1 GSM and Mobile ip

GSM is the radio network you use to access data.GSM uses time division multiple access(TDMA) to send down the digitized and reduced data through a channel . Mobile IP is used to transport your IP data from your device to a centralized exit point where it enters the public internet. Mobile IP is a communication protocol, extending IP, that let to the users to move from one network to another with equal IP address.
Advantages GSM: GSM provides improved spectrum efficiency, Low-cost mobile set and base stations, High-quality speech, International roaming, Compatibility with Integrated Services Digital Network (ISDN).

2 LTE and LTE -Advanced

In comparison with LTE we'll have a number of key requirment and features: we move the datarate until 1 Gbps in downlink and in 500Mbps uplink. We increase the spectrum efficiency and range. Cell edge user throughput is twice than LTE. In the following appraoch we add a number of antennas for increase performance but also we increase the overhead and the return per addictional path is less. Although we use a carrier aggregation technique which let us to utilise multiple channel either in the same bands or different areas of the spectrum to provide the required bandwidth because there is not sufficient contiguos spectrum. It's introduced a scheme known as coordinated multipoint for solving interference of adjacent cells. LTE Relaying for improving coverage.The cost per bit is reduced, and with the faster speeds, users tend to consume more data, thereby raising revenues. Accordingly LTE-Advanced has provided improvements to both users and operators, as well as those providing additional services.

3 SDN Mobile

In LTE ther's not a clear distinction of control and data plane. The main problem of data plane is that is too much centralized in detail the problem is the scalability of packet data network gateway instead the control plane is that is too much distributed in detail problem with handoff and resource radio allocation. Now if we implement a SDN in mobile infrastructure we could have a logically centralized control plane with a common control protocol that works across different cellular technologies. Then we implement a switch SDN able to: 1)reduce the traffic and control the flows 2)reduce the need of extra device 3) create a flexible network virtualization by slicing flow space. CellSDN provides scalable, fine-grain real time control and it's simple to manage , introduce new services and inter-operate with different technologies. Cooper's Law said that capacity improvements come from increasing cell density.Wireless network architecture that provides unified software interfaces to: 1. Query wireless networks about availability, quality, location, spectrum, interference. 2. Control granularly how individual user or application traffic is handled by the network across the entire stack

SDN-Mobile benefits: Major scalability and cost limitations of current cellular networks arise from: – Centralized data-plane functionalities implemented at the gateways – Vendor-specific configuration interfaces that communicate through – complex control-plane protocols and – Inefficient and non-flexible network architecture

4 How copper wires changes from analog to digital

Analog communication the goal is to transmit a waveform which is a function that varies continuosly with time and the following flow must be reproduced exactly at the output of the analog communication system. In practice communication the distortion is unavoidable. In digital transmission the objective is to transmit a given symbol that is selected from some finite set of possibilities for example a value which could be 0 or 1.The task of receiver is to determine the input symbol with high probability.The cost advantages of digital transmission over analog transmission become apparent when trasmitting over a long distance.

5 LOCAL PORT

We're in the case we're interested to access to a page which is visible from a country for example Italy but not into an another country for example in Germany. This happened because there's a running server with restriction regional. Now defining an user with a username "user" and a password as "user" for pc2 and we start the ssh daemon. For access to that page we need to local port forwarding that let us to redirect all the traffic from port 80 of the server to the 9000 of the ssh tunnel from pc1 and pc2. in bash of pc1 we should write
$ ssh -NL 9000:remote_ip:80 user@ssh_server

6 REMOTE PORT

We're into a Lan and there's a gateway which blocks all the traffic to the port 80. Suppose there's running server with a Ip public for example (AmazonWebService) The Remote port forwarding let us to bypass the firewall of the gateway. If we try to access pc using links from s1 and s2, we do not get anything! Lets first create an "user" with password "user" on s2 and start the ssh daemon.The remote port let us to direct all the traffic direct to 9000 on s2 to the port 80 using a tunnel from pc to s2.

in bash of pc1 we should write

$ ssh -NR 9000:local_ip:80 user@ssh_server

7 SSH

The first protocol for remotely connecting to a network node is telnet which now has been deprecated for security reason. SSH runs over TCP protocol on port 22. SSH (Secure SHell) is a client-server protocol that allows remote managing over a secured pipe.It guarantees security features as authentication, encryption and integrity. After two initial handshakes both parties communicate the version of ssh that they support and encryption algorithms supported and then choose the first one that have in common for both topic.Now the server sends to the client its public key and then the client try to authenticate itself using two approachs: username and password or asymmetric cryptography. In the first case the client sends its username and password to the server and, if correct, the SSH session starts. In the second case, the server sends an encrypted message with the public key of the client, through the chosen algorithm, then, the client decrypt it with its private key and send it back to the server encrypting it with the public key of the server.

8 DESCRIVERE IPTABLES AND AN EXAMPLE ROUTING

Routers are processors telecommunications which using routing tables are able to find out the best path for reach the destination of considered packet. Each router is composed by a different number of interface and for each of them we 've an IP address, we should resume that an ip coul be or IPv4(32 bits) or IPv6(128 bits).An IP address could be represent as binary or decimal form. Each router when the packet arrives and read the destination address in the header's packet and looking into the Routing Table decide which is the next hop (another router or the final node)then it's the translation with ARP protocol to the IP to MAC address and send the packet on right interface or to the next hop . The routing table is populated in different way according if we used dynamic or static routing.Each entry of the routing table is composed by Network Destination so IP, Netmask, Gateway, Interface, Metric. For creating the routing table first I should analyze the list of all ip address in the topology,then determine the network type directly or remote connected, then define the routing tree to each IP network and for each element we should define the next hop.

9 DMT

The ADSL modulation could be done in two ways using CAP, that is one version of the QAM in which data are modulated using only one carrier frequency then transmitted over the telephone line; it's defined as Carrier-less because the transmitter does not transmit the carrier information or DMT which is the most used as ADSL modulation. DMT is a multicarrier and the band is divided into sub-band called tones with a gap of 4,3KHz each other. Each sub-band has its own carrier frequency and the transmitted signal is at first split into more inputs through a device and then transmitted over each carrier. We have 256 (sub-channels) of 4,3kHz each with sub-band modulation which could be QAM64 if modulated for clean sub-bands while it is QPSK modulated for noise lines. The carriers can independently transmit data in each sub-channel through a specific QAM modulation. In case there are external interference we reach 249 subchannel in downstream and 25 in upstream. Each sub-channel produces different attenuation on frequencies but we would like an ideal flat channel in which the attenuation is the same but in real world this mean that the probability of the event that each subchannel attenuate at the same way is very low . The attenuation depends on the SNR in the sub-channel analyzed and for evaluate it we use the WATERFILL ALGORITHM,which adapts QAM modulation to the telephone link. Each QAM modulation is chosen according the SNR in the channel take in consideration. The idea is to imagine the frequency band as a swimming pool; the power of the signal for each sub-carrier is determined by the depth of that pool

10 MOBILITY

The concept of Mobility is an important feature born with the evolution of cellular infrastructure. Every technology are different from two dimensions:bitrate and mobility which could be(Fixed,Fast and Slow). In fact we start with

1G when we transmit only voice than with from 1 to 2G there' s the improvement of the datarate. In the 2G there's an high mobility coverage but low bitrate so in 3G we're able to transmit digital data with an higher bitrate. Fixed mobility means the user don't change the access point so the cell instead in the other two way of mobilities the user change in different velocity the access point (example a men into vehicle-fast or walking-low). Wifi is an example of Fixed mobility in fact the access point is always the same and in this case the access point is provided by the modem in other ways the access points are provided by the base stations. There're two methodologies for assigning that to a device: passive or active scanning. The multiple access problem is solved by Base Station. Each cell is cover by a base station and themselves are interconnected with a wired connection or the most used the wireless with the require of the two antennas for the transmitter and receiver. A collection of base station is managed by a BSC and a collection of BSC is managed by the MSC the element that control the mobility. It let us to resolve the handoff problem, which is the problem whose the connection should be maintain alive during the passage between a cell to next where the user belongs. When the user is across the boundary of the cells the respective BSS, that cover the cell where it belongs, advertises the MSC that make a request to the next BSS to prepare from domain the resources for allowing the switch cell. When it's ready there's the switch and when it's happened the previous BSS where the user belongs, deallocates resources.

11 DATA,CONTROL PLANE AND SIGNALING(SS7)

With the passing of time the control information exchanged through the network was getting higher and higher, so it was decide to split the network into the Data Network and Signaling Network DATA PLANE refers all functions and routines to forward packets from an interface to another one. In practice packet of users. CONTROL PLANE refers all function that determine which path to use. A switching system has a switch and a switch controller • Switch controller is in the control plane and with other switch controller is linked by their CCIS network-remember also that Messages on CCIS conform to(SS7):
– does not touch voice samples
• Manages the network
– call routing and forwarding
– alarms (ring bell at receiver)
SS7, which stands for Signaling System 7, is a Control Network, physically separated by the Data Network, and SS7 controls the Data Network.Signaling Network is a packet based network, and in particular it has been the first packet-based network, that controlled the telephone data network, then the IP network was invented.SS7 network had its network components, which were SSP, STP, SCP, so we can see these components as the routers of the old telephone network. Nowadays SS7 implements different protocols that are useful for active a call or close it or managing messages as SMS, and also the number translation.

12 Talk about solutions to use optical fiber in the access network

The light can be amplified in a simple and cheap way using a device called the passive optical splitter. They take this name for the capability of split the light in multiple directions. Combining more splitters together we can obtain a sort of router or demultiplexer. However, we need to remember that each time the split signal is reduces itself of 10 * log(0, 5) = 3dB. If the fibers are fused in a good manner, the performance drop due to this loss are still acceptable. We could use three different configurations the first the most expensive for each user there's a fiber optic line fro user to the c.o. This is called P2P and it's to much expensive so we prefer using the others:1) splitter called PON that is able to split the light into multiple directions, this is the best solution from cost point of view but the signal is attenuated, otherwise we could use an active device called AON that is able to regenerate the signal but the cost is higher than previous one.We could have two kind of modulate the bandwidth resource according TDMA or WDMA. TDMA is prefer in usability and for standard. In downstream we've a point to multiport configuration and the traffic is scheduled in time slots. Each slot carries information about one ONU. The OLT plans the association of timeslots depending on the traffic condition, here could be a privacy problem if there's a malicious user which treats his OLT for spying information.In upstream we've a multiport to point configuration here ONU transmits its own piece of information in a precise time slot. The slots transmitted from the ONUs are then merged in the splitter in a way not to make them to collide. The ONU will be synchronized with the splitter in addiction we could have a problem related on distance from ONUs to to the splitter which couldn't be the same so the OLT sends a request packet and receives a response packet for performing power to use in transmission) this is a method for controlling the gain between two ONUs.The PON is quite used in the following two technologies:
• (EPON): the lowest level level is based on fiber optics transmission while the above one is based on Ethernet.
(GPON): in this scenario we can also use technologies based on more recent technologies than Ethernet.

13 SDN

SDN network makes a a clear separation from data plane and control plane. We can consider three different level a data plane composed by a set of switches that makes "match-action" routines in their flows table, instead control plane is a software composed by a logical centralized server which could be phisically separated or named as controller that is the medium for each communications and a collection of software applications that managed checked . The controller is reached by a switch through the protocol OPENFLOW that is based on TCP on port 6653. We could have according to the actors the following operations: READ/MODIFY STATE, CONFIGURATION, SEND PACKET, PACKET IN, FLOW REMOVED. These routines took the name of API southbound instead the others which let to connect the controller with a particular application are developped typically with REST, or more in general they're called northbound. Important feature is the fact that Dijkstra is run into an external application to the switch and the switch exchange update only with the controller on their links and not each other.

14 DIFFERENCE BETWEEN DYNAMIC AND STATIC ROUTING

Each router has its own routing table that is populated according two type of routing: Static or Dynamic. Static means that every entry is manually-configurated by the network administrator. The other one select the optimal path according to real time logical network change. In practice there's a routing protocol that is responsible for the creation maintenance and updating of routing table. Instead the static routing make these routines manually through an administrator. The dynamic routing require additional resource in terms of pc and ram and it's more complex to initially implement in comparison with static routing. Dynamic routing is generally independent of the network size instead the static routing increases complexity configuration as the network grows. If a link fails, a static route cannot reroute traffic and we need the intervent of the network administrator. Static routing is very secure and very predictable instead the dynamic is not. Problems of the static routing: scalability issues, reliability issues and heterogeneity issues, because the network administrator should always analyze if there's some link fail, then he should have knowledge of different OSs system of different routers.

15 Advantages and disadvantages of directed and undirected routing

Each user is associated with 2 kind of IP(permanent IP address that identify my static identity) and core of Ip address(the ip whih is given to me by the network where I am). The following Ip manages the mobility of users and it's became a standard. Now we introduce two device: an Home agent that is the MSC of the network where I typically stay and we can call it as Home Network,which hold my permanent ID into HLR(similar to a database of permanent ip) and the other device which we can call Foreign agent, it's the Home agent of the network where I am currently and called Visited Network. It holds my Core of Ip address. Now we can say that a direct routing have the problem when an user is moved to a Visited Network to another one and so maintaining the connection because change the Foreign Agent instead the indirect routing spread too much resource in case we're in the same network. Direct network is when A user asks to Home Agent's B where it's (it's the case when B is not in the same and Home Agent's B responds to the request giving the core of Ip Agent. Now I'm able to contact using core of Ip address the user B and the session start after the handshake (request to Foreign agent's B which responses to A) starts the session. The problem of it is that if B changes the Visited Network the session could fall. Indirect routing is when A user wants to speak with B and both are in different Visited Network. A sent the packet to Home Agent's B to discover the core of Ip address. Now will be the home agent's B that will contact the Foreign Agent's B and as a triangle communications the will be the Foreign Agent's B that will contact itself A modelling as Triangle routing. This procedure has as drawback is in the case they 're in some visitor network because is quite inefficient, but as main advantage is the transparency. Actually the problem of direct routing is supported using anchor agent. So when we moved to another visited network the session will not fall because the old Foreign agent will be the anchor agent , devise responsible to managed the connection with the new Foreign agent. The anchor agent create a channel with the new Foreign agent and the packets of the transmission forward on that channel.

16 5G

In the last years there were been a growing of the mobile traffic and an exponential number of users. The capacity of the last technology(LTE) is not more sufficient for supporting these capacities and this low datarate. It's also important the fat that the new technologies challenges are IOT or IOV or D2D are not possible to develop into a system as LTE with this low datarate. The capacity in wirless depends on bandwidth and spectrum efficiency[300Mhz to 3GHz].5G wirless network use an high mm-wave band which let to support hundred of times of more datarate. Requirements of these new technologies are:1) improved experience costumer with a datarate that is increased in terms of (1-10Gbps),2)99,999 % of perceived availability, 3)1ms round trip latency,4)high bandwidth in unit area,

5) enormous number of connected device 6)almost 100% coverage for anywhere connectivity 7) high battery life 8) reduction in energy usage by almost 90%. The first development in 2019 in which we all preliminary 5G pilots in the area for each member state. In 2020 5g launch in at least a big city of the member of the state. In 2025 5g development in the main urban areas and in the main transport line. User in this technology are not more the end of the network but it participates in storage,relaying content delivery and computation. We reduce the amount of size cell to 100-200 metres. The following infrastructure use an adaptive beam forming with beam directional antennas in SDMA guarantees good performance also because let the communication with mm-wave.In the following infrastructure we also a MAxime Mimo so the idea is to increase the number of antennas in each cell for increasing datarate. In the following infrastructure we've also cloud computing based to radio access shared pool of configuration resource. This technology let us to have a faster connection speed, environment transport logistic monitoring and smart energy network.

17 In the computation of the capacity that a channel can provide both the effect of the bandwidth and of the SNR are present, discuss how these have an impact and how they can be managed to improve the channel capacity.

We can define Channel capacity as the maximum datarate at which data can be transmitted over such condition. (Datarate- rate data transmitted in terms(bps)) About the channel capacity we've two different formulas:Nyquist bandwidth
C=2Blog(M)(in base 2) that put in relationship C,B and M respectly (Capacity,bandwidth,voltage level) SNR=10log(signal power/noise power) in base 10) If it's an high value means that we have a need of low number of repeaters. This is a value given in db so the next formulas is EQuation of shannon= C=Blog(1+SNR)(in base 2)
In case $B_s > B_c$ means that there's interference. It's also important the concept of Multiplexing that let us to into a channel sent more than one signal at the same time otherwise we waste resource and we want avoid it.

18 DIFFERENCE BETWEEN PRE-DSL AND ADSL

This technology was devised to provide digital data transmission over telephone infrastructure made of twisted pairs with a bandwidth 0-4khz.Then sine the data transmitted and voice services used same bandwidth the cost for one of this service is the same.Now we introduce an analog modem that let us to split the the two services from logical point of view.This issue limits the datarate to 56kbps. Modem is used for adapting data through twisted pair, this happened because digit should be transported in the correct way. Twisted pair are not shield as copper wire this means that they're affected by interference in cable.Longer is the cable higher is the attenuation.Using the modem we're able to split the bandwidth.Higher for the voice transmission lower for data transmission. It tried to use 2 or 4 twisted pair in order to increase the data rate: this caused a bigger cost due to the use of more wires. It was not possible to transmit both data and voice at the same time and the upstream and downstream were using the same bandwidth. ADSL born with the idea of demand video and streaming TV purpose. In practice it's used for the following services:
– Transparent access to legacy voice service – High-speed digital service
• Voice service
– POTS splitters used in home shunt the frequencies below 3400Hz to POTS wiring
– Frequencies above the voice band are for high-speed data service to get to the ATU-R
It's also important tu recognize that in the adsl we put a DSLAM and that is a multiplexer used for multiplexing the ATU-C which is directly connected with the ATU-R. ATU-R is contained into the modem of the user instead the others two devices are inside the c.o. .It's important how is divided the band spetrum so the first part is the voice with a full duplex link because we would like to have a bidirectional service, instead for the data transmission we consider the two range divided as upstream and downstream. The last update version of ADSL consider thw two bandwidths into different range because is higher the probability to require a file than upload a page or file.This means that the upstream is less than downstream. For increase performance we can overlap the two bandwidths considering so a unique channel but in this we could have a problem which could be resolved by echo cancellation.

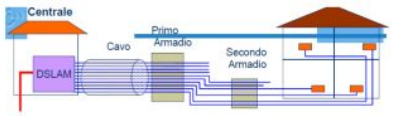
19 subnetting e supernetting

To determine the subnets, detach each interface from its host or router, creating islands of isolated networks and each of them are called subnet. For doing it we can split in steps:
1)Determine the class of the block of IP addresses.
2)Determine the number of subnetworks you need.

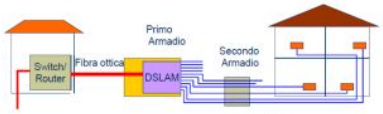
3) Determine the number of hosts for each subnetwork.
With subnetting we've two problems: There is a waste of IP addresses and that Given an IP adddress with a certain netmask, we can't assign all IP addresses to all hosts with given bits of the HOST_ID. We can resolve using: 1. VLSM 2. Supernetting

20 FTTX

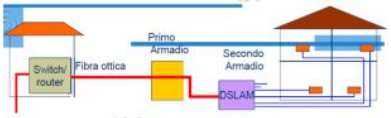
The name of the differents configurations is determined from where the *EOI (Electro-Optical Interface)* is placed.
The current architecture is the **Fiber To The Exchange (FTTE)**. The EOI (DSLAM) is placed in the same place of the CO. From the CO to the user we only have copper.



Fiber To The Cabinet. The DSLAM is in the cabinet.

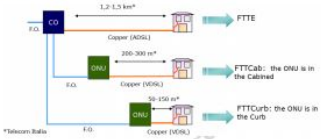


Fiber To The Curb. The DSLAM s in the external distribution box (second cabinet).



Fiber To The Building. The DSLAM is in the internal distribution box till the building.

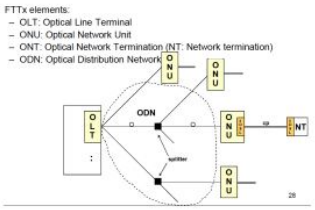
- **FTTE**: the optical fiber terminates to the Central Office (CO) and the CO is co via a copper based line (e.g., ADSL)



- **FTTP/FTTB/FTTH**: the fiber cables arrive to the users' premises

4.9.1 FTTx: Reference Architecture

Below, we have the basic architecture for the Optical Access network.



21 VPN

A private network is able to connect users that share information each other. The line between a private(LAN) and public network (WAN)has always been drawn at the gateway router, where deliver security routines as a firewall to keep intruders from the public network out of their private network. A private network guarantees security feature as a VPNs allow to create a secure, private network over a public network and it creates a secure link between peers. This is achieved through encryption, authentication, packet tunnelling and firewalls. The encryption on a VPN can be done from gateway to gateway or from end to end. Under Linux it's implemented as OpenVPN that requires:
a certificate (public key) and private key for the client and the server
- a master Certificate Authority (CA) certificate and key to sign the server and client certificate It supports bidirectional authentication

22 Usage of Link State Packets in OSPF and cost estimation

Internal Gateway protocols are RIP and OSPF and others.From these we analyze OSPF because most used and faster .OSPF is managed by the Link State Protocols, in which every link state packets is sent by each node to neighbours with the main goal of knowledge of the entire network topology. Link State Packets are sent made flooding and they contain information about the link (so metrics and state) to which the node is connected to. Every router constructs the network topology from the LSP received and, with the Dijkstra algorithm, builds the Shortest Path in terms of metrics for every single host. This will be the router's routing table. In Linux, OSPF Is included in a suite called quagga and the daemon which implements it is called zebra. OSPF is implemented with the division of the areas that let us to divide routers in logical way: The area 0.0.0.0 is called the backbone area. We can identify 3 kind of routers:
• Internal Router; all interfaces belong to the same area
• Area Border Router; connects one or more area to the backbone
• Backbone router; has at least one interface on the backbone

23 DESCRIVERE BANDA DI ADSL

Larger the bandwidth the higher is the data rate. However, we can reach the same goal by reducing the signal- to-noise ratio which depends on the distance from the signal's source. The first idea was to use a larger bandwidth w.r.t. the one used for voice traffic: from 4 KHz to 1 MHz.Voice traffic is separated from the data. ADSL has two different frequency bands: one is used for upstream, from the user to the CO while the other for downstream from the CO to the user. The two bands are obtained through FDM. The so called guard bands are used to divide the different bands among each other so that to reduce as much as possible, interference between signals.With ADSL they decided to transmit the voice in the 4 KHz while using higher frequencies for data. The larger is the bandwidth, the higher is the data rate while, for the upstream, the data rate is lower. On the other hand, for voice traffic, we have a bandwidth which is shared both for upstream and downstream (full duplex).

24 local loop

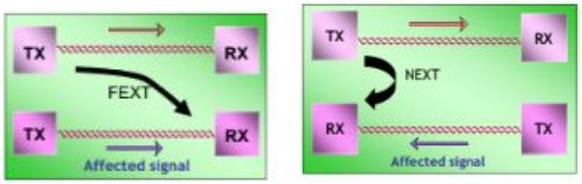
it's the phisical link which connect from the demarcation point of the costumer premises to the edge of the carrier network. In practice is a wireline from end user to the c.o. composed by electical circuit as a single twisted pair in support of voice. Local Loop connections include Electrical local loop, Optical local loop,Cable local loop, Wirless l.l. Satellite l.l. In modern implementation may include a digital loop transmission system or fiber optic transmission system.It' used to provide some service, including DSL,ISDN for carrying digital signal directly to an higher bandwidth than they used only for the voice.

25 NETFILTER

Netfilter is a Linux framework that provides hook handling used for intercepting and manipulating network packets. A hook is an entry point within the networking subsystem. Packets traversing the IP stack are intercepted by these hooks, verified through a set of rules and processed it according an action before set by the user.Packets pass through a sequence of tables (queues), each one dedicated to a specific packet activity and is controlled by a chain. 4 built-in tables: Filter, Nat, Mangle, Raw. Typical rules are on: source/destination address or network, interface, source/destination port. Typical actions are: accept, drop, masquerade, dnat, snat, log. Within netfilter, packets can be related to tracked connection which can be labelled as new, established, related and invalid. The command iptables is used to configure the netfilter tables adding or removing rules. A chain is a list of rules which can match a set of packets and each rule specifies what to do with a packet that matches, these are called targets.

26 Describe the two type of cross-talk and how to solve them

A binder group is affected by the cross-talk noise. There are interference between cables that share the same binder group. In the same binder group, two cables can interfere with each other if they are transmitting on the same frequency band. Therefore, the quality of ADSL transmission depends on the distance, on the quality of the cable and also on other characteristics. This problem was already present in telephone network: this was managed by the central office using an electric device. However, this is still a problem in the ADSL. Considering the cross-talk noise, we've two types:
• FEXT signal crosses all the channel is the cross-talk between transmitters at the same side and a receivers at the same opposite side of the cable; the lower receiver obtain an overlapping of the two signals affected signal and the FEXT. According to the length of the cable there's the interference high or low.
• NEXT signal is the cross-talk between a transmitter and a receiver placed on the same side of the cable. The signal is powerful how much for an high interference since it arrives from a small distance and the quality of received data is poor.



Crosstalk increases if it's increase also the frequency and also if the distance decrease reason we will have that Next crosstalk is more dangerous. A way for solving these problems could be:

- split the bandwidth of upstream and downstream without any union of the bands

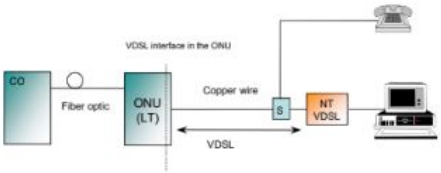
- we use echo cancellation event in which if A and B transmit at the same time, B is able to obtain the information because knowing what he transmit it's able to remove from the signal received that flow value.
- reduce the number of cables into a binder group.

27 TRACEROUTE

The following command let us to test connection between two hosts traceroute a.b.c.d
This command exploit that every packet has a TimeToLive field which is an integer value when the packet leaves the NIC of the sender so the host from which we all this routine. Every hop meets decrease by one the integer field TTL but when we're in the constraint TTL= 0, the host in which is stopped sends back to the sender an ICMP error packet. The packet contains the IP address of the host who expired the TTL.In the next iteration the sender increase to 1 the starting TTL field value .We continue the iterations until I reach destination otherwise return NEtwork unreachble.In the first iteration we consider TTL=1.

28 VDSL AND VECTORIZING

It's the an upgrade of ADSL in which we pass the DSLAM and the ATU-C from the C.O. to the cabinet .It's able to use the band until 12 MHz and it's able to support a datarate of 50Mbit/s in downstream and 6,5 Mbit in upstream in case the bandwidth is splitted otherwise it reachs 25 Mbit/s. The main goal is to increase the datarate reducing the amount of the copperwire with a dimension from 300 to 1500 m and with an increasing amount of the fiber optic. In this way the bandwidth of the transmission is increased and so we increase the probability of the cross-talk event. For avoiding it we should synchronized all the transmitted signals and evaluate an anti-signal value. It's the concept of vectorizing. It let us to remove the effect of the cross-talk because it's transmitted with the signals also the anti-signal. When vectoring is not applied the number of interference signals increase and the distance with DSLAM increase, performance decrease in terms of datarate . When the datarate is similar to ideal performance possible is when it's applied the vectoring.



29 DNS

DNS system is created for (load balancing, decoupling with address name and address ip), guarantees reliability and avoid name collision. DNS service could be done through a distributed database, composed by server. DNS structure is composed by a large inverted tree divided in domains.Each node is a label without dot. Each domain space is a path in the tree. A zone is managed by the upper zone through NS record.Each zone is running in more server, for redundancy reason.The different server use a master-slave pattern which a master server that answer to the query and send updates to other slave servers using exchange SOA message , because it's important that each server contains same information. Browser can use two methods to invoke name resolution :gethostbyname & gethostbyid