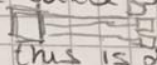
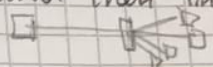
How do we provide those fibers?
The idea is: starting from the original structure based on copper, we replace part of it with the fiber.
(FTTC cabinet or FTTC curb)
(FTTB building)
(FTTH home)

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

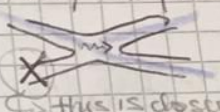
1) put the fiber replacing completely the copper cable, so we have one fiber for every user.
(REPLACE FIBER TO THE WHOLE PATH and this is done by performing digging. Micro digging cost 30/40 K €/km)



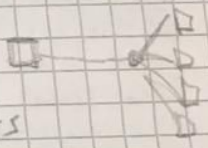
2) put only one fiber till a network element (for example the curb/cabinet) and then have other media like copper from the cabinet. (Ho una sola emea di fibra fino alla cabinet)
The curb/cabinet is called ACTIVE ELEMENT because it is the element where the optical signal is received, is converted to a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

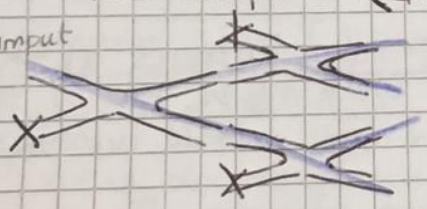


3) there is ~~another~~ simplest solution that is named PASSIVE ~~SPLITTER~~ (and this is where derives the name passive optical network) PON. It is named PASSIVE because this element is very simple:
The splitter is fusion between two fibers together and it has the possibility to split the light because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



1x2 splitter
1 input 2 outputs

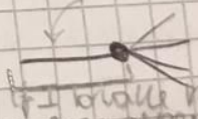




1x4 splitter
1 input 4 outputs

1xm splitter
1 input m outputs

CONS:
- Every time the signal is split in two ways, the signal is reduced by $10 \log(0,5) = 3dB$
  Loss is circa $3dB \times \log_2(\#^{n°} ONUs)$
- 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.

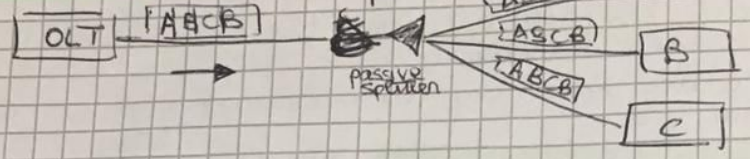
How to recognise the information of the users ?

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 arm, an address, but this address is needed to pick up the from the only my information from the aggregated flow

Upstream e Downstream hanno colori di frequenza diversa, quindi passo fare confusione. Dovrei up.

N.B

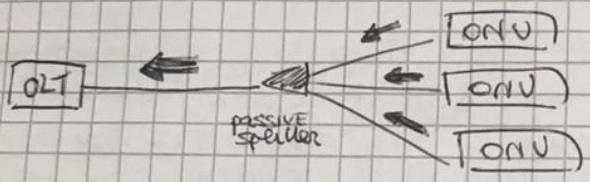
DOWNSTREAM



(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



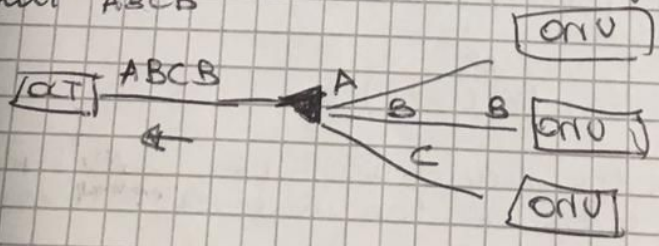
So we have signals that may overlap. (at the splitter some collision may happen).

N.B

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 units have to transmit. And this 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 some msg changes. But we don't want a signal that changes during the burst, so the →

Optical line Terminal (OLT) provides a mechanism to [illegible] the level of the signal ~~on the~~ basing on the distance.
So it sends a ~~ma~~ 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 all'utente a quale potenza deve essere mandato il segnale)
(This is done burst by burst)
↳ manda un burst di messaggi a tutti gli utenti

PON is very used and the solutions that current operators offers 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 ~~ef~~frequenze di quel colore

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

N.B 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. ~~Then~~ In the upstream the different wave lengths 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 wave length that can be supported in the same fiber (in order of 10s)

How to implement EPON configuration?

1) OLT → ONU, ONU, ONU — TREE topology

2) OLT, ONU, ONU, ONU — RING in two directions topology

3) OLT → ONU, ONU, ONU — TREE with redundancy (trunk)
evita il single point failure
redundancy

4) OLT, ONU, ONU — BUS topology

19/11/2525

LTE / LTA-A CELLULAR SYSTEM

WIRELESS ACCESS

2 kinds of wireless systems:

- **BROADCASTING SYSTEM** (broadcast) (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 and 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 BACKHAUL)
  ↳ le interconnessioni tra BS sono backhaul

What is the difference between control and user information?
(Data supporters) → 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 the possibility to support mobile users.

(Because while in 3GPP ~~and ...~~ from the very beginning ~~opportunity~~ 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 preluminar 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)
Them technologies evolved toward other solutions and the most compelx 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~~ needs ~~need low~~ low latency connection.
(Low latency means more real time simulation)

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 & it is important the ~~handling~~ handeling 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 & 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 ~~telephones~~ & 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 HAND OFF 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 maintain 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.

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 silliest 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 multihop 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 vehicolar 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 viene 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 (while in a fixed network you can control who is accessing, who performs the routing, you can't control devices connected wirelessly)
  - ~~energy~~
  - 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 ~~matter~~ 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 compoments:

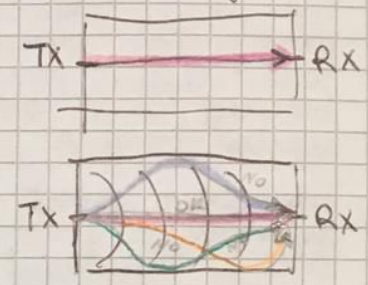
  In the ~~~ Spectrum depends on which is the spectrum we can have the interference of internal sources (devices that by ~~[illegible]~~ the spectrum are authorized to transmit in the same spectrum) and devices that are external that are not authorized to transmit in that spectrum but generate some interference.

  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 →

  non puoi trasmettere su una banda medica o su quelle della polizia.

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

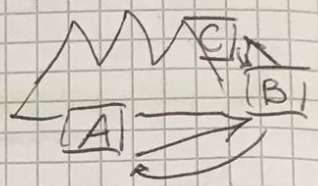
(*) se più è alto SNR più posso avere BitRate alto (QUAM 256 (8 bits))

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

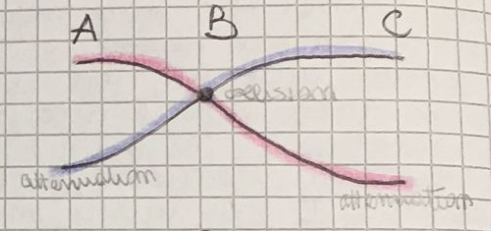
- Another phenomenon which is only present in the wireless is the **hidden terminal problem**.
The devices composing my channel are not known by all the users because of no radio propagation condition

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 Inter Frame 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 received by the other side.

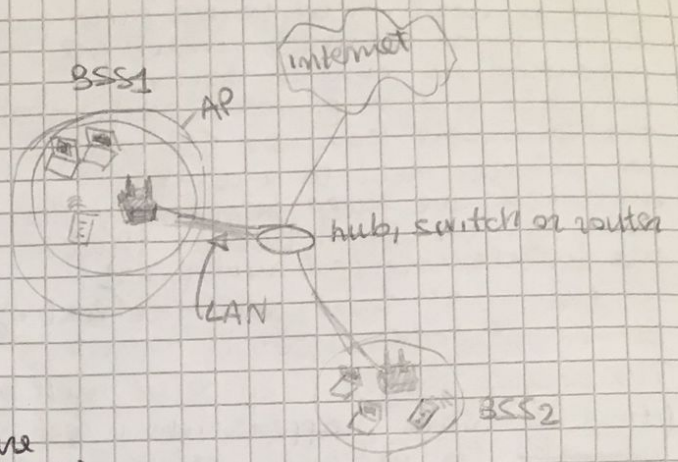
<u>On the receiver side:</u>
If they are received correctly, the receiver listens for a while to the channel and time is SIFS (short Interframe Spacing) and then the receiver sends an ACK to the sender so It can know that the data were received **correctly**

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 receive 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 ~~doesn't~~ increases at every attempt.
In this way I try to avoid next collision.

25/11/2020

WIRELESS ACCESS pt 2

LAN ARCHITECTURE

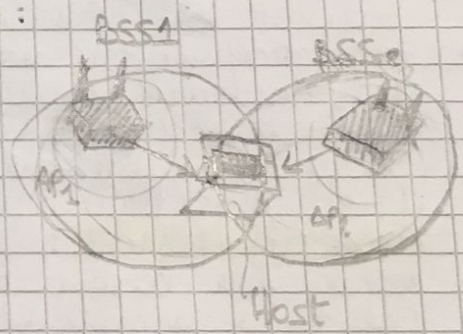


there is an area covered by an access point (AP) that contains several mobile hosts that are interconnected wirelessly to the AP.
In the WI-FI terminology this area is called Basic service set (BSS) (it is the corrispondent of a cell).
The BSS is interconnected with a very simple infrastructure which is local area network (LAN) to a switch or a router that allowes 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) quindi privato

For association there are two methodologies:

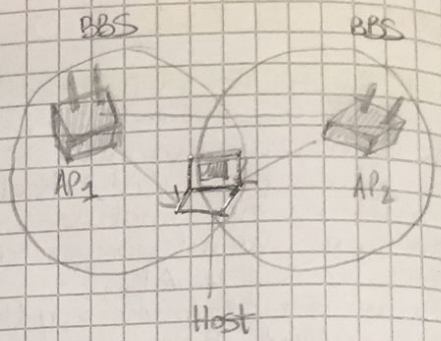
- **PASSIVE SCANNING**



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. ~~send 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.

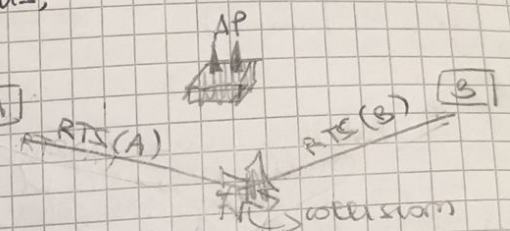
During association response we do authentication.

ACCESS for MOBILE SYSTEM

- there are two ways that have been implemented in WI-FI:
  - perform 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 occurr in wired connection because in terms of signal in a wired conn. there is no way that I cannot ~~see~~ 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 acknowledgment.
    So if the acknowledgment 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^m where m 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.

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

it is executed in a distributed manner but there are control msg named requests to send and clean 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 wasting 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
succesfull 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 clean 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 B wants, it can go to sleep mode because the sleep mode in the Wi-Fi saves energy.

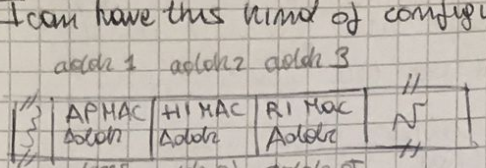
So in this case the protocol is much more performing, but the price to be payed is the time spent to send control msgs.

ADDRESSING

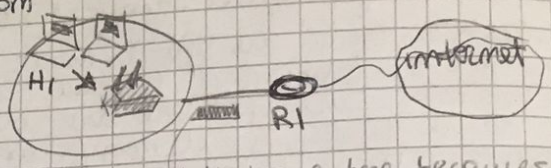
Like in the 802 family, the frame of Wi-Fi is formed in the classical manner, so there is control frame, duration, addresses, sequence control a variable size payload and CRC (connection code)
There are 4 spaces for the addresses.

Address 1: MAC address of 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)

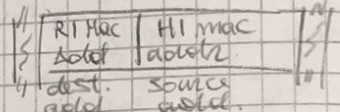
- I can have this kind of configuration



(802.11 frame)



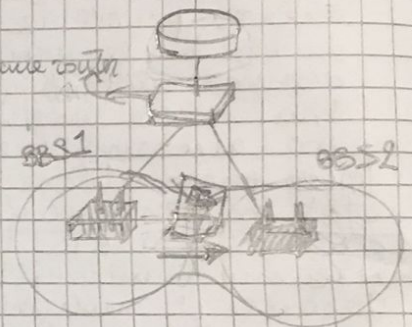
↳ the frame here becomes a classical internet frame (802.3 frame)



- in the Ad-hoc mode we can perform multi-hops on devices, so there is also the address of the next hops 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 anymore).



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 perform on my wireless channel, changes depending on the channel SNR, so 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

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 Haul). 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 haul now is becoming fondamental 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).

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

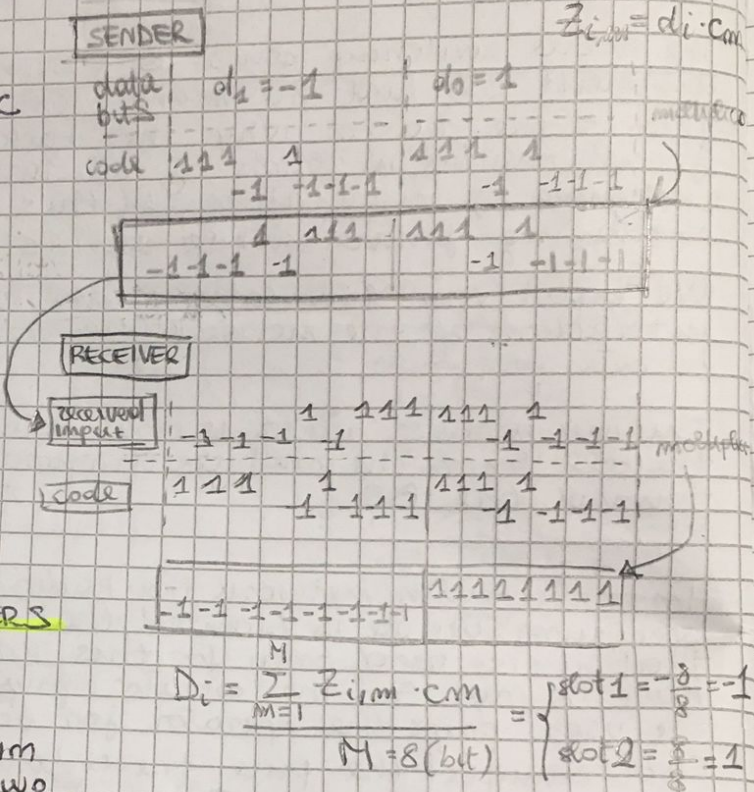
1) Frequency division multiple access (FDMA)
In frequency there are different channels, and in these channel I can put the transmission of one or multiple users (Multiple users may transmit on multiple channels).

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

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

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



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

TRANSMISSION OF MULTIPLE USERS

in this case each user has its 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 information of a specific user and to cancel in 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.

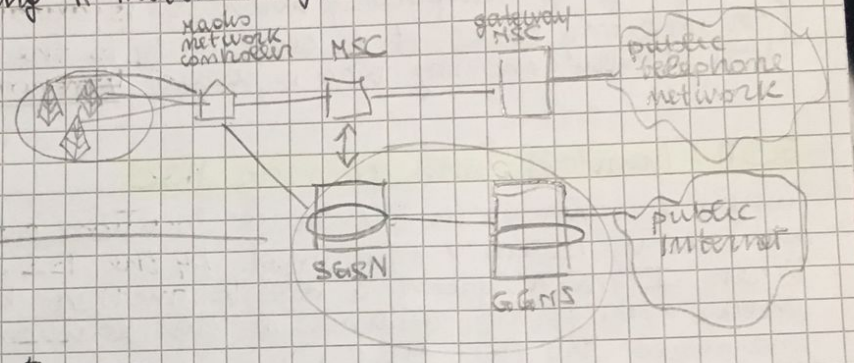
) the assignment of the code is performed by the BS

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 Visited 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 mutually 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 change 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 Anchor MSC)

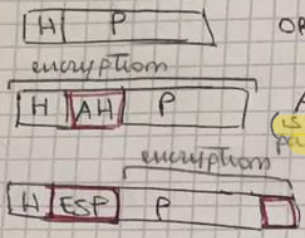
GSM: handoff with common MSC

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.

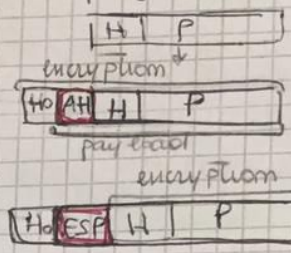
IKE IPSec part 3

3/12/2020

Recap of transport mode



Recap of tunnel mode



(ESP in tunnel mode can protect payload and header of the original msg)

N.B in a VPN we usually use tunnel mode

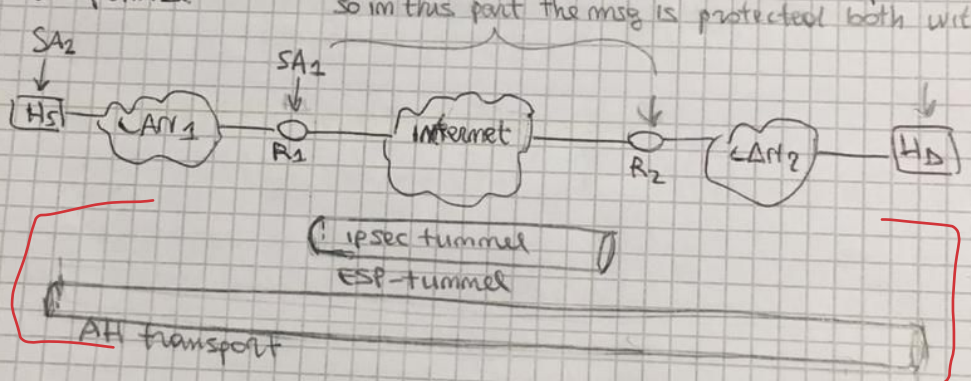
COMBINING SECURITY ASSOCIATIONS

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.

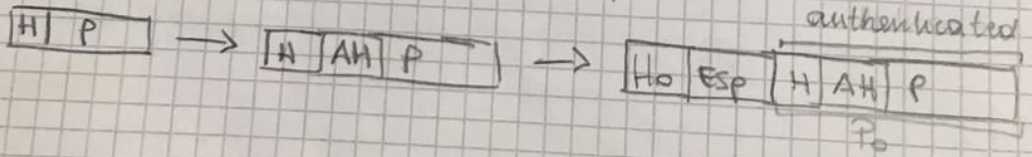
The SAs in a bundle may terminate at different endpoints or at the same endpoints.

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 being 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) If 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)
   - 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 workstation 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

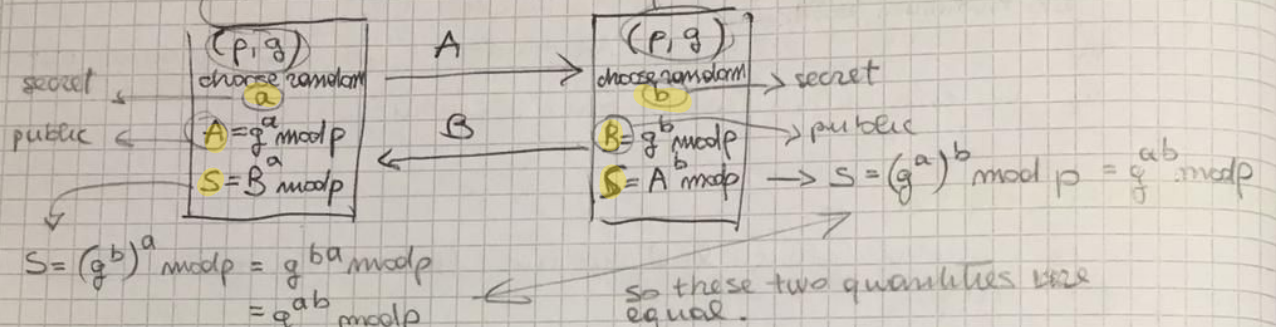
OAKLEY KEY DETERMINATION PROTOCOL

based on Diffie-Hellman

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

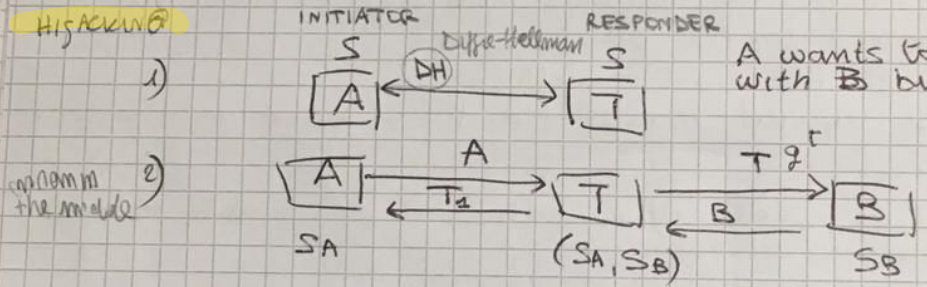
we use asymmetric cryptography like RSA.

two peers exchange these numbers (they are public)



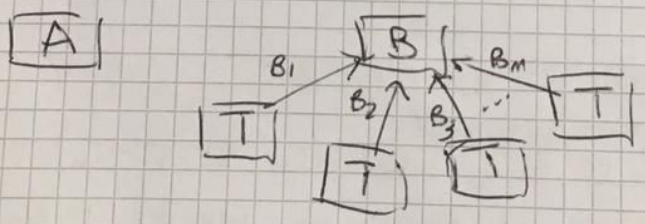
It allows us to create keys on-demand. We don't need a preexistent infrastructure.
There are weaknesses: it doesn't provide any information about the identities of the parties.
It is subject to man-in-the-middle attacks

HIJACKING



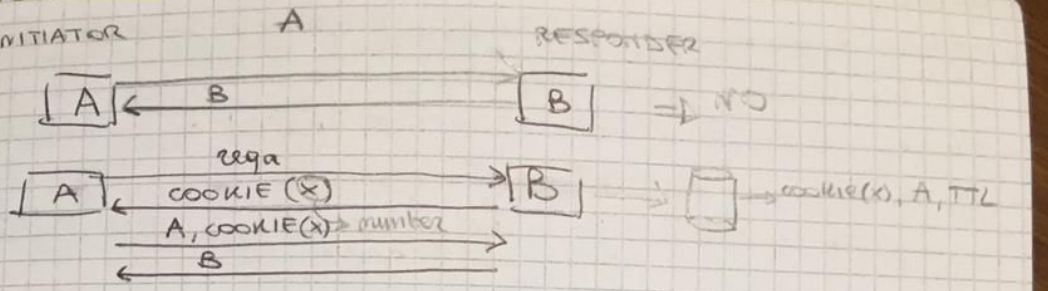
So T knows both S_A and S_B and it can decrypt msgs from B and A and send to A and B.
So B and A think that they are talking to each other

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 $(B_1, B_2 \dots)$.
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

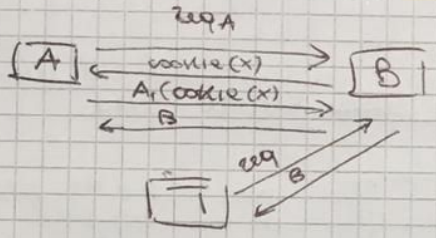


A tells B to start a DH exchange, so it sends its public parameter A. As B receives the request, it starts doing stuffs. To avoid this situation the action is a little different.

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 msg. If the TTL of the cookie isn't expired yet, B 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 server 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

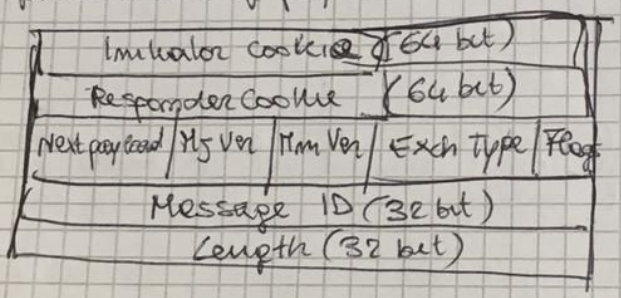
- Oakley supports the use of different groups for the DH key exchange and each group includes the definition of the two global parameters and the identity of the algorithm.
- Oakley employs nonces to ensure against replay attacks
- Three different authentication methods:
  - digital signature: the exchange 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



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

messages are incapsulated in UDP ~~segments~~ 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 (it is a set) (through which we describe the proposal number of proposal payload)
- 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 ~~NECESSARY~~
- Nounce payload is for carring nonces

ISAKMP EXCHANGE TYPE

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

Initiator → Responder
- HDR, SAproposal, Nonce$_i$
- ← HDR, SA, choice, Nonce$_R$
- HDR, KE$_i$, ID$_i$, Auth$_i$
- ← HDR, KE$_R$, ID$_R$, Auth$_R$

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

Initiator → Responder
- HDR, SA proposal
- ← HDR, SA choice
- HDR, KE$_i$, Nonce$_i$
- ← HDR, KE$_R$, Nonce$_R$
- HDR*, ID$_i$, Auth$_i$ (encrypted)
- ← HDR*, ID$_R$, Auth$_R$

Authentication Only Exchange: used to perform mutual authentication

Initiator → Responder
- HDR, SAproposal, Nonce$_i$
- ← HDR, SA choice, Nonce$_R$, ID$_R$, Auth$_R$
- HDR, ID$_i$, Auth$_i$

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

Initiator → Responder
- HDR, SA proposal, KE$_i$, Nonce$_i$, ID$_i$
- ← HDR, SA choice, KE$_R$, ID$_R$, Auth$_R$
- HDR*, Auth$_i$

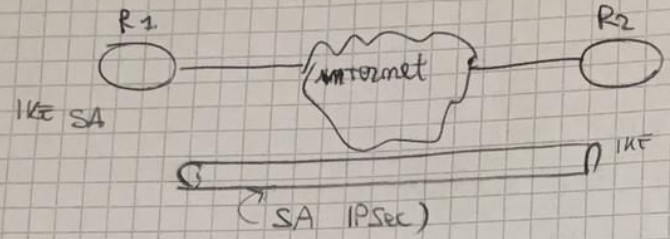
IKE PROTOCOL

Internet Key Exchange (IKE) protocol is a hybrid implementation of the Oakley key exchanges which is described 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 negotiations (main mode)
- IKE PHASE II negotiation (quick mode) (enstablishes 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!)

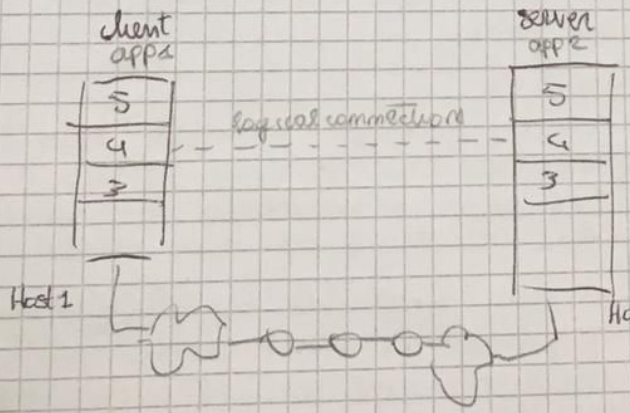
Networks are infrastructures that allow network applications to exchange msgs.
The idea is that there are two different processes that are running into different machines at layer 5. Those msgs are exchanged ~~through~~ delivering packets to the lower layer protocols (At layer 4 we establish a logical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

FORWARDING: 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)

DESTINATION BASED FORWARDING.

In the ROUTING TABLE 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 router 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 table.
Paths are chosen accordingly to the following points:

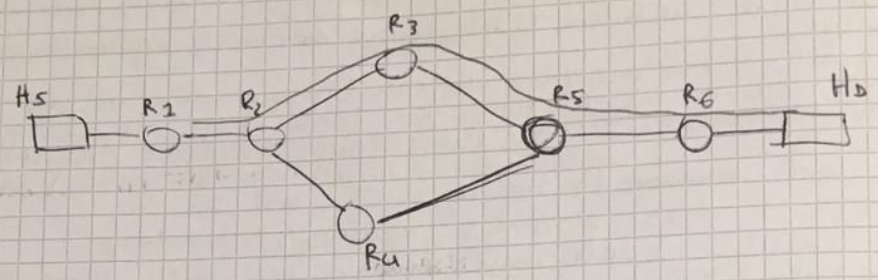
- always select the least-expensive path. And in case all the links of the network have the same cost with respect to the routing protocol, then the least-cost path is the shortest path.



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 tables.

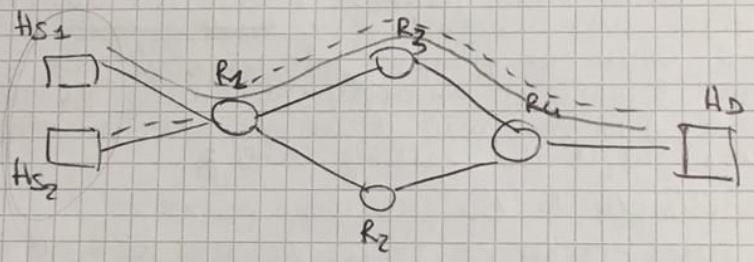
In it we decide what is the next ~~node~~ to visit

(HOP BY HOP ROUTING). So R_1 send packets to R_2

but R_2 can decide ~~if~~ send packets to R_3 or R_4; so path can change between A_1 and R_2 and other routers

destination: dest prefix	next hop: output port
H_D	R_2

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 generate by an application that requires low-latency path.

~~The best 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)

↳ performed in software

ROUTING FUNCION belongs to CONTROL PLANE

FORWARDING FUNCION 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 vsing 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 principe is to decouple the data plane from the control plane, not from a logical prospective but physically because they are implemented in different machines. (in switches)
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).

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 tables 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 vsed 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 its own programms, they interact with the controller vsing 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.

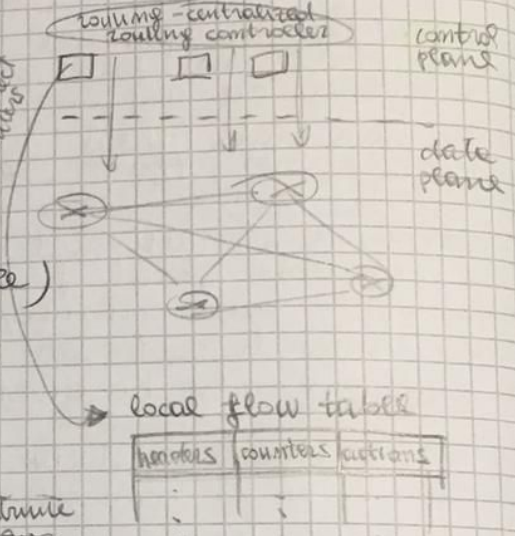
We want to have a programmable network. the switches can be programmed to act in different ways.
- ex) MIDDLE BOXES is a device (logical sometimes) that performs specific functions

→

- (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 TCP/A 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 ft. ti vengono costruite a partire dai diversi headers (che indicano che ~~sono~~ gli switches lavorano su strati diversi?)



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

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

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

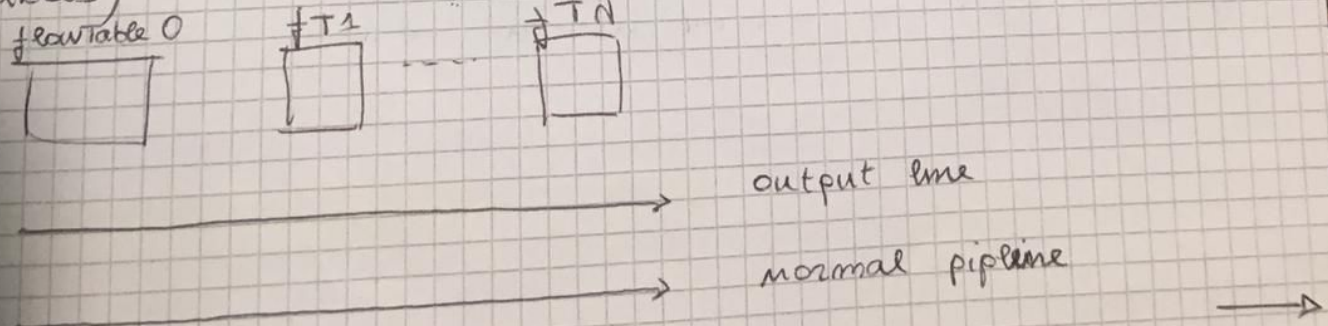
3) DESTINATION-BASED LAYER 2 (SWITCH) FORWARDING wildcard everything but MAC source. Action is on port 3
   (This is the behaviour of an ethernet switch).

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

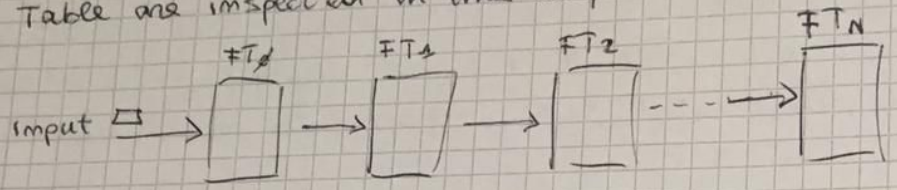
- ROUTER: apply longest destination IP prefix matching
  the action is the forwarding.
- SWITCH: match only on the destination MAC address
  action is forwarding or flood (like ethernet switches)
- FIREWALL: match on IP address and TCP/UDP port numbers
  action is permit or deny.
- NAT: match on IP address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



~~Essa~~ Whereas a SDN switch can act as a normal ethernet switch Table are inspected in this way



~~sospa~~

~~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 0) Table 0 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 each t~~ 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 indipendent 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 paied by the auts 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 internals details of the organization (AS) and present outside only the aggregate of its networks
In this way we semplify the model and we can consider in the internet domain model the connection between border routers of different organization and borders gateway routers of the same organization
This is done using TCP connection and BGP protocol
(TCP connections are called peering/transits)

INTERNET EXCHANGE POINT (IXP)

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

INTERNET PEERING AT IXPs

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

One domain / PEERING LAN : it is a broadcast domain

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

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 0 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 interconnection
it interconnects physically different operators in an IXP
Operators can enstablish a PNI (private network interconnection) 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, local)

- if two network operators are located inside the same data center 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 for 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 providers 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 on 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 of 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 miscomfiguration 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 concerted 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 ~~has to~~ wants source address validation

COORDINATION

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

ROUTING SECURITY AT IXP

- ~~they 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 that 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 decouple the control plane functionalities from the data plane functionalities.

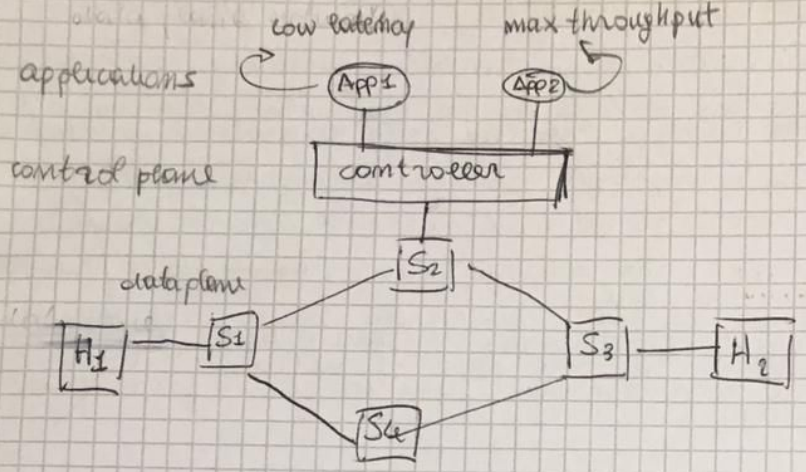
ANALOGY: mainframe to PC evolution

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 that 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



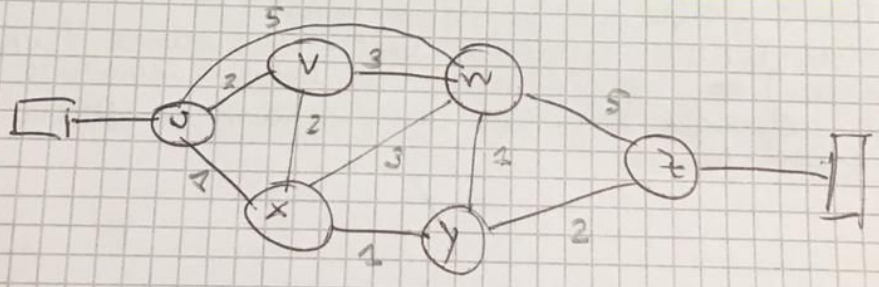
SDN can work with two different approaches:

- 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 tables 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 ~~[illegible]~~ 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. ~~[illegible]~~ (WEIGHT OPTIMIZATION ALGORITHM) It takes as input a graph $G(N,L)$, $\Delta(f_1, f_2 \dots f_n)$, Link capacity
graph demand
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 ~~[illegible]~~ and get the routing that we want.
HOWEVER: this algorithm is heavy, we need to run it offline using a simple 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.

---

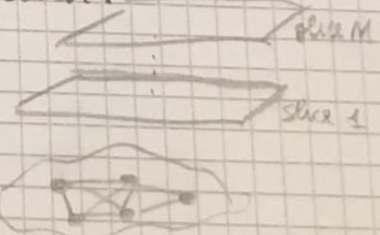
3) Another example is NETWORK SLICING (it is the way to differentiate how the traffic is handled) (It is one of the basis of 5G architecture).

5G has a set of requirements:

- Massive machine type communication MMTC
(and this intended to ~~[illegible]~~ 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
- Enanced Mobile BroadBand .. 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