very precise

In the fiber cub we find some rigenerator elements that are fully made in the optical domain. So it means ~~that~~ that enters light and exits light and these amplification of light can be done by some material that can bust the light power.



In general we use fiber cables for very very long interconnections (~~oceanic~~ oceans are crossed by fiber cables)