A TELECOMUNICATIONS NETWORK MODEL (Slide 0)

8/10/2020

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

The networks are divided into tree areas:

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

LAN (Local area network)
smaller extension (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)
  (it can be used only by few users, that are authenticated by credentials)
  ~~Pub~~ Public network and private user 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 ~~ha~~ have the same role

- **CLIENT / SERVER Networks**

  server applications can be very difficult

  CLIENT: ~~end~~ user PCs

  SERVER: helps with application processing and also manages the network.

My smartphone ~~is a server~~ 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 (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 (we can cover more area) Using satellites and antennas
  - 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 base 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.

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.

9/10/2020

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

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. (base 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

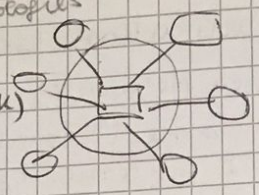
→ easier to update when technology updates

other differentiation is that by topologies

NETWORK TOPOLOGIES

devices are connected to a same device called access point.

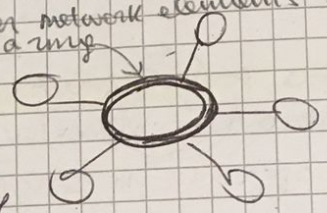
- **STAR** —> is used in corner network (not in core network)
  - Ties and user computers to a central computer
  - Consider the less reliable



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.
Single point of failure. (if there is an error the network stops but only other network elements

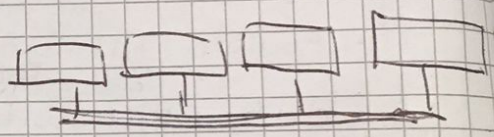
- **RING** (TOKEN RING) —> different user, not the media shaped in a ring
  - Ties local computer processors together in a ring on a more equal basis.
  - Considered more reliable and less costly



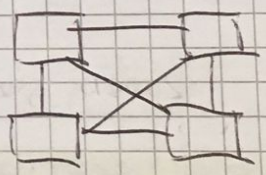
ADVANTAGE: if something is broken, I can run the ring on the other direction to reach all points connected

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
  - ~~TBE~~ is a variation which ties ~~every~~ 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 thank 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

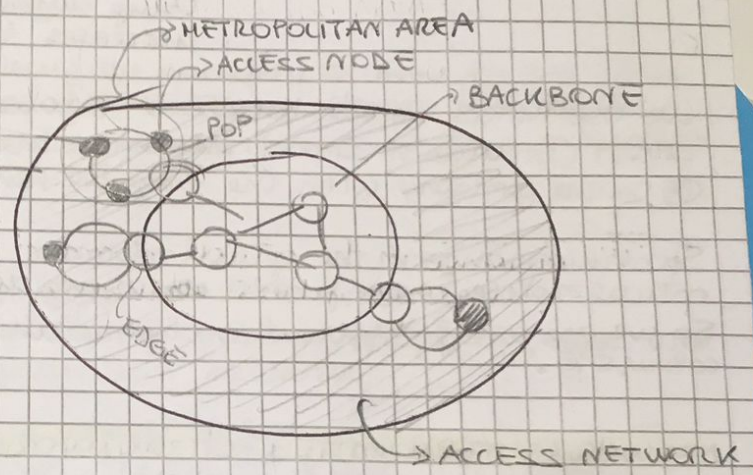
We use very different technologies for the access: ~~while the core evolved by the~~ ~~ITU~~ communication carriers have used ~~COPPER LINE~~ COPPER LINES.

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 telephone network and it is used for all ADSL family.
  wired
  short range
  Provide access from the peripheral 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

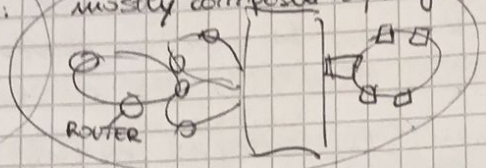
There are other differences for example security, cost, coverage, data rate.
The ~~wi~~ wired ones are faster than wireless, but cellular access is faster than copper (especially the 5G)
Wired is more stable than mobile (unless damage in wire)

EXEMPLE OF TELECOM ITALIA

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

BACKBONE NETWORK

The backbone is mostly composed by rings using fiber



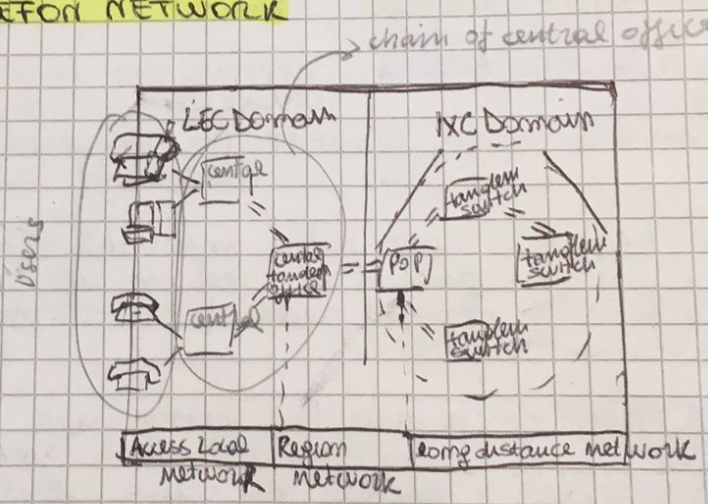
FIBER WORKS EXCHANGING LIGHT, so the router are able to transfer different colours. So different colours represent different subcarriers
Using different colours at the same time increases the capacity of the fiber

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 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 carrier is an operator)



- Incumbent LEC (ILEC)
  is the starting owner 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 carries in the local area that are Incumbent. 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

link between user and network (slide 2)

LOCAL LOOP (the last mile)

25/10/2020

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

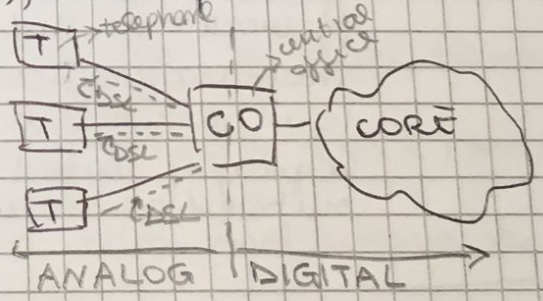
To prevent the owner from using the monopoly to monopolize other fields of trade, some ~~utilities~~ jurisdictions require utilities to UNBUNDLE the local loop : that is make the local loop available to their competitors.

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~~ add DSL ~~to~~ 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 (yellow line) and local loops that use fiber (red line 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 element are interconnected to other elements like the Mobile swither 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 ~~is that~~ 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) ~~and~~
(an example is ~~802.15~~ 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.

BACKBONE

links connect one continent to another using submarine cables

The access for the backbone is provided by using wired links that are implemented by using ~~fiber~~ 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

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 asymromous Transfer mode (ATM) and gigabit Ethernet (GbE)
On layer 3 we implement multiprotocol Label switching.

~~[illegible]~~

22/10/2020

XDSL

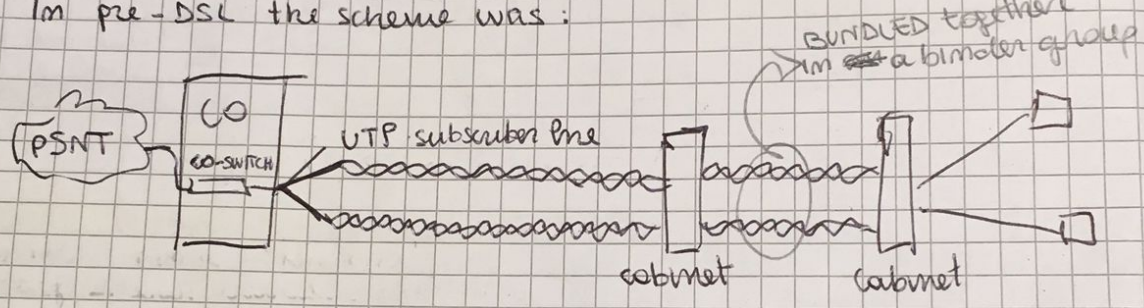
XDSL is a family of technologies that provide digital data transmission over the wires of a local telephone network.

DSL originally stood for digital subscriber loop

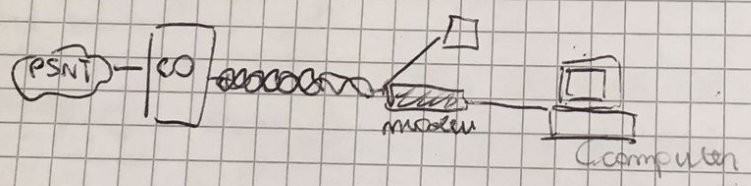
- **IDNS**: this solution used the same copper line of telephone network but provided 2 copper wides because

(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 wire to be transformed into an analog form, so~~ 4H
So 4 KHz was enough bandwidth 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

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

W → bandwidth (or B)

C → data rate or channel capacity

SNR is in db (SIGNAL TO NOISE RATIO)

In the next years there were other solutions (x DSL)

- **X** stand for the different options that we have for DSL for instance 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 DSL)

what is the winning point?

- the fact that it is asymmetric. it is almost random result because when the happens the interest of having digital services at home was driven by the video on the manod 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 surf 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 POTS (voice) telephone network)

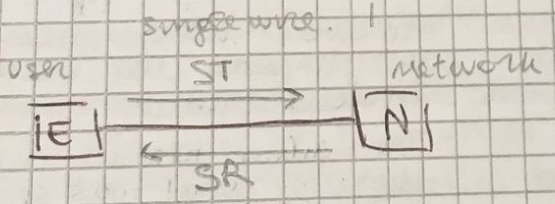
25.875 KHz - 133 KHz Upstream

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 transmit contemporary data in up and downstream through the operation called **ECO CANCELLATION**

ex



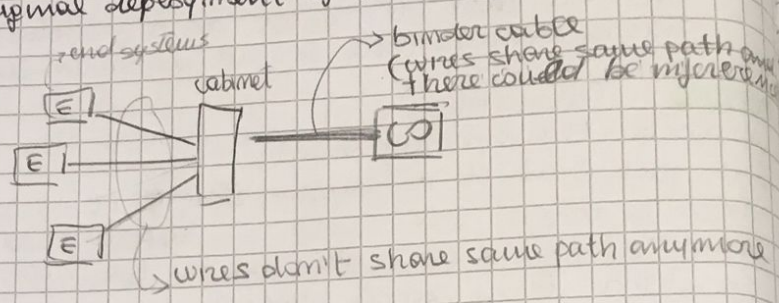
the communication is intrinsically bidirectional (same bandwidth, same time). How can I control that the two do not interfere? there is no way. But I can do ECO CANCELLATION

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.

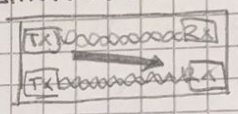
CROSS-TALKS

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

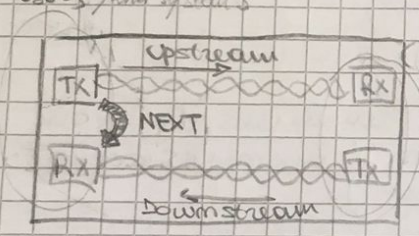


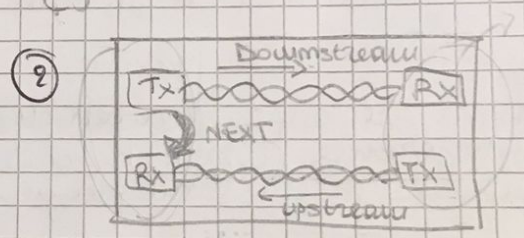
This interference has two names: FEXT or NEXT

FEXT (Far-end cross-talks)
it is the cross-talk between a transmitter and a receiver placed on opposite sides of the cable



NEXT
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:





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 ~~betw~~ different users that use different cables.
So this means that NEXT must be in CO, so downstream and upstream are inverted

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 ~~also~~ full bandwidth in downstream
The solution is that the the CO, knowing what was sent in downst, 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

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

MODULATION

23/10/2020

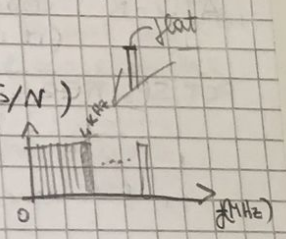
is a way to create a shape of the signal that is going to transport the bits. (We are talking about digital comunication)
There are different schemes:

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 ~~one~~ this signal is quite large, the frequency behaviour in the spectrum is not ideal.

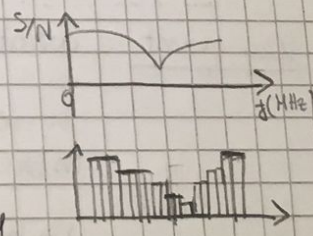
Which is an ideal behaviour in a spectrum band? It is when you have an attenuation (as a function of the frequency) ~~to~~ flat, that is all the frequences are attenuated in the same manner. So while it is quite easy to assume that the channel is flat, when the bandwidth is large it is complex to have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

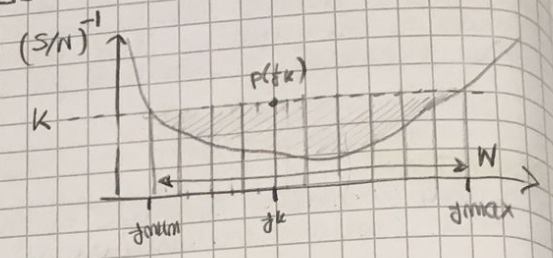


So in each ~~subchannel the~~ subband the channel becomes flat and for the frequences in that subband you can ~~characterize~~ characterize the attenuation with a value which is the same for the whole subband.
~~This multi tone modulation~~ So it is called discrete because you divide it in subparts. MultiTone 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 (efficient modulation) when you have low attenuation.
On the contrary, you have to put less bits (less efficient 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 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 when the attenuation is the worst.

We have a theoretical maximum upstream and downstream bandwidth:

number of channels X bit/channel X width of subband.

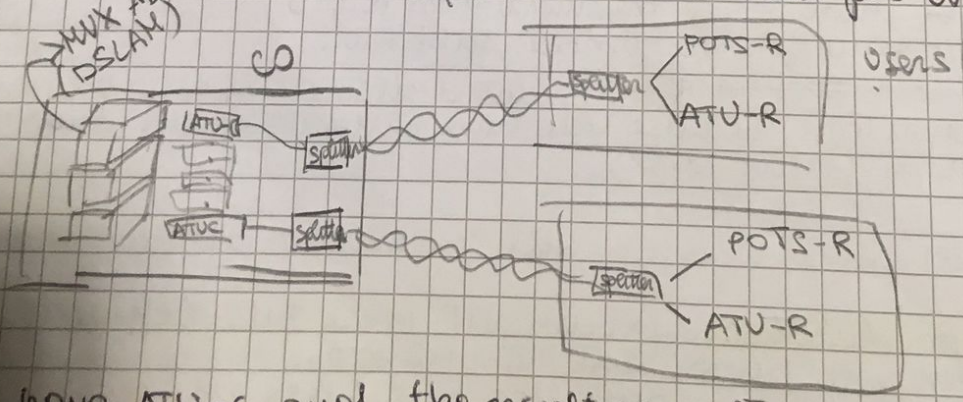
In ADSL we have modems:

ATU-R : 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 downs stream
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 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 3 types

- close to the modem (SPLITTERED)
- splitter distributed in the house (DISTRIBUTED SPLITTERS)
- you don't have the splitter (SPLITTELESS) 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 ~~calls in~~ in buying DSL free telephone calls because the telephone calls, instead of being transmitted in the telephone band, are transmitted as bits ~~in a way~~. 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.

~~[illegible]~~

IPV6 INTERNET PROTOCOL VERSION 6 (29/10/2020)

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) ~~are very~~ 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 ~~public~~ 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 if have 2 different private networks I can use the same prefix. (With this solution I can reuse addresses)
THIS IS A MIDDLE TERM SOLUTION because there are some problems:
- requires to play with layers that are upper with respect to the layer 3

<u>So as LONG TERM SOLUTION WAS DESIGNED IPV6</u>

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.

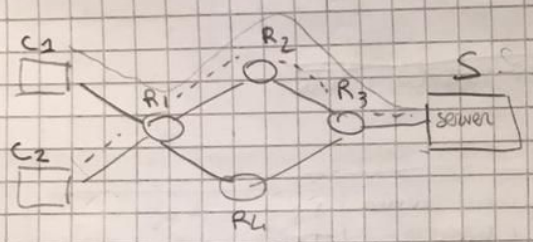
• **header format simplification**

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 encount a link which is smaller than the packet length. So most of the time 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

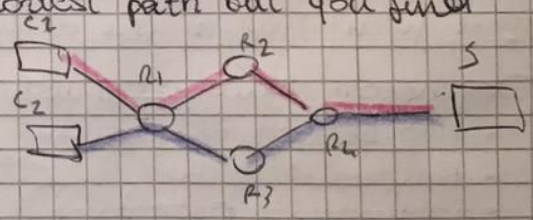
ex consider a network infrastructure



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 port in the net that is overloaded and the other not, so there is a possible congestion in one port 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 send's it one up and one down)
Not a good way because at layer 4 there is TCP protocol which is sensebe 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 send it on the right flow.

• authentication and privacy capability

BASIC HEADER IPV6

Version	traffic class	Flow label
pay load length	Netx header	Hop limit
Source Address (more bits		
Destination Address		

} more bits than the other fields

Optional internet-layer information is encoded in separate headers

basic header	Extensions		
IPV6 header Next header = TCP	TCP header + date		
IPV6 header Next header = routing	Routing header Next header = TCP	TCP header + date	
IPV6 header Next header = routing	routing header Next header = fragment	fragment header Next header = TCP	fragment of TCP header + date

PROCESSING AN IPV6 PACKET

Extension header 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 in a specific order~~ be of different types:

- Hop-by-hop options → it is allowed to be processed by intermediate node. (it uses pooling)
- Fragment
- Destination options
- Routing
- Authentication
- Encapsulating Security Pay load

The order is fundamental for headers:

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

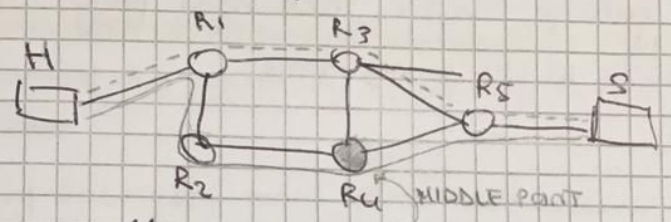
ROUTING HEADER

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

Next Header	Header Ext Len	Routing Type (8 bits)	Segment left (8 bit)
type-specific data → list of middle points			

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

ex



If I doesn't specify nothing the packet will take this path

for example it could choose one router to be the middle point (ex: router R4) this means that the packet must go through it

TYPE 0 ROUTING HEADER

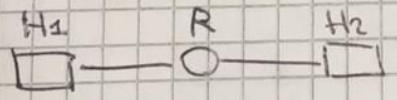
it has been deprecated because it creates problems about network security. It was used to create the DoS service attack in the network. It tried to create a congestion such that you have a lot of ~~packet~~ lost packets.

The vulnerability is that in type 0 routing header 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 AB AB AB). This makes the ~~pac~~ 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 largest packet allowed to be transmitted over that link.

If the packet is larger 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: (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 PLAT under discover 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 wait 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:

$$PL_{orig} = \underbrace{PL.first}_{\text{payload length of 1° fragment}} - \underbrace{FL.first}_{\text{fragment length of 1° fragment}} - \underbrace{8}_{\text{length of fragment header (8 byte = 64 bits)}} + (8 * \underbrace{FO.last}_{\text{fragment offset of last fragment}}) + \underbrace{FL.last}_{\text{fragment length of the last fragment}}$$

(8 byte)

30/10/2020

ERRORS IN REASSEMBLY

- Insufficient fragments are received
  (reassembly must be abandoned and al received fragments are discarded)
- the length of a fragment is not a multiple of 8 octets and the M flag is 1 (pacchetto solo l'ultimo pacchetto può avere non 8 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 ~~pkt~~ 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

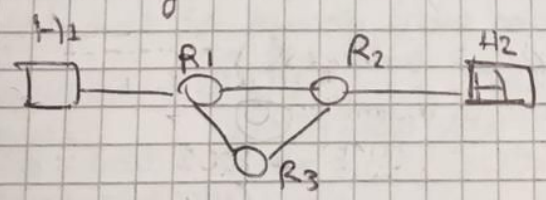
while in IPV4, every single node is allowed to do fragmentation. In IPV6 only the source node can. (it reduce the overhead)

The problem is that the source node is asked to create fragments that are ~~[illegible]~~ 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 amongst 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 source node that update the new value of MTU. In the end the source node fragments the packets at the minimum MTU found.

PMTDU and Black Holes

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



H1 -> R1 -> R2 -> R3 -> R1
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.

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 2001:0DB8:0000:CD30:0000:0000:0000:0000 / 60
(2001: exadecimal; 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 60 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 => 2001:0DB8:0000:0000:0000:0000:0000:0CD30
(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 ~~two~~ public addresses are assigned only at servers, global unic. addr. are assigned also to hosts.

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 subnetworks 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 is considered for multicast addr., exept those starting with 000

GLOBAL UNICAST ADDRESSES

general format is

n bits	m bits	128-n-m bits
global routing prefix	subnet ID	interface ID

value assigned to a site (I assigned it to a subnet)

identifier of a link within the site

determined starting from link-layer address

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

10 bits	54 bits	64 bits
1111111010	0	interface ID

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

8	4	4	112 bits
11111111	flags	scop	group ID

- 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 in 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

nodes 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 node 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 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

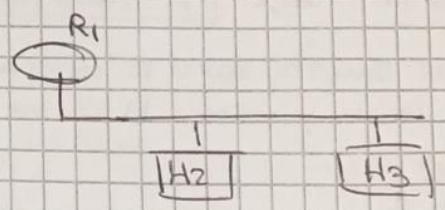
There are three ways a host can get an IPV6 address :

- manual configuration
- stateless configuration (created automatically) (SLAAC)
- stateful conf g. (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 him self 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 & B share same (symmetric) key: K_S
PUBLIC KEY CRYPTOGRAPHY: B has 2 keys (private K^- and public K^+)
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 specified 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 containing E's public key digitally signed by CA. CA says: "this is E's public key".

→ IPSECURITY sono servizi applicati al livello alto

12/11/2020

IP SECURITY SCENARIOS

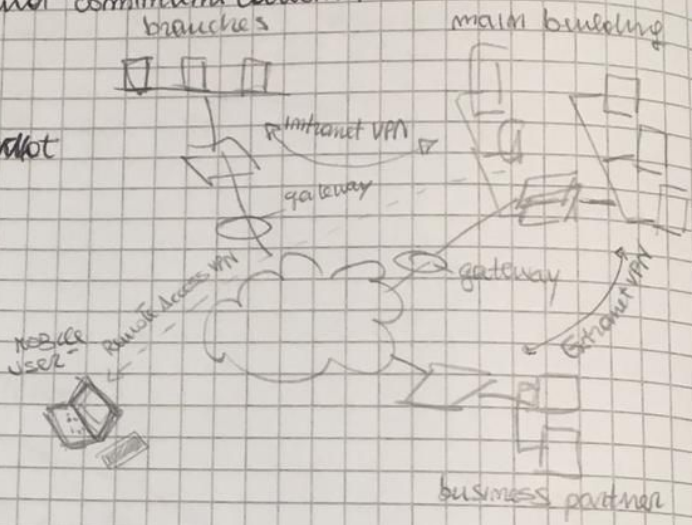
IPsec provides the capability to secure communications across LAN, private and public WANs, internet

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 ~~[illegible]~~ 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)

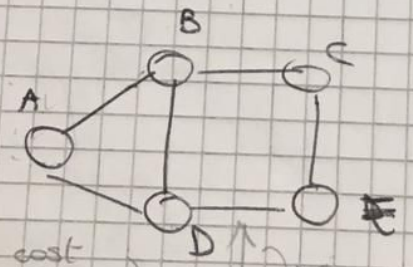
The third case is when we want to communicate securely through mobile users
(REMOTE ACCESS VPN)



ROUTING APPLICATIONS

GLOBAL ROUTING PROTOCOL: In order to ~~[illegible]~~ 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



$$LSA_A \begin{cases} \langle \overset{link}{(A,B)}, \overset{cost}{C_{AB}} \rangle \\ \langle (A,D), C_{AD} \rangle \\ \vdots \end{cases}$$

F 0.0.0.0/0
cost 0
attached

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

FLOODING: the router B receives the LSA from A and it finds out the link between A and B and its cost.
~~Also~~ 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 ~~then~~ trust 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 ~~also~~ in the network trust 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~~

IP SEC 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 replayed 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 connectionless 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 association.
    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)

~~to~~ it has a local meaning (this means that could exists 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 increases in every single 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 ~~when~~ 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.

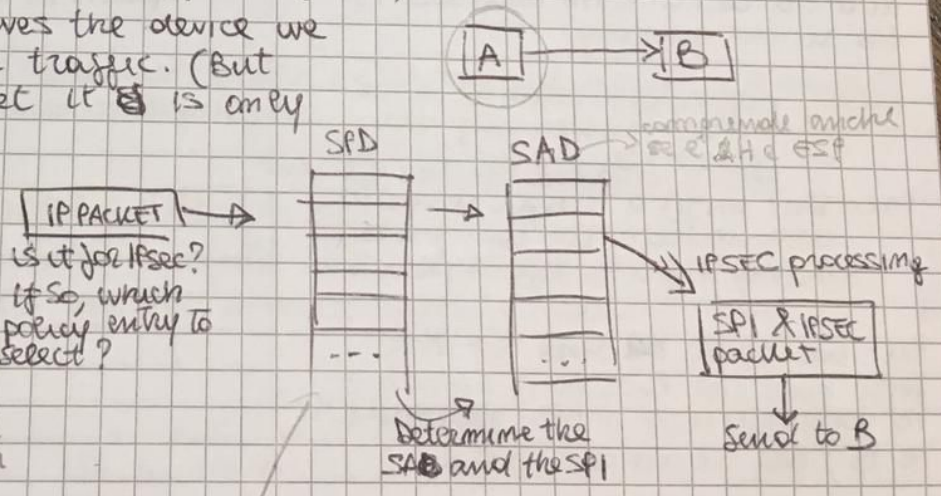
We use SECURITY POLICY DATABASE (SPD) ~~as~~ that sets traffic filters for SA. (We can consider a traffic filter like a routing rule where we ~~spec~~ also specify the source and destination address, the port number of source and destination, the type of protocol and so on.

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

→ dietro il traffico

SPD + SAD : Outbound traffic (on A)

when the traffic leaves the device we referred to as IPSec traffic. (But befor ~~B~~ becoming IPSet it ~~B~~ is only IP packet)

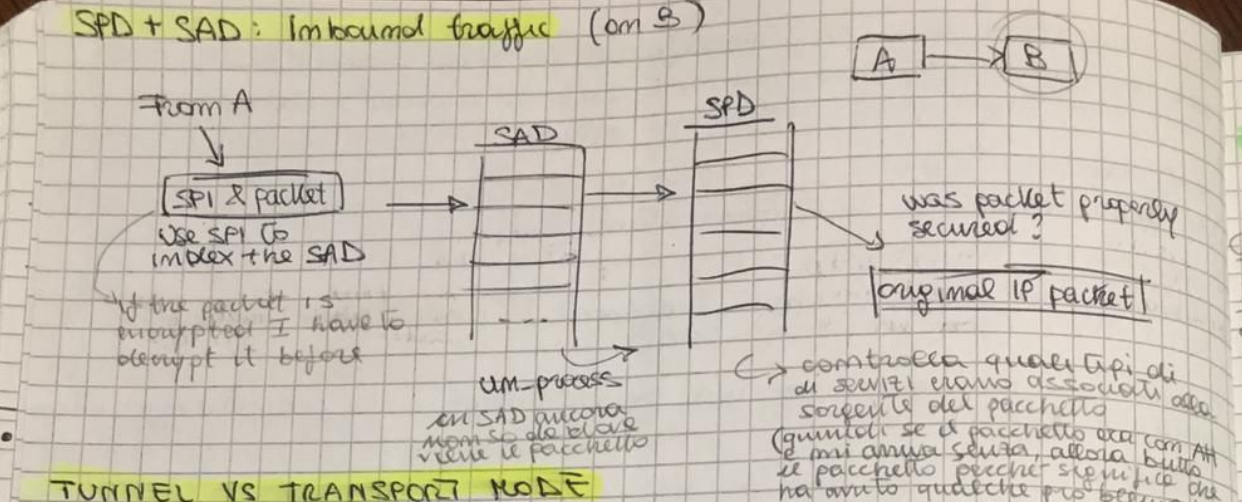


SPD contains entries which define a subnet of IP traffic and point to an SA for that traffic.

a/a SPD viene preso il indirizzo di destinazione

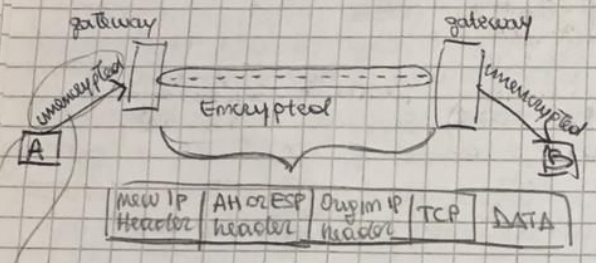
(Dentro SPD si decide se il pacchetto è IP normale o se è IPSEC a seconda dell'indirizzo di destinazione)

SPD + SAD: Inbound traffic (on B)



TUNNEL VS TRANSPORT MODE

TUNNEL MODE



here msgs are sent like plain text

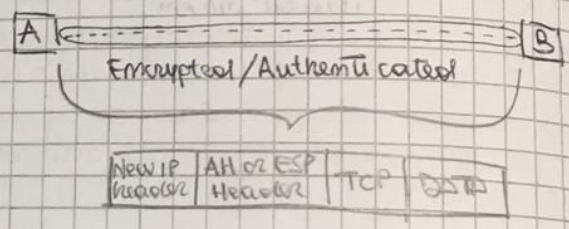
In the Tunnel mode the packet is encapsulated into another IP packet
In this IP packet the source address is that of the first gateway and the destination address is the second gateway.

CONS: bigger overhead because we are increasing the packet length because we put the origin ~~IP Hea~~ 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

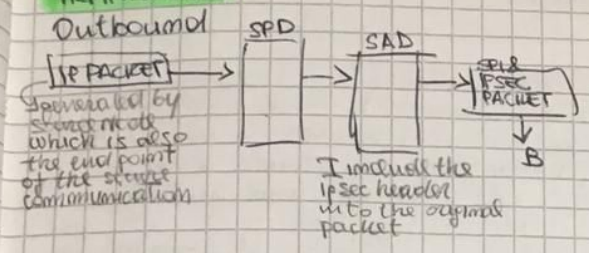
N.B. While for host-host communication we can decide to use either transport or tunnel mode, in case of gateway to gateway communication we must use tunnel mode

Si usa la tunnel per sfruttare le strutture IPV4 per IPV6 senza rifare tutto

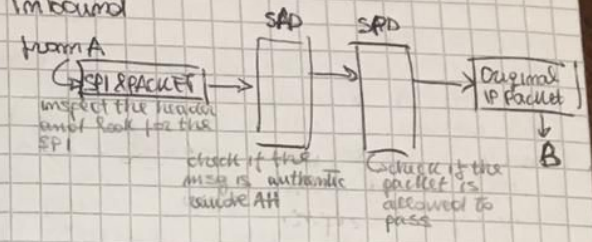
Apply transport or tunnel mode to Outbound traffic.

TRANSPORT

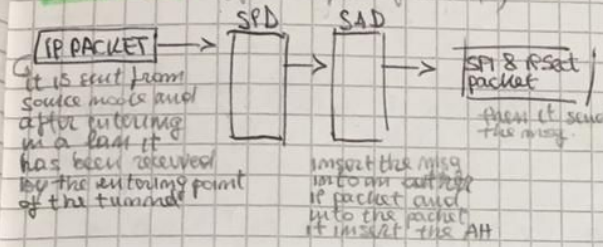
Outbound

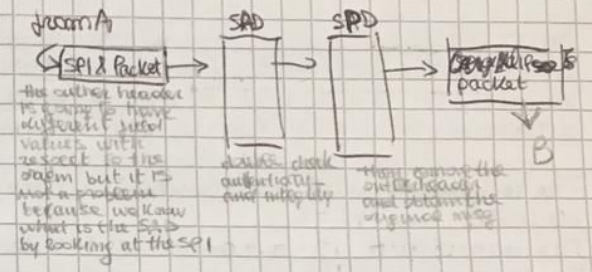


Inbound



TUNNEL (gateway to gateway)





In transport c'è bisogno di meno sicurezza che nel 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 criptato)

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

(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

0	15	31
Next header	Payload Len	Reserved
Security parameters Index (SPI)		
Sequence number Field → used to prevent replay attacks		
Authentication Data (variable)		

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 Ø. 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 Ø, so it terminates the SA and negotiates a new SA with a new key.

per mantenere elevato livello di sicurezza

RECEIVER SIDE

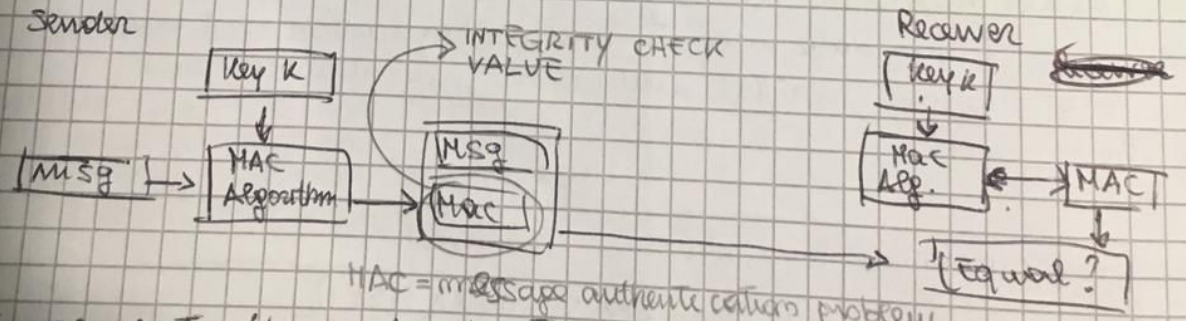
it is connectionless, (main difference with respect to TCP), unreliable service, so there will be no guarantee that packets will be delivered in order (or simply delivered)

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 ~~[illegible]~~ 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 che sono più vecchi di un tot tempo)

INTEGRITY CHECK VALUE

(it is authentication only)
(the msg non è stato cambiato)

~~integrity~~ 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 ~~funct~~ way function, nobody else apart from the source can generate a ~~MAC~~ MAC (which is the integrity check value) is inserted in the authentication date 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 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 il MAC (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)

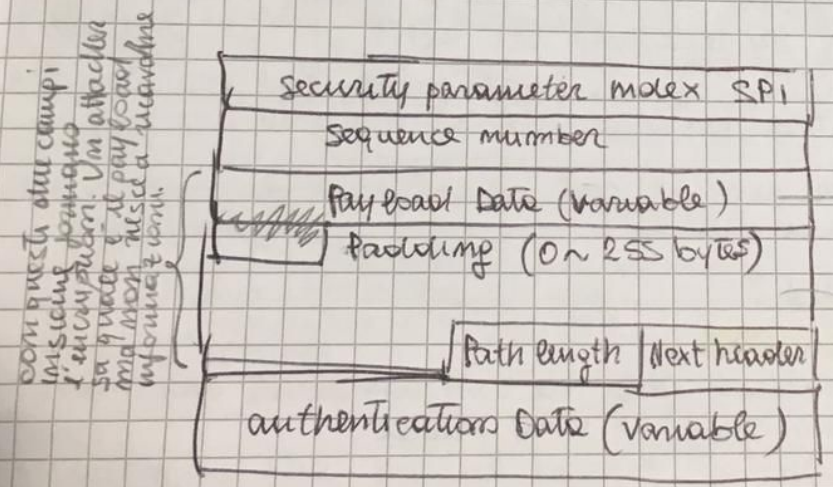
Not all IP-header fields are going to be authenticated because some of the header fields change value while transiting from the source to the destination

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)



encryption part is inserted here and we use padding if it is not of the right length

l'attacker non può distinguere quale è la parte del payload e quale è la parte vuota del padding
(prima fase padding e poi cryptoing il pacchetto)

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 ~~s~~ 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 characteristis:

- When we talk about fiber we talk about trasmission at some specific ~~wave~~ length (nm).

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

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 utilizzare 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 performances 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 end and)
This reflection can cause some dispersion 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 transmitted?

It is transmitted by using LASERS. → sono dei rigeneratori, quindi ripropagano 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 when~~ that ~~it~~ 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)

How do we provide those fibers?
The idea is: starting from the original structure based on copper, we replace part of it with the fiber.
(FTTC cabinet or FTTC curb)
(FTTBuilding)
(FTTHome)

How do we implement the path between the switch/router to the home? 3 possible solutions:

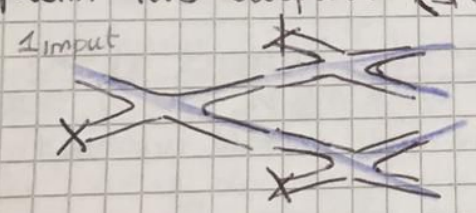
1) put the fiber replacing completely the copper cable so we have one fiber for every user.
(REPLACE FIBER TO THE WHOLE PATH and this is done by performing digging. Micro digging cost 30/40 K €/km)

2) put only one fiber till a network element (for example the curb/cabinet) and then have other media like copper from the cabinet. (Ho una sola linea di fibra fino alla cabinet)
The curb/cabinet is called ACTIVE ELEMENT because it is the element where the optical signal is received, is converted to a electromagnetic signal, is processed and then in case it is retrasmitted.

3) there is simplest solution that is named PASSIVE SPLITTER (and this is where derives the name passive optical network) PON. It is named PASSIVE because this element is very simple:
The splitter is fusion between two fibers together and it has the possibility to split the light because it enters from one input and exits from two outputs (SPLITTING OF THE LIGHT)
(soluzione poco economica)

this is costosa

1x2 splitter
1 input 2 outputs



1xm splitter
1 input m outputs

1x4 splitter
1 input 4 outputs

cons:
- Every time the signal is split in two ways, the signal is reduced by $10 \log(0,5) = 3dB$
  LOSS is circa $3dB \times \log_2(\#\text{ONUs})$
- it is similar to a hub in the way of working, so it could be some collisions if some users use the same light frequences
- We have a single point of failure at the splitter (as for FTTC)
- You have to keep in mind the number of users you have because every time you split the signal.

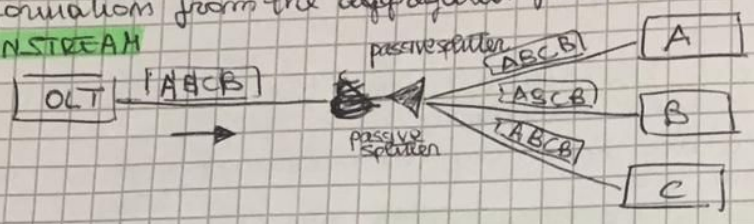
How to recognise the information of the users ?

The idea is to build up an approach where the information that is sent to this media is separated (for instance in time) and in each piece of information you put (an aim, an address, but this address is needed to pick up only my information from the aggregated flow

Upstream e Downstream hanno colori di frequenze diversa, quindi passo fare contemp. Downe Up.

N.B

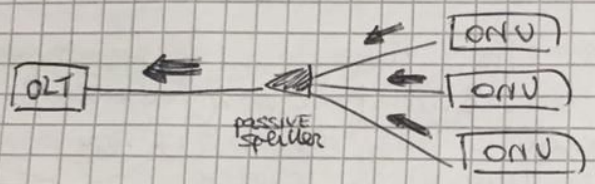
DOWNSTREAM



(In case of ACTIVE ELEMENT the separation is made by the active element
In case of FIBER to the whole path the selection is made directly by the user).

UPSTREAM

All ONUs share the same upstream channel

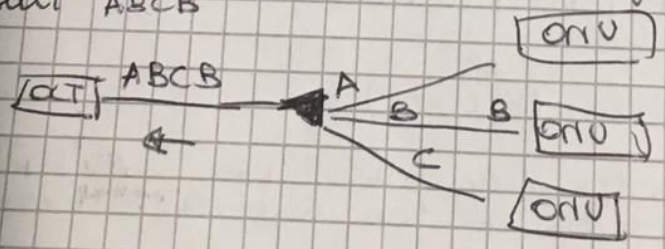


So we have signals that may overlap.
(at the splitter some collision may happen).

To solve the problem of collision:

- in the collision based a terminal is able to understand and recognize when the collision happens.
- On the contrary in this case the collision happens at the splitter (in the upstream). So the ONU will never know the fact that there is a collision and so we can't work with the classical collision based approach.

The only way it can work is:
The optical line terminal schedules the time period when the difference of optical network unit have to transmit.
And these time periods are designed in order to have the result ABCB



(we need SINCRONIZATION and SCHEDULING, both performed by OLT)
The OLT does also another thing:
Since ONUs can have different distances from the splitter, it can be that the power of same msg changes. But we don't want a signal that changes during the burst, so the →

Optical line Terminal (OLT) provides a mechanism to tune the level of the signal ~~on the~~ based on the distance.
So it sends a ~~an~~ pilot signal to measure the attenuation and once this attenuation is measured, says to the different users at what level the users has to "speak" in order to have all signals arriving at the same level. (OLT dice agli utenti a quale potenza deve essere inviato il segnale)
(This is done burst by burst)
→ invio in burst di messaggi a tutti gli utenti

PON is very used and the solutions that current operators offer for FTTH are GPON or EPON

EPON: Ethernet PON
the structure of the time slot where the information is took(?) is a time slot accomodating a 802.3 frame
It uses symmetric bitrate for the two directions

GPON: Gigabit PON
We use asymmetric bitRate for the two directions

anche assegno a ogni utente un determinato colore e poi gli mando le frequenze di quel colore

N.B. Alcuni colori nella fibra soffrono un'attenuazione maggiore e quindi non vengono usati

NB when we use classical PON we have a color (wavelength) used in the downstream and a different color (wavelength) used in the upstream, on the same fiber.
It means that up and downstream are separated.

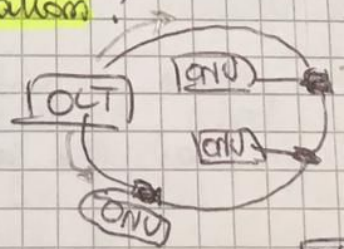
The evolution of PON is achieved by the evolution of the technology that gives the possibility to run multiple colors on the same fiber: WAVE DIVISION MULTIPLEXING WDM-PON

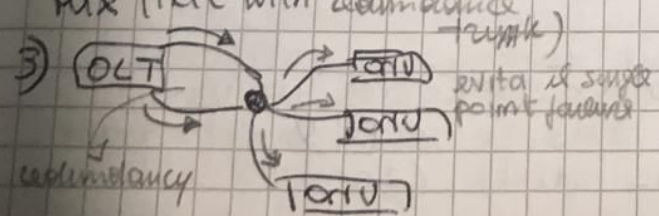
In the same fiber I have different wavelength and ~~in this way~~ I put splitters (optical routers) that take in input ~~the~~ all the colors and then they split them (so the output are different colors)
So in the downstream we have different users on different wavelength. ~~and~~ In the upstream the different wavelengths are transmitted and are combined in the same fiber.

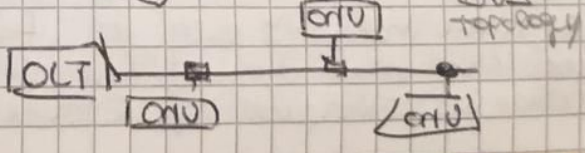
ADVANTAGE: you have a kind of physical separation of the user.
DISADVANTAGE: it depends on the number of wavelength that can be supported in the same fiber (in order of 10s)

How to implement EPON configuration?

1)

2) 

3) 

4) 

19/11/2025

LTE / LTA-A CELLULAR SYSTEM

WIRELESS ACCESS

2 kinds of wireless systems:

- **BROADCASTING SYSTEM** (oldest) (TV SYSTEM)
  we have a main transmitter (ground antenna or satellite) with a very large coverage area. The transmitter is the one dedicated to broadcast digital services.
  It was mostly designed for television or radio broadcasting

- **CELLULAR SYSTEM**
  The architecture is composed by having some network elements called base stations (BS or BTS) which cover by a specific range a set of users/customers.
  There are different areas (CELLS) and each different area is covered by a BS. Those areas may change because it depends of the physical area where the BS is. (So for instance if a BS is on top of a building the radio propagation is better than having a BS on the ground)
  The BSs are interconnected by wires (in general fiber optics) to other entities that interconnect the cellular network to the backbone. (This interconnection is called BACKHALL)
  ↳ le interconessioni tra BS sono backhall

What is the difference between control and user information?
(Da ripassare) → control information is the header of the packet like (flow label, traffic burst).
User information is the pay load of the packet

In the field of the wireless access we have several standards and there are two main important factors to describe these standards:

3GPP (third generation project)
was born when GSM was designed and then evolved for several other technologies including 5G. They provide all the specifications.
GSM → EDGE → UMTS → LTE → LTE-A

These standards are provided mostly in the east part of the world (Europe and Asia)

CDMA 2000
This standard is provided mostly in the west part of the world such as in the USA

Even if they were used for different things, now the path is the same, so both 3GPP and CDMA 2000 are used in LTE (so now we have the same standards)

IEEE
These standards are used for many technologies networking and one of the most famouse is Ethernet. We use in the wireless version of Eternet is Wi-Fi (802.11)

Now we have other standards such as IEEE 802.11m
What is change is: the kind of technology try to improve the performance. On the other side the goal in this framework is ~~to~~ the possibility to support mobile users.

(Because while in 3GPP ~~and~~ from the very beginning ~~opt~~ ~~from~~ the support of digital information, another fundamental novelty ~~from~~ of the standard was to support digital information in a mobile environment

On the contrary, in IEEE, the idea was to provide a wireless access at the very beginning at local area and then extend more but in general without having the mobility as a key requirement.

Some standards in the IEEE framework (like 802.16) where designed in order to support high data rates and mobility but ~~the~~ 802.16 is not so used as LTE, 5G and HSPA

We can figure out how in terms of mobility this standards are valid:

- first distinction is if we move in an indoor environment or in an outdoor environment
- second important aspect is data rate

INDOOR

- first kind of mobility is no mobility (we have fixed access, so we are in a stable position for example with my laptop in my room)
  There is a form of mobility: for example I am connect to the same network but I move from a place to another, like different rooms or floor of a building)

- Walk (keeping our connective active)
  ~~that~~ that means that you walk and change room but you don't change the IP address.
  The advantage is that you can always keep your internet connection fluent. So if you are exchanging datas you don't see an interruption or some packet loss as if you are in the fixed

OUTDOOR

- I can have the fixed
- I can have walk
- I can have vehicle version that it is at high speed (the speed changes) and the higher is the speed, the complex is to maintain the connection active.

The original cellular network 2G and 3G was intrinsecally designed to support mobility (keep IP-address, keep the data flowing without interruptions ----)

The challenge becames harder and harder as the mobility increases. This is why in the very preliminar version of the solutions like WI-FI, they were not designed to support these kind of requirements.

On the contrary, looking at the bitrate, there are differences:
There are technologies that originally where designed to support some bitrates (2G and 3G 1mbps)
Then technologies evolved toward other solutions and the most compex and performing technologies are LTE/LTEA (4G) because they combine high bitrate with very high mobility

There are some techn. that by designs have high bit rates but low capability on supporting mobility like ~~W-LAN~~ W-LAN IEEE 802.11a

Where should we put the 5G?
The 5G will have the highest bit rate and the highest mobility

We have to consider also another dimension of metrics with respect to bitrate and mobility tha is latency.
Latency is the time that passes from the moment I send data and the instance I receive response. and it is important for fast communication that needs real time for example autonomous dri ~~ving need low~~ needs low latency connection.
(Low latency means more real time simulation)

$\boxed{\text{LATENCY}}$ is the response time that we have in our interaction with the network.

So 5G is not evolving only in mobility and bitrate but also in latency.

WIRELESS AND MOBILE NETWORKS

Background:

Wireless access is the combination of wireless access and mobility and there are different forms of accessing the media and different forms of managing mobility.
in mobility is important to keep the address and to have an address but ~~to~~ it is important the ~~[illegible]~~ handling of mobility in cellular network and the management of mobility and higher-layer protocols (for instance when you have mobility it is not only something related to the third voice ~~#~~ level ~~[illegible]~~ but it is also related to authentication.

The infrastructure is based on sections:
The peripheral parts of the networks called CELLS, each cell has a BS to which wireless hosts are connected (such as pc and ~~[illegible]~~ smartphones)
These end terminal could be mobile or stationary (so they can move or be static).

The first fundamental network element in the CELL is the Base station BS. The BS has to provide coverage, connectivity to the users in the coverage area (the area where the radio signal transmitted by the BS arrives).

The radio range depends on the power of the signal, the environment where the signal is transmitted. The goal of the BS is to set up the coverage in a specific area and to provide the wireless access to the different end users that are connected.

MULTIPLE ACCESS is when we have users accessing a wireless media that is shared. (Users share the spectrum band)
The multiple access is managed in part or fully by the BS.
The BS has to manage also the mobility of users that move from different cells. This operation is called HANDOFF or HANDOVER.

HANDOFF: is the passage of the communication from a BS to another. This management is done by different methodologies depending on the speed, how frequently it happens, how fast we need to keep the connection active, and so on. It depends also on the area covered by the BS and on how is is possible to manage this in terms of signal.
(We have two levels: HARD HANDOVER when I pass to another BS, I disconnect from the previous one and connect to the new one.
SOFT HANDOVER is the methodology where I start one or multiple connections toward the area where I'm moving. And I mantain both connections active during my movement in order to sure that my connection doesn't interrupt.
Through handover we can also predict if a user will use a certain BS in order to prepare datas and IP addresses and so on.
→ soft and hard

in the access wireless world there is also the possibility to don't have any infrastructure (INFRASTRUCTURELESS NETWORK) it is the networking made only by the end devices.
It is also called AD-HOC network
The interconnection of devices is made through wireless interconnections.
The AD HOC mode was designed more than 20 years ago. Real technologies that are using this mode have less potentiality with respect to the real potentiality. So there are applications that use this ad-hoc mode, the simplest one is the one that we use for instance when we set up our hotspot (the computer is connected to our smartphone which is connected to the BS)
We can use the multi hop solution that offers the possibility to extend the coverage of this ad-hoc network. A typical application of this multihop communication is the framework of the vehicular networks. (They are ad-hoc networks that are implemented in a vehicular environment. So we have vehicles that are the mobile nodes and they exchange data in an ad hoc mode, so they set up their network in an ad-hoc mode. The channel should be secure & there are standards like 802.11p).
Other frameworks are those of the wireless sensor networks (internet of things IOT) so there are devices and sensors in a given area and they are wirelessly interconnected in an ad hoc mode →

~~Which are the advantages of INFRASTRUCTURELESS NETWORKS~~

Which are the advantages of INFRASTRUCTURELESS NETWORKS?

- Latency is extremely reduced (because I don't pass through another element like BS)
- Direct communication → la latenza nulla deriva dalla diretta comunicazione
- Every device is a device but also a router. A router should have different functions, for example should know a way to route information. (there is no way to know a priori the how to route information because it doesn't have knowledge of the network infrastructure, to know this I can broadcast everything, but it is not efficient in term of performance. So I have to discover the routs first and then apply the routing.
- Another advantage is the cost
- Flexibility, because this network is a dynamic one. It adapts to the environment. (this is the main advantage)

disadvantages:

- the management of the network and of the protocols is a disadvantage and related to for instance the routing or other aspects you have
  - security issues (where in a fixed network you can control who is accessing, who performs the routing, you can't control devices connected wirelessly)
  - energy loss (because we are giving more functions to a device, so it will use more energy).

WIRELESS LINK CHARACTERISTICS

there are important differences from wired links:

- in a wireless transmission the signal power decreases (so the radio signal attenuates as it propagates through the media (path loss) it is more significant with respect to a wired network.

There are two important models: one related to the so called Line of sight condition LOS (I am on the same line as a receiver and a transmitter)

The second one is Non Line of sight condition (NLOS) where we do not have the direct electromagnetic link toward the radio frequency.

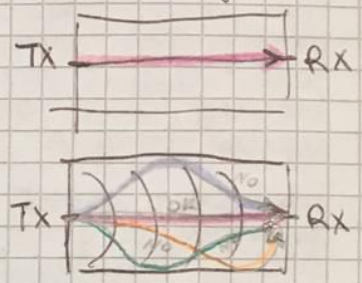
Interference: We have different sources of interference. There are two important components:

In the spectrum depends on which is the spectrum we can have the interference of internal sources (devices that by the spectrum are authorized to transmit in the same spectrum) and devices that are external that are not authorized to transmit in that spectrum but generate some interference.

The spectrum could be licensed or unlicensed, it means I can allow users to use a spectrum without license (industrial scientific medical bands, that is the band used by Wi-Fi

So in this band can transmit Wi-Fi and other devices, for example bluetooth. So the interference is present here because of the transmission of multiple technologies.
In the licensed case (where only users that have a license can use that frequence to transmit) I have to know how to manage the transmission of different users.

- **multipath propagation**: multipath is a path in the radio frequency signal that are used when you transmit a signal.
In a wired connection the signal is linear, it goes from sender to receiver



But in case of wireless, the signal goes by waves, in several directions, so in this framework different other paths may generate.
The result of this multiple paths in this environment is that the receiver receives more times the same information.
- If these more signals are not managed in the right way, they can cause interference.

So multiple signal interference is bad unless it is the same information so we manage it as the same information, so it may become an advantage, because if I'm able to combine different signals, I can make my signal stronger.
The important fact is that I need to have a full synchronization of these signals to combine them in the right way.

The multiple propagation depends on the carrier frequency of the signal.
The reflection (passing from a surface or an object depends on the frequency. So there are some surfaces that reflect a signal at the given frequency and do not reflect the signals at other frequences. The higer is the frequency, the lower is the kind of surface that can reflect my signal. So if I use very high frequences also a drop of water in the rain or a leaf from a tree may reflect the signal.
The reflection depends on the environment and on the frequency.
So this is why is complicated to model this system

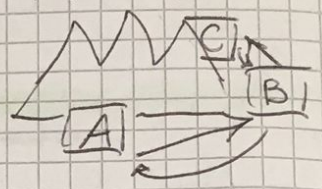
(*) se più è alto SNR più posso avere BitRate alto (QUAM 256 (8 bps))

Another important aspect of wireless link is that giving at the end a measure of the quality of the signal (in general expressed with SNR (signal to noise ratio))

- **SNR** it is the ratio of the power of the signal to the power of the noise when I receive a signal.
Depending on SNR I can provide more sophisticated and powerful modulation schemes and that implies that I can (*) achieve higher bitrate on my link.
larger is SNR, easier is to extract signal to noise (because it means that the noise is very small with respect to the signal). Higher is SNR lower is BER (bit error rate)
SNR depends on the environment and I can't choose it → BER ↑ in target

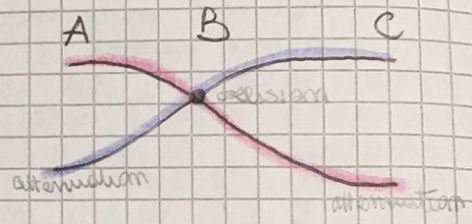
- Another phenomenon which is only present in the wireless is the **hidden terminal problem**.
The devices composing my channel are not known by all the users because of no radio propagation condition

So in this example A can hear B and viceversa C can hear B and viceversa but A can't hear C and C can't hear A



The signal transmitted by A by propagation attenuates or in the worst case, when it arrives to C is almost blocked, so C does not receive any signal from A. Same thing from C to A.

The other aspect is that in B signals from A and C arrive with good quality. This means that if A an C would like to transmit, in B we have a collision, an interference of these two signals, and this is a problem because A ~~and~~ doesn't know the presence of C and transmit to B and C doesn't know the existence of A and transmit to B. So there are protocols in the wireless access that must solve this kind of problem.



One protocol is on the framework of 802.11 (CSMA)
The protocol is the **COLLISION AVOIDANCE**
it is a way of exchanging information in order to avoid this kind of collision.

<u>On the sender side:</u>
I measure for a while the channel (CHANNEL SENSING) and the time dedicated to this channel sensing is named DIFS (Destributed InterFrame Spacing).
I cannot be always sure that there are **no other communications**
Let's assume that it is free so I can transmit and I transmit my data and are recieved by the other side.

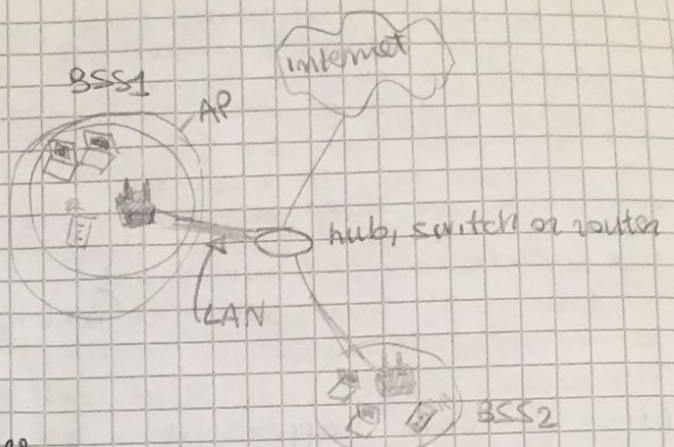
<u>On the receiver side:</u>
If they are recieved correctly, the receiver listens for a while to the channel and time is SIFS (short Interframe Spacing) and then the receiver sends an ACK to the sender so It can know that the data were recieved **correctly**

If the channel is busy, I postone my transmission and the postpose is done by this criteria: if the channel is busy or I haven't recieve an ACK, I use a BACKOFF MECHANISM that is designed to randomize my next attempt.
So my next attempt is performed in a time window that ~~changes. So I do~~ increases at every attempt.
In this way I try to avoid next collision.

25/11/2020

WIRELESS ACCESS pt 2

LAN ARCHITECTURE

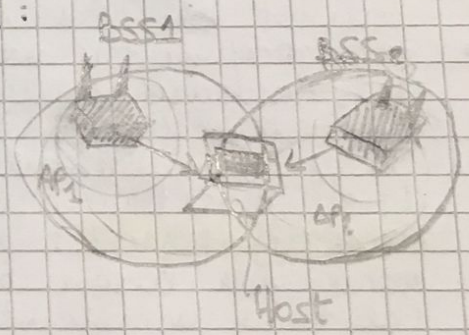


there is an area covered by an access point (AP) that contains several mobile hosts that are interconnected wirelessly to the AP.
In the WI-FI terminology this area is called Basic Service set (BSS) (it is the correspondent of a cell).
The BSS is interconnected with a very simple infrastructure which is local area network (LAN) to a switch or a router that allows the interaction with different access points and on the other side toward the Internet.
Different BSS are interconnected because it could be of some interest to provide mobility. (so you can move to one place to another without disconnect)

The access points manage the access to the wireless interface and in case of WI-FI there is an association with a specific access point. This association is performed by scanning the channels searching for some specific control msgs sent by the Ac. Point. named beacons(?) So beacon frames are short msgs sent out continuously by the APs and include the MAC address of the AP and its name (SSID)(Service set ID).
The association selects an AP and performes an authentication.
In general these AP run the DHCP in order to have assigned to the mobile host an IP address (which is typically an intranet one) private

For association there are two methodologies:

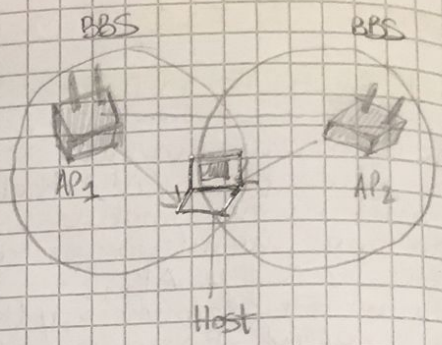
- **PASSIVE SCANNING**



everything starts by having two different access points sending out beacons.
So beacon frames are captured by a mobile host, and the mobile host, once he receives multiple beacon frames from diff. access points, selects the acc. p. to who he wants to interconnect.
(So the host can choose manually the access point or it could be automatically chosen the one with higher signal)

- **ACTIVE SCANNING**

- **ACTIVE SCANNING**



this procedure is started by the mobile host that sends out some probe requests which are intended as requests toward possible access points (SSID) that the terminal knows. (So when we interconnect to a WI-FI network, we keep in memory the list of WI-FI networks that are interconnected with us).
So the host sends out the list of WI-FI networks that it knows. (SSID table)
The access points then send back a response. ~~and thanks to this~~
(this is what happens when we select "connect automatically" ~~on the~~ to internet networks on my ~~pc~~ devices)
This method is more automatic than the other.
A thing to note is that there is a sort of privacy violation, because when I send back my probe request, I'm sending out my list of known WI-FI networks.

During assocuation response we do authentication.

ACCESS for MOBILE SYSTEM

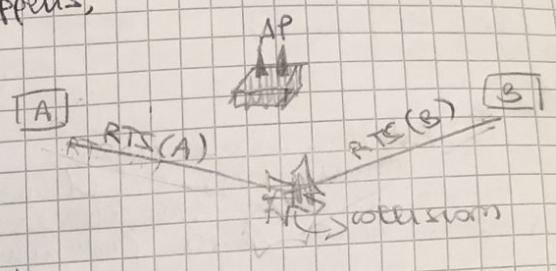
- there are two ways that have been implemented in WI-FI:
  - performe the channel sensing in time using DIFS. If the channel is free I send my data. DIFS doesn't assure that datas arrive correctly to the receiver because there is the hidden terminal problem: (there could be collisions at the destination)
    This problem doesn't ocurr in wired connection because in terms of signal in a wired conn. there is no way that I cannot see other terminals in my wire. On the contrary in the wireless it could happen. For this reason the standard includes that the receiver after another time period (SIFS) sends back an acknoledgment.
    So if the acknoledgment doesn't come back, the sender tries to retransmit but the new attempt is done in a **back off period**: at every new attempt the transmission is done in a longer period.
    The time windows increase in an exponential number 2^n where n is the number of attempts.
    The reason for increasing the time window ~~is to delay~~ is that you have the possibility to avoid next collisions. ~~The disadvantage is that~~ The enlargement of time window has as max $W = 2^{10}$ (We can reach this number when the channel is always busy)
    The disadvantage is that at every ~~time~~ attempt increases the delay.

every attempt is a different time

- **The other possibility is to use control msg.** This protocol is more complicated but has stronger multiple access.

~~Too~~ it is executed in a distributed manner but there are control msg named requests to send and clear to send (CTS viene mandato in broadcast)

Requests to send are short msgs sent by the devices who intends to transmit the data.
We are not sure if there are other devices transmitting at the same time. So it may happen that those short msgs collide. When this collision happens,
there isn't acks to A and B, so A and B are not aware, so I retray the msg.
So there is a waste of capacity in sending those msgs but msgs are short because they don't need to transport data.
So next attempt made by A may be succesful and then it could be succesful.



1) Does B know that RTS(A) was succesfully received by the AP?
No because it is hidden from A, so to let it know, the access point is requested to send a clear to sent (CTS) in the whole area where the AP can be heard. So the CTS arrives also to B. And the CTS(A) to B indicates to B that there was someone else in the network asking for accessing the network.
In the protocol it is included also the time duration of my intended transmission.
In the RTS there is a field where I can put the duration of my transmission. This period is repeated in the CTS because it indicates to B there is someone who is going to transmit and the transmission will last that period.
In this way you give to B two important informations:
1) do not attempt again to transmit the information in this period because there will be another transmission
2) ~~if you w~~ if B wants, it can go to sleep mode because the sleep mode in the Wi-Fi saves energy.

So in this case the protocol is much more ~~robust and~~ performing, but the price to be paid is the time spent to send control msgs.

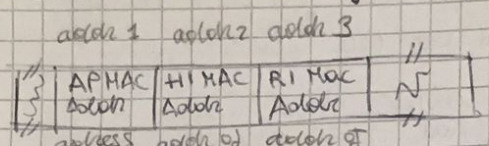
ADDRESSING

Like in the 802 family, the frame of Wi-Fi is formed in the classical manner, so there is control frame, duration, addresses, sequence control a variable size payload and CRC (correction code)

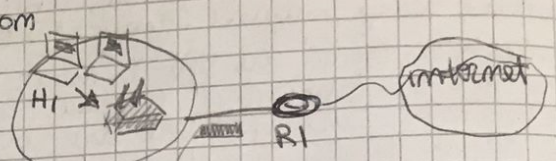
There are 4 spaces for the addresses.

Address 1: MAC address of ~~transmitting~~ receiving host,
Address 2: MAC address of transmitting host
Address 3: MAC address of the router of the access point which to it is interconnected
Address 4: Not used in general. (only in Ad-hoc mode)

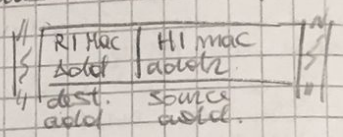
• I can have this kind of configuration



(802.11 frame)



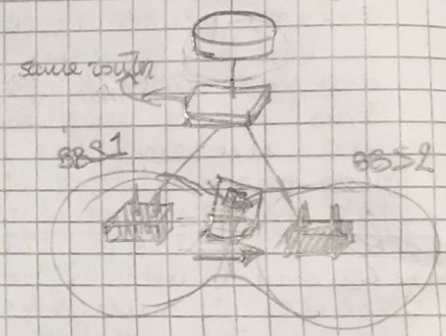
↳ the frame here becomes a classical internet frame (802.3 frame)



• in the Ad-hoc mode we can perform multi-hops on devices, so there is also the address of the next hop device (4th address)

Mobility within the same subnet

In the Wi-Fi there is also the possibility to have some form of mobility. In particular to move in the same service set from an access point to another by keeping the connection (on the authentication)
(if I change area or network, the auth. is not valid any more).



RATE ADAPTATION

In order to select the best access point the rule is to select the one with the higher signal to noise ratio SNR. (that is the one with higher signal)

In Wi-Fi there is also the possibility to adapt the rate. The data rate that I performe on my wireless channel, changes depending on the channel SNR, so ~~the~~ if the SNR is low, I will use a low modulation scheme BPSK (1 Mbps). If the SNR is high I can use a high modulation scheme (QAM256 (8 Mbps)) and then obtain a high data rate.

So the rate changes during my communication on the base of the received SNR.

ANALYSIS of CELLULAR NETWORK

~~Obs~~ Cellular network are different from classical Local Area because the first important aspect that has been designed in cellular network is support of mobility.
(It was already included in GSM).

There is the concept of cells: a cell is an area where different mobile stations (base stations) cover with their signal a given area.

Multiple BS are interconnected to →

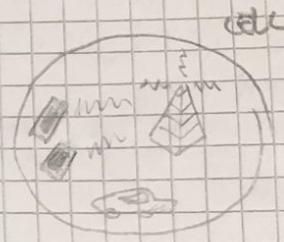
Multiple BSs are interconnected to a network element named Mobile Switching center ~~Back Hall~~ (Back Hall). It is typically wired (initially was wired by using copper cables coaxial and now fully fiber optic)

Mobile operators (like TIM) has this fiber optic infrastructure which is very capillar because it arrives to all the BSs. So even if this infrastructure was provided for other purposes (mobile network), it is use for other things.

The Mobile switching center provides the interconnection of different BSs and the management of the mobility
This is the reason why the back hall now is becoming fomodamental in terms of bit rate, because there is quite big exchange of information in this part of network for managing future mobile services.

We expect very low latency and latency depends also on this interaction of the network (devo avere massima mobilità, massima bit rate e minima latenza)

The very wireless access is only into the cell from the mobile terminals toward the BS.



in the cellular network the radio spectrum we use is Licensed, that means that it is used only for this kind of services and so you have to pay. So the operator pays to use that spectrum and the user pays the operator for using the spectrum.
(for example the price the operators have to spend to use 5G is 2,4 billions for TIM and by all operators 7 billions).
License
speb in Italia

The way to perform multiple access:
you can have a multiple access where you divide the spectrum portion in pieces (in order to give each piece to every user).
Today is requested to have a grate flexibility in managing these pieces.
How do we divide these pieces?
there are 3 methods

1) Frequency division multiple access (FDMA)
In frequency there are different channels, and in these channel I can put the transmission of one or multiple users (Multiple users may transmit on multiple channels).

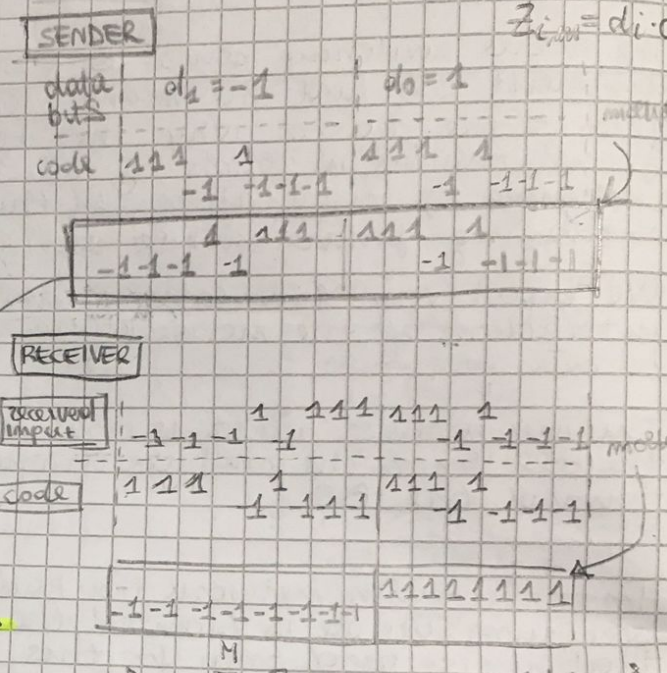
2) Time division multiple access (TDMA)
The division in time slots and you can assign to different multiple users different time slots

3) combined FDMA / TDMA Divide the spectrum into frequency channels and each channel into time slots

~~Flow~~ Who performs this assignment? the BS. So the BS manages these resources in order to allocate the bandwidth, ~~the~~ to its different users

3) Code division multiple access (CDMA)
that operates on the principle of allowing users to transmit data bits by multiplying them with a code.
The code is made by small bits name chips and the code is unique for a sender.

What is transmitted is the multiplication of the data bit d_i and the code C
$Z_{i,m} = d_i \cdot C_m$.
This information that it is sent in the channel once it is received, it is demultiplyed by code (same of the sender) and is normalized by the number of chips that are included in a code.
$M = 8$
Thanks to this operation I am able to derive back my bits.



$$D_i = \frac{\sum_{m=1}^{M} Z_{i,m} \cdot C_m}{M = 8 \text{ (bit)}} = \begin{cases} \text{slot } 1 = -\frac{8}{8} = -1 \\ \text{slot } 2 = \frac{8}{8} = 1 \end{cases}$$

TRANSMISSION OF MULTIPLE USERS

In this case each user has its ~~one~~ one code. So this transmission contemporary in frequency and in time, by two or multiple users having therefore codes allows at the receiver to recognize thanks to the code in these mixed signal the ~~req~~ information of a specific user and to cancel in ~~some way~~ the information of the other user.
So thanks to the code I am able to differentiate the flow of a user with respect to another.
And you can have contemporary transmission in time and in frequence.

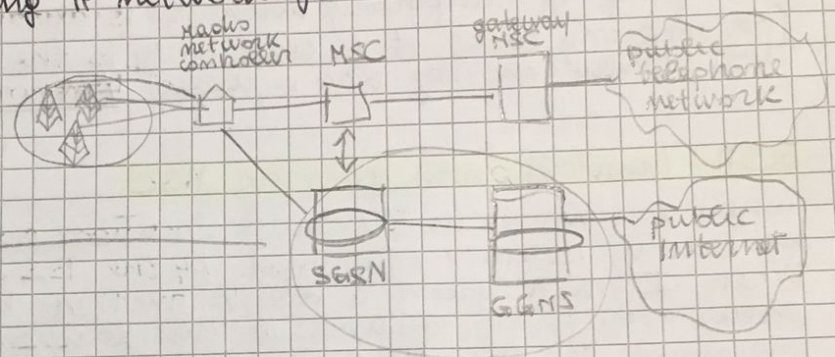
) the assignment of the code is performed by the BS

2G (VOICE) NETWORK ARCHITECTURE

The system from the GSM evolved:
The GSM was mostly designed for voice, only few information where included in the 2G by having the SMS (Short messages)
Short messages where sent in a field that originally was designed in the standard for other purposes -
(there was a field not used for any application). This is the reason why they initially assigned a price for SMS and the amount of characters that we were able to provide in SMS was constrained (because it was not designed for data)

3G (VOICE + DATA)

After 2G they passed to the real use of data part, and it was designed as the classical IP-network (so by providing the support of IP-packets and so on).
Now we are mostly using IP network for data transmission and to transmit the voice.



So network infrastructure is more complicated.
Because we have the first part, but the gateways have to perform the routing but they have also to perform IP-addresses, authentication,
So this part can transmit voice and also the potentiality to transport IP packets

COMPONENT OF CELLULAR NETWORK ARCHITECTURE

As said in the cellular network there is the support for the mobility (in MSC).
How is managed the mobility? There are different aspects

- When we use our mobile terminal, we have an area called location area. So our system is recognized as belonging to a given location area. This tracking of location area is designed into the standard in order to know that I am moving from a place to another. This area continuously updates itself by control msgs

- There is also this aspect: as for the network I have an element whose identity is stored in a database called Home Location Register (HLR). It is the home db of my router where my identity is officially registered.
This happens in this way: suppose that you have a contract with a mobile operator. the mob op provides you a SIM. So you give to the mob op your identity. The number related to the SIM (not the telephone number) is provided in this db. This number is used also to provide mobility in this way: when you move in another area, you are recognized in a Visitor Location Register (VLR)
What does VLR? 2 things:

GSM - Indirect routing to mobile.

What does VLR? It does 2 things:

1) It assigns to the mobile user a **temporary ID** and this new ID is put near the basic ID of the SIM.
So when I receive a call or a msg, the call is initially sent to my HLR. The HLR checks where I am by the IDs and then the call is sent to the VLR.

2) You have always the passage through the home, where all the information of the locations where I move are stored.
You can provide the list of the networks accessed by the user

GSM: handoff between MSCs

When you change from a MSC to another, (change location area) During this change, you chang the temporary ID, and this changing of temporary address is always sent back to the HLR. (Or in some cases it is send only to the first MSC from where you started moving who is called <u>Anchor MSC</u>)

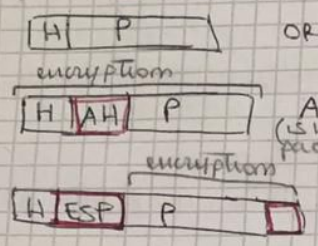
GSM: handoff with common MSC

When you move in the same location area, in the local area this mobility is only managed by the BS.
When I move from a BS to another but in the same location area, everything remains in that location area and it is managed by the MSC.
Where a set of msgs are exchanged from a BS to another through the MSC to allow the handover (keep your connection active and you still remain covered by some BS.
There are several control msgs that are exchanged in a mobile network to manage mobility and these set of msgs must be exchanged in a fast and efficient way in order to keep our mobility.

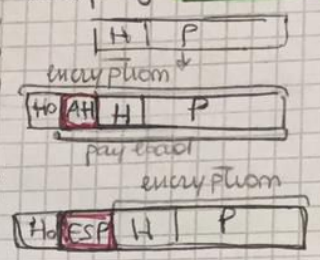
~~So if our speed is changing~~

IKE IPSec part 3 — 3/12/2020

Recap of transport mode



Recap of tunnel mode



N.B in a VPN we usually use tunnel mode

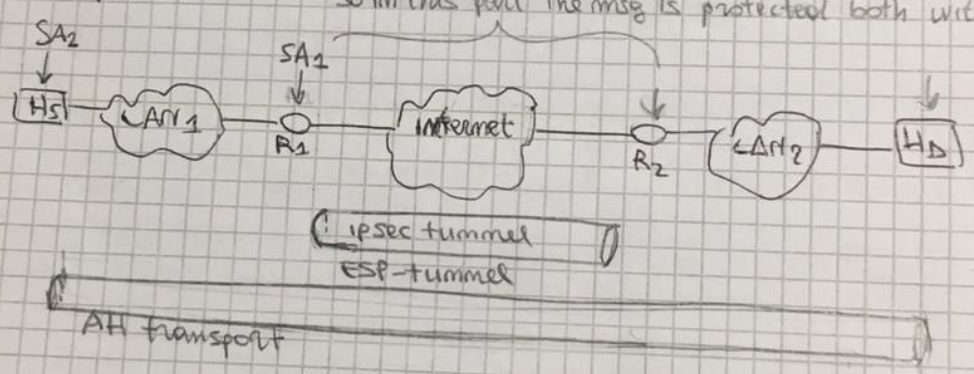
COMBINING SECURITY ASSOCIATIONS

With a single SA we can enforce a single IPSec protocol (so I can use only AH or ESP but not both)

To do that IPSec supports the concept of SECURITY ASSOCIATION BUNDLE. It means that there is a set of SAs. It is a sequence of SAs through which traffic must be processed to provide a desired set of IPSec services.

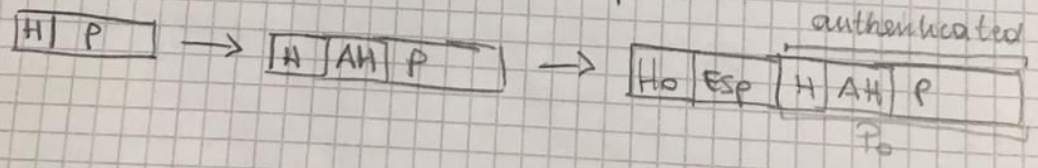
The SAs in a bundle may terminate at different endpoints or at the same endpoints.

ex



$\forall H_S \to H_D$, $B = \{SA_1, SA_2\}$

in this case the two SAs in the bundle start and end at different points



In general, bundle are used in case we want more advanced services. (For example if we want AUTHENTICATION + CONFIDENTIALITY)

- We can use a single SA ESP with Authentication Option
  - Transport mode: the IP header is not protected
  - Tunnel mode: the entire inner IP packet is protected by the privacy mechanism

- **Transport Adjacency** that uses a bundle of SAs
  it uses two bundled transport SAs with the inner begin an ESP SA and the outer being an AH SA (so we encrypt both payload through ESP and header through AH).
  The advantage is that the auth. covers more fields, including the source and destination IP addresses
  The disadvantage is the overhead of two SAs versus one SA

- **Transport-tunnel Bundle** that uses a bundle of SAs
  use bundle consisting of an inner AH transport SA and an outer ESP tunnel SA
  In this way we use authentication prior to encryption

COMBINATIONS OF SA

1) All security is provided between end systems that implement IP-sec
   examples of bundles:
   - AH in transport mode
     ESP in transport mode
     ESP followed by AH in transp. mode (ESP SA inside AH SA)
     ~~Same for~~ Any of the previous ones inside an AH or ESP in tunnel mode

2) case referred to VPNs
   security is provided only between gateways and no hosts implement IPSec
   Only a single SA is needed for this case
   Tunnel could support AH, ESP or ESP auth.
   Nested tunnels are not required because the IPSec services apply to the entire inner packet

3) gateway-to-gateway tunnel provides either auth or confidentiality or both for all traffic between end systems

4) Provide support for a remote host that uses the internet to reach an organization's firewall and then to gain access to some server or workstations behind the firewall
   Only tunnel mode is required between remote host and firewall

KEY MANAGEMENT

for every SA we need to use a security key
there are two types of key management
- **MANUAL**: used for small and relatively static environments
- **AUTOMATED**: it creates keys on-demand. we use it for very large distributed systems with evolving configurations. It is also important to negotiate SA.

In case of IP-Sec the way keys are managed and handled is by using **internet key exchange protocol**. It is a hybrid mechanism that is inspired by ISAKMP / Oakley.

Oakley is a key determination protocol (It is a Diffie-Hellman algorithm but that provides added security)
ISAKMP it defines msg format and actions that two peers have to do in order to negotiate SAs and secret keys

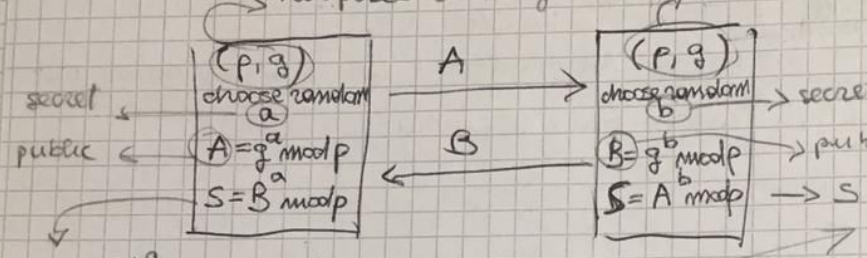
OAKLEY KEY DETERMINATION PROTOCOL

based on Diffie-Hellman

- prior agreement on global parameters
  - p is a large prime number
  - g is a primitive root of p g = generator

we use asymmetric cryptography like RSA.

two peers exchange these numbers (they are public)



$\rightarrow S = (g^a)^b \bmod p = g^{ab} \bmod p$

$S = (g^b)^a \bmod p = g^{ba} \bmod p$
$= g^{ab} \bmod p$

so these two quantities are equal.

It allows us to create keys on-demand. We don't need a preexistent infrastructure.
There are weaknesses: it doesn't provide any information about the identities of the parties.
It is subject to man-in-the-middle attacks

HIJACKING

INITIATOR — RESPONDER

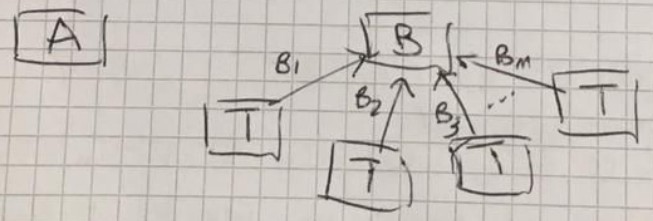
1) S [A] ← DH (Diffie-Hellman) → S [T]

A wants to exchange information with B but there is truly T

man in the middle 2) [A] —A→ [T] —T g^t→ [B]
[A] ←T_1— [T] ←B— [B]
SA — (SA, SB) — SB

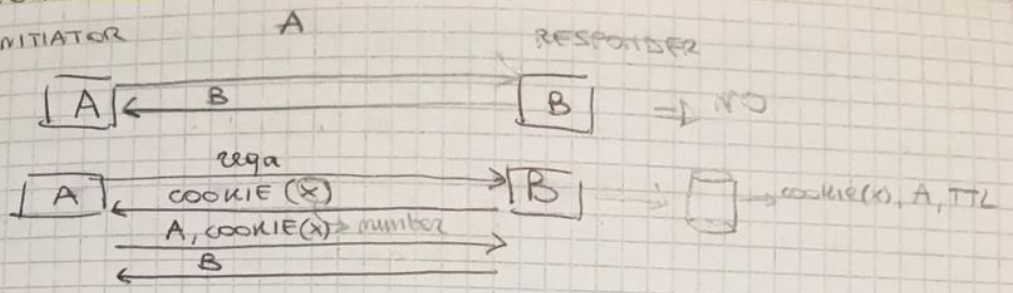
So T knows both S_A and S_B and it can decrypt msgs from B and A and send to A and B.
So B and A think that they are talking to each other.

Spoof 3) T spoofs IP address from A and T sends a lot of requests to B.
So B starts to create different public parameters (B_1, B_2 ...).
This is a heavy computation



- in order to prevent these attacks (as a difference from Diffie-Hellman) it uses a mechanism based on cookies.
- DH parameters are not passed from A to B
- it uses nonces to ensure against replay attacks
- it defines the msg format to exchange the public data.
- it authenticate the Diffie-Hellman exchange to avoid man-in-the middle.

COOKIES MECHANISM

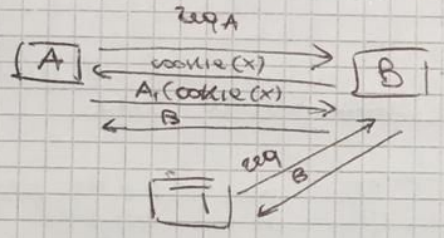


A tells B to start a DH exchange, so it sends its public parameter A. ~~and B does the same~~ As B receives the request, it starts doing stuffs. To avoid this situation the action is a little different.

1) A sends a request without specifying the public key A.
2) B responds to this request saying to A: send me the request with this number (COOKIE)
3) So A sends its public key and the cookie.
4) Finally B generates the public key B.

When B assigns the cookie, it is stored in a db in which it is reported that cookie(x) is assigned to A.
The cookie has also a time to live (TTL)

In this situation what could do an intruder T?



T could spoof the ip address of A and asks B to send him ~~the cookie~~ msg. If the TTL of the cookie isn't expired yet, B ~~would~~ could send directly the public key B to T.

But T could also spoof different ip addresses from different peers in the database and make different requests.
This forces B to access a lot of rows in the db and it could lead to a crash of the db.

In order to solve this problem the idea is to use STATELESS COOKIES, so that the only way verify a cookie is stored in the db.
I don't need to store the information, if I look the cookie I immediately get all the information I need. So I have to generate a cookie that is a function of parameters

$$COOKIE = f(A, B, secret)$$

So COOKIE is not stored in a db anymore but it is created as a function.
In order to avoid problems with any clock in the receiver calculating cookie we must guarantee that generation and verification of cookies must be fast.
There are three basic requirements for cookies:
- must depend on specific parties (A, B)
- nobody else apart from B must be able to generate private cookie
- cookie generation and verification must be fast.

OTHER SECURITY MECHANISMS

- Oakley supports the use of different groups for the DH key exchange and each group includes the definition of the two global parameters and the identity of the algorithm.
- Oakley employs nonces to ensure against replay attacks
- Three different authentication methods:
  - digital signature : the exchange is authenticated by signing a mutually obtainable hash
  - public-key encryption : the exchange is authenticated by encrypting parameters
  - symmetric-key encryption : a key derived by some out of band mechanism

AGGRESSIVE EXCHANGE

it is called aggressive because it uses the smallest possible number of msgs to perform the DH exchange.
(it is described in RFC 2412)
Slides at minute 1:26:00

ISAKMP

is a framework that defines the msg format and the functions to establish, negotiate and modify, ~~SAs~~ delete SAs.
It defines a set of payloads

Initiator cookie (64 bit)				
Responder Cookie (64 bit)				
Next payload	Mj Ver	Mn Ver	Exch Type	Flags
Message ID (32 bit)				
Length (32 bit)				

an ISAKMP msg consists of an ISAKMP header followed by one or more payloads

messages are incapsulated in UDP ~~segs~~ segments

There are different types of payloads for ISAKMP

- Security association payload used to define SAs (Important is the DOI (Domain of Interpretation) parameter).
- proposal payload (it is only 1) used to provide a set of different algs. for SAs
- transport payload (through which we describe the proposal number of proposal payload) (it is a set)
- key exchange payload
- identification payload used to share the identity of two peers.
- Certificate payload and request is used for exchange certificates
- Hash payload used for integrity of the msg and authentication
- Signature payload ~~[illegible]~~
- Nonce payload is for carrying nonces

ISAKMP EXCHANGE TYPE

Base exchange : allows key exchange and authentication material to be transmitted together

numbers request

Initiator $\xrightarrow{HDR, SA\ proposal, Nonce_i}$ Responder

$\xleftarrow{HDR, SA, choice, Nonce_R}$

$\xrightarrow{HDR, KE_i, ID_i, Auth_i}$

$\xleftarrow{HDR, KE_R, ID_R, Auth_R}$

Identity protection Exchange : expands the base exchange to protect user's identity.

Initiator $\xrightarrow{HDR, SA\ proposal}$ Responder

$\xleftarrow{HDR, SA\ choice}$

$\xrightarrow{HDR, KE_i, Nonce_i}$

$\xleftarrow{HDR, KE_R, Nonce_R}$

$\xrightarrow{HDR^*, ID_i, Auth_i}$ encrypted

$\xleftarrow{HDR^*, ID_R, Auth_R}$

Authentication Only Exchange : used to perform mutual authentication

Initiator $\xrightarrow{HDR, SA\ proposal, Nonce_i}$ Responder

$\xleftarrow{HDR, SA\ choice, Nonce_R, ID_R, Auth_R}$

$\xrightarrow{HDR, ID_i, Auth_i}$

Aggressive exchange : minimize the number of exchanges at the expense of not providing identity protection

Initiator $\xrightarrow{HDR, SA\ proposal, KE_i, Nonce_i, ID_i}$ Responder

$\xleftarrow{HDR, SA\ choice, KE_R, ID_R, Auth_R}$

$\xrightarrow{HDR^*, Auth_i}$

IKE PROTOCOL

Internet Key Exchange (IKE) protocol is a hybrid implementation of the Oakley key exchanges which is designed according to the ISAKMP framework.

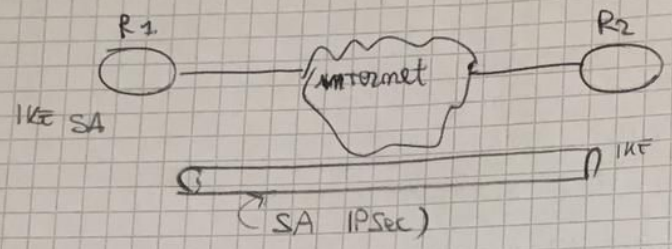
IKE negotiates and establishes both the ISAKMP SA and the IPSec SAs. It works in two phases:

- IKE PHASE I negotiation (main mode)
- IKE PHASE II negotiation (quick mode) (establishes IPSec SAs)

→

• PHASE I (main mode) is called identity protection exchange

create a secure channel (IKE channel) so that the two peers could authenticate eachother (the channel is protected with respect to integrity and confidentiality) (create a IKE SA) (at the end of phase I there are 3 different keys (two used to encrypt the last two msg of phase 1. The third one is used for IPSec



• PHASE II the SA for IPSec will be negotiated

SOFTWARE DEFINED NETWORKING (SDN) (p1) 4/12/2020

(VEDI PRIMA LEZIONE DEL 3!)

Networks are infrastructures that allow network applications to exchange msgs.
The idea is that there are two different processes that are running into different machines at layer 5. Those msgs are exchanged ~~directly~~ delivering packets to the lower layer protocols (At layer 4 we establish a logical connection between the two hosts) and then they can be sent ~~directly~~. To the layer 3 and so on.
Then the layer 3 does 2 things: routing, forwarding

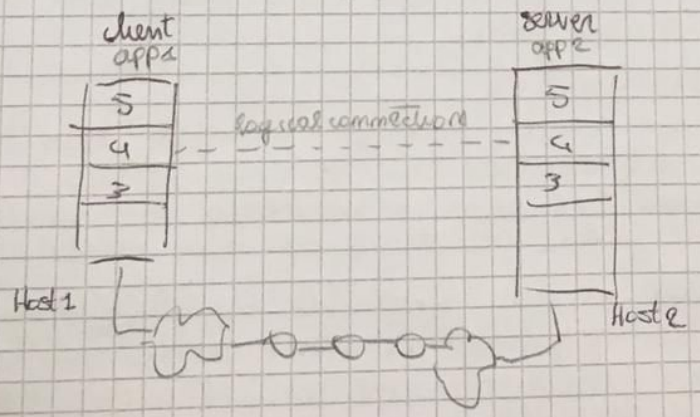
<u>ROUTING</u> is about to create and end to end path from the client to the server.

<u>FORWARDING</u>: it has to instruct the router on how to move a packet arriving from an input port and to send it to the proper output port.
(The decision is taken according to the destination address)

<u>DESTINATION BASED FORWARDING</u>

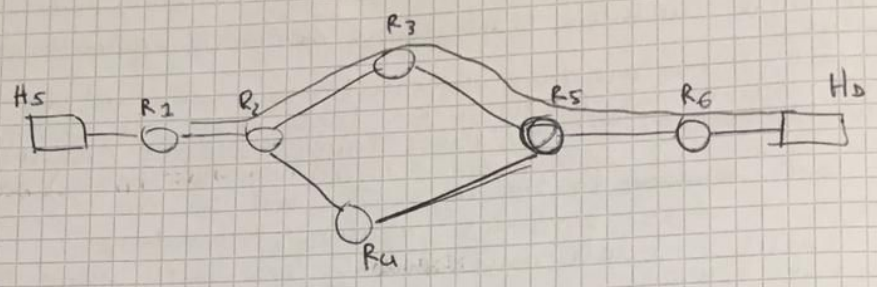
In the <u>ROUTING TABLE</u> there is the destination prefix and the output port.
How do we fulfil the routing table? this task can be performed by the routing function.
They run a running protocol that implies that every single router has to know the topology of the network, in order to do that you do the OSPF protocol.
There is a db in every single router (called topological database) where all the msgs links their advertisment msg ~~by the OSPF~~ sent by the OSPF peers are stored. Once the process has finished, the routers knows the topology and locally it can apply the routing algorithm (for instance dijkstra alg.) In this way it can discover the shortest path, and then it can fulfil the routing tables.

Paths are chosen accordingly to the following points:
- always select the least-expensive path. And in case all the links of the network have the same cost with respect to the routing protocol, then the least-cost path is the shortest path.



there is another important feature of an IP end-to-end packet delivery

Other important feature of an IP end-to-end packet delivery
Consider the following network:



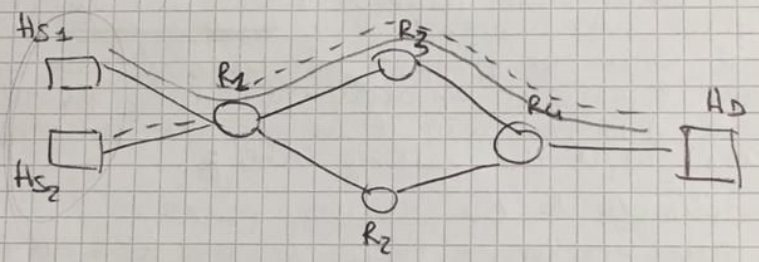
All routers run a routing protocol (as OSPF).
R_1 determin the end-to-end root to deliver packets from H_S to H_D and for example it finds that the least-cost one is the —
(all costs are the same).

So we insert a new row in the routing table.

destination dest prefix	next hop output port
H_D	R_2

In it we decide what is the next ~~node~~ to visit
(HOP BY HOP ROUTING). So R_1 send packets to R_2
but R_2 can decide ~~to~~ send packets to R_3 or R_4; so path can change between R_1 and R_2 and other routers

ex



the router R_1 doesn't know what is the source of the packets he received, so it send them all on the same path. But this cause an overload on one of the two paths.
How to solve this problem?
I define two different objectives: for example H_{S1} packets are generated by an application that requires low-latency path.
~~The blue one is made~~ The H_{S2} is generated by an application that requires high throughput. (So there are two different objectives)

This type of problem is not supported by IP because in IP the control plane (the set of functions that determin the end-to-end path) is distributed. (there is a distributed algorithm)

ROUTING FUNCION belongs to CONTROL PLANE → performed in software

FORWARDING FUNCTION belongs to the DATA PLANE
→ generally implemented in hardware

Control plane and dataplane functions are implemented in the same device
Control plane functionalities of all routers talk to each other, so →

the algorithm is distributed because every router participates and determines the output of a router.
(communication performed by using routing protocol (such as OSPF))
Control plane functionalities are implemented in software.

The forwarding is a mechanic function implemented in hardware.
While control plane is smart and flexible, data plane is constrained. (is a mechanic function)
Local forwarding table is the same as Routing table (they are implemented in the same device)

In SDN the main principle is to decouple separate the data plane from the control plane, not from a logical prospective but physically because they are implemented in different machines (in servers)
In the data plane there are switches (without control plane functionalities, that is what differentiate a router from a switch)
A switch is a multi-port device that ispect incoming packets and take decisions about forwarding, but in this case the forwarding table is not automatically fulfilled by the device itself but there is a remote controller that configures that table.
(So there are only hardware devices in data plane). → some be applice from the same server
The software part is in the control plane (which is remote).
We have a single controller which controls the network.
The controller knows the network topology, the capacity of each link and so on.
The routing table are in the control plane, but we need them in the data plane, How can we do that?
The way the control plane uses to communicate with the data plane is defining a south bound interface (south bound because it connects the controller to the switches).
The protocol used to communicate in OSPF is OpenFlow

ex
Consider an example in which a user in the user space wants to run a network application to perform different objectives, using a high level programming language (C, python, Java)
So the network operator writes itsown programms, they interact with the controller using the south bound interface and the controller translate the high level commands to a low level one (called Flow Rules that is the basic instruction that a switch in the data plane can interprete and perform). And after that it programms every single device to realize the intense of the application.

We want to have a programmable network. the switches can be programmed to act in different ways.
- ex) MIDDLE BOXES is a device (logical sometimes) that performs specific functions

→

- (ex) we have a programmable device and we can force it to work in different ways and behave like a firewall, a switch etc, depending on the program we are going to run on it

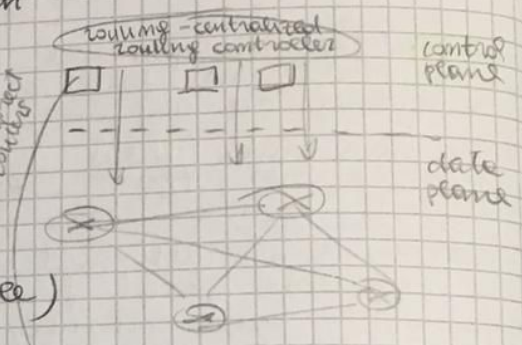
GENERALIZED FORWARDING and SDN

We can't program a network without generalizing forwarding.
So forwarding looks on many different header fields (source and destination IP, TCP ports, lower layer header fields such as MAC address, and so on)
So this device is not working as a switch but it is a multi-layer switch, so it can work over different layers of the TCPA stack?

multi layer switch or SDN switch

SDN switches can inspect different sets of fields in the header but it is not the only difference between the entry of the routing table and an entry of the so-called flow table.
(So in SDN switch we have a flow table)
The other difference is that for every each row of the table we have a set of counters to get statistics on the traffic, plus we have a set of actions to be applied on every single packet.

↳ negli SDN switches abbiamo flow tables al posto di routing table e queste f.t. vengono costruite a partire da diversi header (che indicano che ~~[illegible]~~ gli switches lavorano su strati diversi?)



difference with respect to the routers

local flow table

headers	counters	actions
⋮	⋮	⋮

OPENFLOW DATA PLANE ABSTRACTION

- flow is defined by header fields
- rules for generalized forwarding:
  - Pattern: match values in packet header fields
  - Actions: for matched packet: drop, forward, modify, matched packet or send matched packet to controller.
  - Priority: disambiguate overlapping patterns
  - Counters: number of bytes and of packets

→ for example if we have 2 different sources like in the previous example, then I can distinguish the two flows of packets using the sources and the ports and so on.

→ Is it common in IP that incoming packets have multiple entries in the routing table that have a match but the router will consider only one using the longest prefix match technique (entries having the highest priority)

↳ we assign a number to every flow rule to disambiguate overlapping patterns.

STRUCTURE OF A FLOW RULE

wildcard → I don't care the value, I put attention only to the first two elements

1) SRC = 1.2.(*).*, dest = 3.4.5.* → drop (in case there is a match, then we drop the packet)
2) SRC = *.*.*.*, dest = 3.4.*.* → forward (2) → port number
   (don't care about source)
3) SRC = 10.1.2.3, dest = *.*.*.* → send to controller
   (don't care about destination)

HOW TO TURN THE SDN SWITCH INTO DIFFERENT TYPES OF MIDDLE BOXES

(la flow tab. viene definita per ogni dispositivo, quindi per cambiare il software applicato in diverso mbox (middleboxes) è più utile agli switches)

1) We force the SDN switch to work as an IP router (by data plane prospective) **DESTINATION-BASED FORWARDING**
To do that we wildcard all the fields (*) except for destination address. Actions in Destination based forwarding are on port 6

2) **FIREWALL**: in this case we wildcard everything but TCP dport which is 22 and drop as an action
in this way we are blocking (not forwarding) all datagrams destined to TCP on port 22

Or we can have a different rule for dropping based on the source (so block all packets arriving from the particular IP source

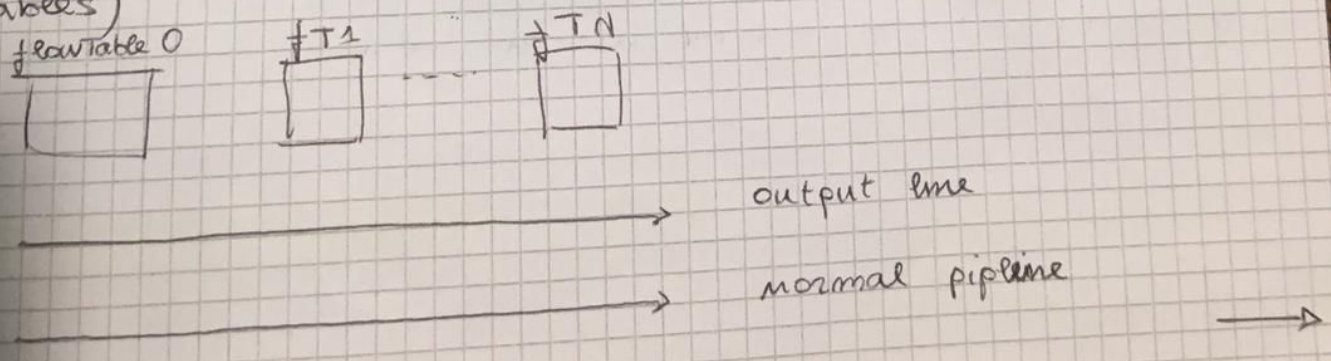
3) **DESTINATION-BASED LAYER 2 (SWITCH) FORWARDING** wildcard everything but MAC source. Action is on port 3
(This is the behaviour of an ethernet switch).

How we can program the end-to-end switch to perform different behaviours?

- ROUTER: apply longest destination IP prefix matching
  the action is the forwarding.
- SWITCH: match only on the destination MAC address
  action is forwarding or flood (like ethernet switches)
- FIREWALL: match on IP address and TCP/UDP port numbers
  action is permit or deny.
- NAT: match on IP address and port
  action: rewrite address and port and eventually forward it

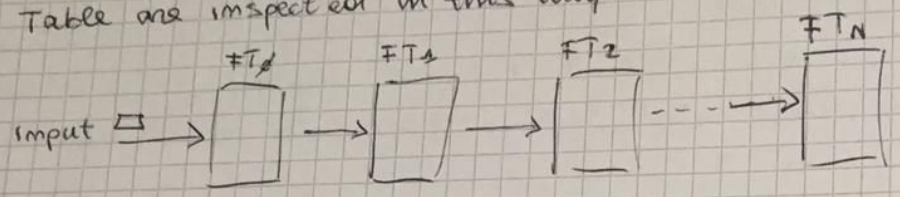
Multiple actions can be applied in SDN

In SDN there is not a single table but we implement a pipeline (by logical point of view it is organized into a pipeline of flow tables)



~~Ess~~ Whereas a SDN switch can act as a normal ethernet switch

Table are inspected in this way



~~Scopa~~

~~so packets are redirected to~~ So incoming packets are sent and redirected to where the starting point ~~of~~ the pipeline is (which is always table ∅) Table ∅ is the only table always inspected,

In each table if there is a match there is a rule that has a set of actions associated to it. ~~This set of actions is a~~ For each ~~TEMPORARY~~ incoming packet is created a TEMPORARY STRUCTURE ~~in which it~~ in which there are actions from each table, related to the packet. Actions are done ~~only~~ forward, I can't go back to a previous action

N.B. An SDN switch doesn't require an IP address for its interfaces (so hosts connected to different ports could be of the same subnet)
This is an important difference from routers

NAMEX SEMINAR

4/12/2020

Namex: internet exchange point

Internet is an interconnection of independent autonomous networks that we call autonomous systems identified by a number.

There are two principal kinds of autonomous systems:

- autonomous system that provide access to the Internet, to users and to other aut. sys.
- aut. syst that hosts content (distribute content on the internet)
- aut. sys that can do both.

Aut. sys. have to be interconnected to exchange information. There are two relationships:

- Transit relationship: where an aut. sys provides another one an access to internet. Provides connectivity
  This service is paid by the aut. sys that wants to connect itself to internet. (it is a commercial relationship)
- Peering relationship: it is not a commercial relationship, it is a mutual agreement to share resources.
  There is an improvement of the performance between two aut. sys.
  We can lower the latency if two aut. sys peer each other and share resources.
  Improvement of the overall bandwidth

BORDER GATEWAY PROTOCOL (BGP)

aut. sys use this protocol to exchange mutually information.
They can build a routing table and they can pick the best route to reach a destination
The BGP is the only protocol we use in interdomain system

INTERNET DOMAIN ROUTING

Is the domain where internet exchange points work. It is a routing between different aut. sys
They exchange information using BGP protocol.

Approach: hide the internal details of the organization (AS) and present outside only the aggregate of its networks
In this way we simplify the model and we can consider in the internet domain model the connection between border routers of different organization and border gateway routers of the same organization
This is done using TCP connection and BGP protocol
(TCP connections are called peering / transit)

INTERNET EXCHANGE POINT (IXP)

It is a place where network operators can converge to setup their relationships (peering / transit / other services)
The scope is to provide a peering service to autonomous systems →

INTERNET PEERING AT IXPs

Peering platform : is a switching platform where aut. sys can intercommect the routers and start enstablishing peering session.
FABRIC

One domain : it is a broadcast domain
PEERING LAN

One commodity : service that IXP provides to customers.
ROUTE SERVERS

ROUTE SERVER

it reflects the i BGP sessions to all the peers. It is a way to facilitate the peering agreements between IXPs (IGP interconnections)
It is an accelerator of the peering service because in this way aut. sys can use the peering service at time ~~because~~ and it is the only way to get prefixes from the IP content providers.
On router server infrastructure tipically IXPs do filtering controls ~~and they can~~

COLOCATION AND MMR

network operators can install a point of presence inside IXP data center (represented by equipment like routers, switches and so on)

MMR (MEET ME ROOM ?)
can allow network operators to enstablish private network intercommection
it intercommects physically different operators in an IXP

Operators can enstablish a PNI (private network intercommection) ~~among~~ between them

Through the peering session over platform operators can enstablish a peering session or VPNI (virtual PNI)
or they can have a peering session with the route servers as well
→ in MMR we use fibers

NAMEX

IXP in Rome, second IXP in Italy (→ it is a consorcium)
is neutral, non-profit, member based
Services : PEERING (there is a data center in San Lorenzo) (the main one)
REMOTE PEERING (which is the peering with the IXP of north Europe)
There are different points of presence in Rome.

There are different INTERCONNECTION OPPORTUNITIES in NAMEX

- if two network operators are located inside the same data center (local) they can do public peering and they can also use i-PNI and VPNI for other services.
- if they are in different data centers they have peering, VPNI and Metro PNI (MPNI)

Why network operators may choose virtual interconnection instead of physical interconnection?
Big content providers don't allow small internet service providers to have private interconnection because they are very small, they generate not so much traffic so they can communicate physically through a port.
On private interconnection big network operators (like Netflix) can redirect a great amount of traffic

INTERNET TRAFFIC

during spring (covid 1) there was an +40% of traffic and we had a peak in the middle of march (152 Gbps)
There were many upgrades on customers ports on peering
(this sudden increase of traffic brought many problems to internet providers about capacity. So the IXP supported them in order to enlarge the capacity of infrastructure).
So NAMEX provided free upgrades To members

PRE-COVID: most traffic was in the evening from 21 to 23

DURING COVID: everything changed because the peak of the traffic was not in the evening anymore but the level of traffic in the morning was the same in the afternoon and in the evening

(Now in Autumn the traffic is as in spring and sometimes in the morning is higher than in the evening)

During the pandemic and up until now there was a +60% in upload because we are more connected and we do much smart working, online meetings and so on.

ROUTING SECURITY

BGP was a protocol created before security was a concern. It assumes all networks are thrustworthy.
There is no validation process inside BGP. So when two aut. sys. establish a peering session, you have to specify the aut. sys number, you have to announce your prefixes and on the other side you can receive the prefixes the other part announce to you but: Are you sure that those information are thrustworthy?

In BGP there isn't a check, it assumes all networks are thrustworty

ROUTING INCIDENT HAPPEN ACROSS THE INTERNET

2019 over 10 000 routing outages or attacks (hijacking, leaks and spoofing)

→

ROUTING THREATS

Route hijacking: a network operator pretends to be another one so the traffic to a destination will pass throug the first one

Route leak: it is a misconfiguration issue. It happens when we have an aut. sys which has smaller than 1 upstream provider.

IP address spoofing: technique used to hide the identity of a server and to impersonate someone else. (Attack called DNS amplification attack)

TOOLS TO HELP AGAINST THREATS

Prefix filtering, but not enough. We need coverted actions to improve routing security

REGIONAL INTERNET REGISTRY: IP addresses and aut. sys numbers are allocated and assigned by entities in the world called regional int. reg.
In our region (Europe and Russia) we can identify RIPE NCC
In it there is internet routing registry that contains information about internet resources (such as origin and prefix objects...)

PEERING DB is a db where network operators can update regarding its points of presence, internet exchange points where this network has an interconnection, information about prefixes

RESOURCE PUBLIC KEY INFRASTRUCTURE

it is a robust security framework for verifying the association between resource holder and internet resources.

The result is a list of all valid combination of ANS.
Validated ROA contents are called "Validation ROA Payload"

Based on BGP announcements and on ROAs you can instruct your router to make some decisions: modify LP, filter the announcement...

GLOBAL VALIDATION

Is a mechanism to face the threads.

FILTERING

aut. sys can filter from IRR DATA, RPKI OV or filtering from upstream or big networks

ANTISPOOFING

a router can check only the destination address and the network operator ~~ha tale~~ wants source address validation

COORDINATION

update peering DB database with noc contact information
update IRR with noc contact information

ROUTING SECURITY AT IXP

- ~~we do~~ they do filtering inside route service infrastructure. Filtering is based on the information inside the internet routing registry by using a (AS-SET) object

they do a validation of RPKI

they filter MARTIANS and BOGONS prefixes based on Team Cymru service (list of bogons and martian prefixes tha is used to do filtering)

Invalid prefixes are dropped.

- protect the peering platform on Layer 2. Only IPv4, IPv6 and ARP protocols are allowed.

IXPs publish the policy of traffic not allowed.

They perform monitoring

- remote-triggered blackholing it means that they use a blackhole server to redirect all malicious traffic

---

hijacking is a problem among aut. sys. not ~~end~~ end users. ~~It is about~~

SOFTWARE DEFINED NETWORKING (SDN) pt. 2 | 10/12/2020 |

there is a central controller which is in charge of running control plane functionalities.
On the other hand there are devices in the data plane that can act as simple switches. (Though they can apply generalized forwarding)
Through SDN we can create a programmable network.

SDN was thought in 2005 to rethink network control plane
Since the born of internet the periferic areas have changed a lot but not so much the core.
(for example BGP protocol is pretty much the same as it was in 1989). Change the way the core works is really hard.
So how to add flexibility to the core part of network? It is necessary to decaple the control plane functionalities from the data plane functionalities.

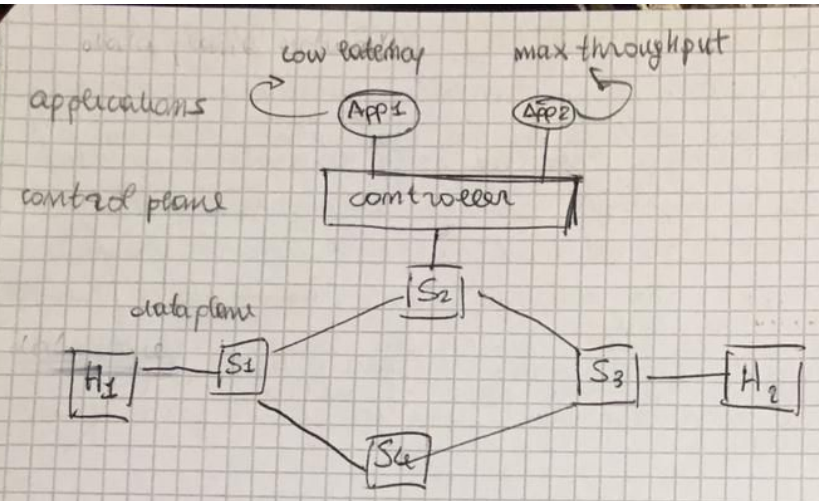
ANALOGY: mainframe to PC evolution

The path was the same from mainframe servers to PCs.

Initially there were mainframe server realized with specialized hardwares and performing. On top of that there is a specialized operating system tha can interact with the hardware.
And on top of that run specialized applications.
(Vertically integrated system)
It is hard to update. (because it is also expensive)

So then we passed to a different configuration where is a general purpose hardware (cheaper) (Microprocessor).
So in the middle between apps and hardware there is another layer (the operating system) which can interact with the applications (written in a high level programming one).
(In this way we don't have to write programms in machine language).
In this way using Horizontal Open interfaces we have a better flexibility

this is the same philosophy that SDN wants to apply to a network.
So our network is composed of SDN switches (hardware) so there is the data plane where no software runs.
There is an entity which interacts with dataplane (which is the SDN controller) (it represents the network operative system
On top of that network engineer can program different applications to perform different tasks



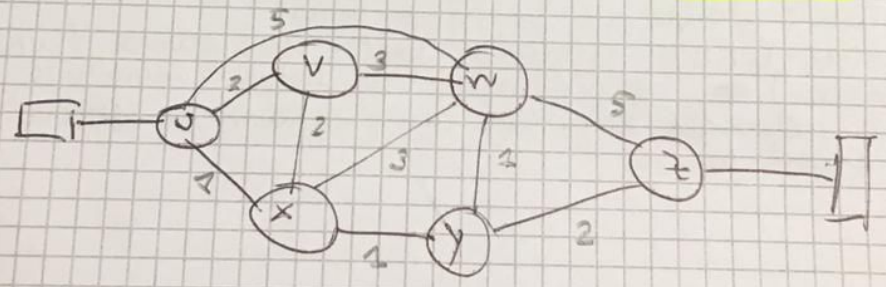
SDN can work with two different approaches:

- PROACTIVE: SDN switches have a set of preinstall rules. (so if a packet arrives, they have a rule to handle it without talk to the controller).
- REACTIVE: at the beginning the flow table of the switches are empty. When a packet arrives to the switch, since the switch doesn't know how to handle the packet, it will send the packet to the controller. The controller takes its decisions and says the action that the switch has to do

We can use both approaches together and this is good because it is useful to have a set of preinstalled rules but for specific flows I will ask the controller

This is a huge difference between IP routers because when they receive packets and don't know what to do, they drop the packets.

TRAFFIC ENGINEERING: DIFFICULT TRADITIONAL ROUTING



1) network operator wants to go from u to z with path u, v, w, z and another path from x to z x, w, y, z
How can we do it in IP? It is very hard (quite impossible)

In IP the idea is that we can exploit the link weights and move them as the are "knobs" in order to change the routing.

Tipically the best path (shortest one) from u to z is u x y z,

but I want U, V, W, Z. So how can I force IP control plane to find a path as the shortest one?
We can play with the links weights, for instance we can increase a lot cost UX and UW

How can I go X, W, Y, Z? there are a set of algorithms that do this job. They are centralized algorithms.
(WEIGHT OPTIMIZATION ALGORITHM) It takes as input a graph $\underbrace{G(N,L)}_{graph}$, $\underbrace{D(f_1, f_2 \dots f_n)}_{demand}$, LINK capacity
and it returns as output the weight W that optimize this function which is that that minimize link congestion
Now we can configure in the router this set of weights W and get the routing that we want.
HOWEVER: this algorithm is heavy, we need to run it offline using a single server, and it configures the weights

So once I do that the IP control plane will take the decision in a distributed manner and it will end up finding the exact path that I want, but in the meanwhile, the traffic demand could change, so we could to it once more.
So it is quite hard to do that using the distributed control plane.
On the other hand if I have the central controll we can simply monitor the infrastructure using the openflow protocol and always optimize the routing according to the current demand.

---

2) Another problem is if we want to split the traffic from U to V and X.
This is not something that can be done with IP control plane.

---

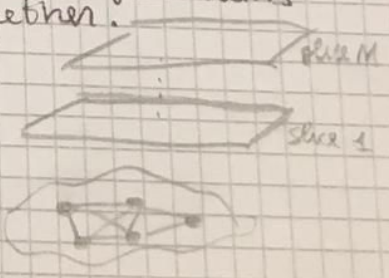
3) Another example is NETWORK SLICING (it is the way to differentiate how the traffic is handled) (It is one of the basis of 5G architecture).

5G has a set of requirements:

- Massive machine type communication MMTC
  (and this intended to provide connectivity for IOT networks and to provide machine-machine communications. It is used to realize smart environments)
- Ultra Reliable and low latency communication URLLC
  (this is hard to realize because the connection is wireless, so there could be obstacles along the path).
  It is used for example for remote control of drones or robots
- Enhanced Mobile Broad Band MBB
  (provides a lot of data rate speed to inbound and outbound traffic)

These three requirements represent 3 different objective functions and they are almost impossible to get all together.

So we have the physical infrastructure and a set of virtual layers called slices (as many as we want).



i need to serve different applications in different ways