Questions NI

Automatically updated every 5 minutes

Legend

x) Question closed/answered well
y) Question not answered
z) Question not secure about

Question to do (I strongly encourage you to add/adjust these missing answers) :

Cuomo

- A1 - Describe the two types of cross-talk noise in ADSL and how to solve them
- A2 - Differences in topology and technology of Access, Core and Edge network
- A3 - Talk about solutions to use optical fiber in the access network
- A4 - Advantages and disadvantages of directed and undirected routing
- A5 - Noise in digital transmissions and resolution
- A6 - DMT (Discrete multi tone) modulation
- A7 - How copper wires changes from analog to digital
- A8 - How the frequency band is used in ADSL and how this is reflected in the ADSL architecture (Frequency division, upstream downstream, voice)
- A9 - What are the key differences of using the old copper wire to provide data (analog voice band modem) and the digital one
- A10 - 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. (= RELAZIONE TRA Bs e Bc e rapporto tra Bs e bitrate) (*seems the same of A1)*
- A11 - Mobility
- A12 - Fiber technology FTTx
- A13 - Differences pre DSL and ADSL
- A14* - subnetting e supernetting
- A15* - local loop

Spaziani

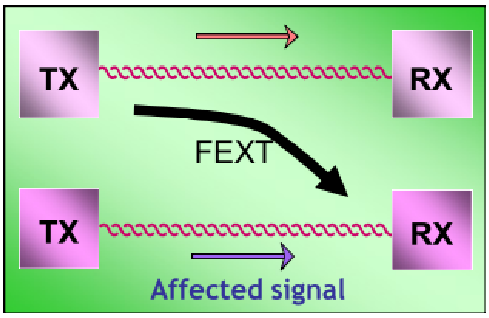
- B1 - Describe public and private key roles in ssh authentication with an example
- B2 - What is netfilter and how it is used to implement firewalls
- B3 - Usage of Link State Packets in OSPF and cost estimation
- B4 - Remote and local port forwarding
- B5 - SSH
- B6 - Describe with an example how tracert (Traceroute) can discover the path taken from a packet directed to a specific destination
- B7 - Advantages and disadvantages of ip static and dynamic routing
- B8 - What are the fields of an ip routing table and how they are used to route a packet to the destination ? Make an example.
- B9 - VPNs
- B10 - describe all the fields of Iptables and an example

Extra

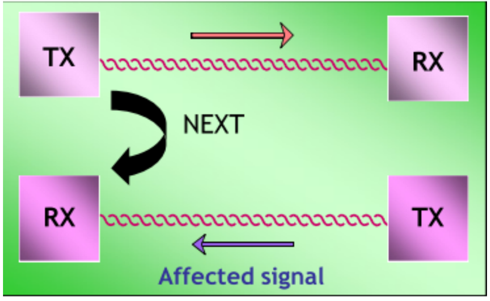
- **E1 - SDN Mobile**

In general, when two or more wires are bounded together they interfere each other producing noise.

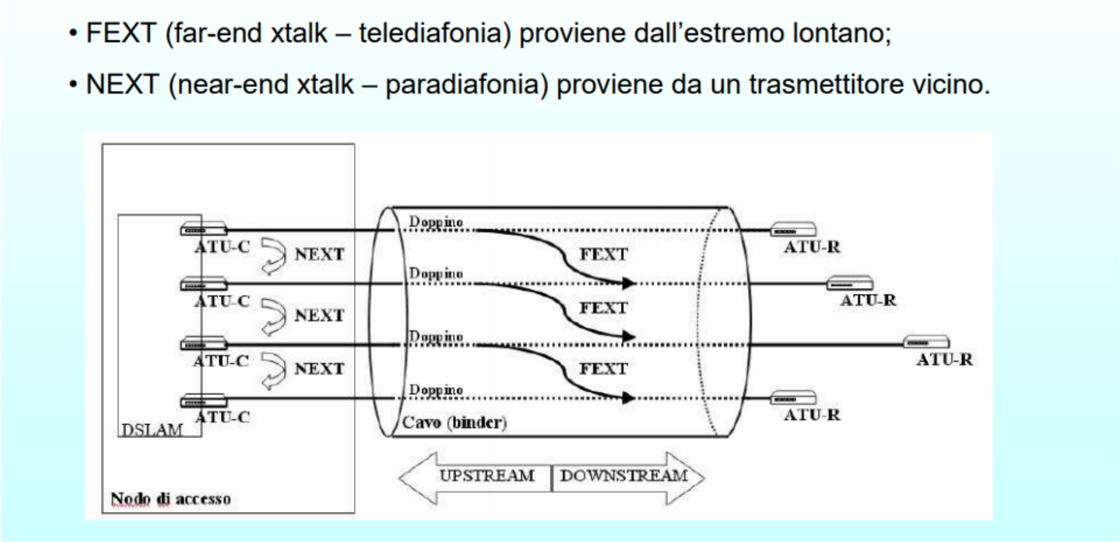
1. **FEXT : far-end cross talk** is the kind of noise generated when a transmitter and a receiver are placed in the opposite sides of the cable. In particular, in ADSL systems the wires are not so long so the signal is not attenuated. This cause an interference because if a wires transmits data near an active receiver (means that is receiving), the signals will interfere each others.



1. **NEXT: near-end cross talk** is the cross-talk between a transmitter and a receiver placed on the same side of the cable. It consists in: I receive my signal but it is affected by the transmission of another user. NEXT is one of the reason of the frequency division for upstream and downstream in ADSL.



Crosstalk typically increases with frequency, so **this is an important drawback of the adsl, in special case the HDSL (High Data Rate DSL).** With the ADSL2+ these problems are managed better then the previous ADSL standards. To reduce this kind of noise a cable usually doesn't contain more than a dozen twisted pairs.



- FEXT (far-end xtalk – telediafonia) proviene dall'estremo lontano;
- NEXT (near-end xtalk – paradiafonia) proviene da un trasmettitore vicino.

Example

A solution for this problem is differentiate the different bandwidths. This is done by some network elements, called **splitter,** they split out a frequency band with respect to another. They are able to to filter out the telephone bandwidth from the bandwidth of the ADSL; filter out the cell

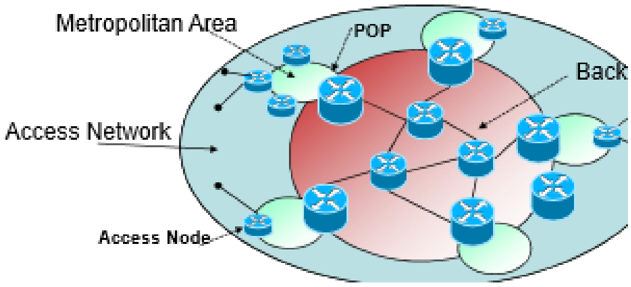
- or DSL signal is "filtered off" at each phone by use of a low pass filter, also known as microfilter.

05_XDSL_Family.pdf

A2 - Differences in topology and technology of Access, Core and Edge network

Access network

- Part of a communications network which connects subscribers to their immediate service provider.
- We have some subnetwork named metropolitan area networks.
- Need to be very capillary towards the user. Need to find the way to reach all users.
- In Italy a big part is build up using **copper lines**. First used only for voice signal, then for Digital Subscriber Line technology, meaning that the initial part of the network is digitally implemented. Today we use optical fibers in access network.



- Star topology. It is natural to have a star. We have the end users that are connected to the network, so we think about them as leafs in a three. We can say that in the access part stars are the best topological structure to interconnect devices.

Core Network

- Is a *backbone* network
- Different devices like switches and routers
- Topology of fully mesh network: all nodes belonging to that part are connected together one to the others. These nodes are reconfigurable but more they have capacity to reroute the traffic. As a principle, if you reconfigure a ring, where do you root the traffic? In a fully mesh you have more options. This is the reason why in a mesh is much more robust, in case it needs much more redundant capacity.

Edge of the network

- Can perform intelligent functions that are not performed inside the core network
- Ring topology, meaning that you have a single media, for instance the most of the networks set up in metropolitan area also private networks, like Sapienza network. Is a network where there are a lot of routers, located in different parts. All of these are mainly interconnected not in a star topology but in a ring one. Also because rings are easy to be reconfigured. If one node fails, the ring can be reconfigured, it's much more robust to failures.
- the core network is considered relatively "dumb" while the edge is considered "smart" because the **path selection through the core is determined by the edge**

03_Network_Fucntional_Areas.pdf

A3 - Talk about solutions to use optical fiber in the access network

The are several kinds of solutions to take advantages from the optical fiber in the access network:

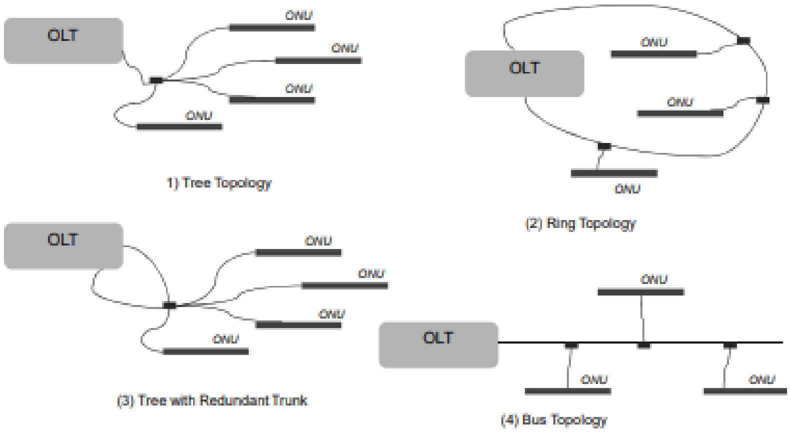
- Point2Point - P2P much expensive and not so used. per each why

A PON can be distinguished by the channel separation mechanism to fairly share bandwidth resources. It can be the time (**TDMA** time division multiple access) or the wavelength (**WDMA**). TDMA is the one standardized and used practically. It has very low-budget devices as **splitters** or lasers. It dynamically adapt the power to forward packet based on the distance of the various ONU's

PON works as follows:

- downstream: an Optical Line Terminal (OLT) schedules the traffic (if tdm the slot are time-based scheduled), then a passive splitter forwards the traffic to each ONU and user
- upstream: each user has a "window" to send its traffic to the OLT. In TDMA case this window is a time slot.

The configuration for OLT, splitters and ONU can be different. In an EPON (Ethernet-PON), where the packets are encapsulated in Ethernet frames, the topologies can be:



1) Tree Topology

(2) Ring Topology

(3) Tree with Redundant Trunk

(4) Bus Topology

Ring topologies are used a lot in the access network.
The advantage of using rings is that we can have the very last past of the network (buildings, cabinets) close to the home but not so close as the situation where the system ends.

In EPON (the Ethernet MAC protocol) cannot operate properly in the upstream channel (no collision detection) since each ONU cannot hear other ONU, so it has been developed a Multi-Point Control Protocol for this specific sublayer.

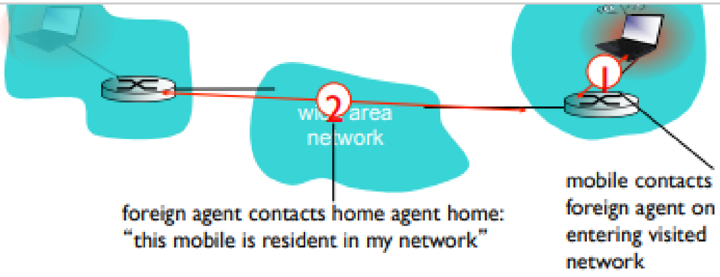
06_Passive_optical_networks.pdf

A4 - Advantages and disadvantages of directed and undirected routing

In LTE technology the are two types of approaches to afford mobility, both are handled by end-systems:

- Indirect Routing
- Direct Routing

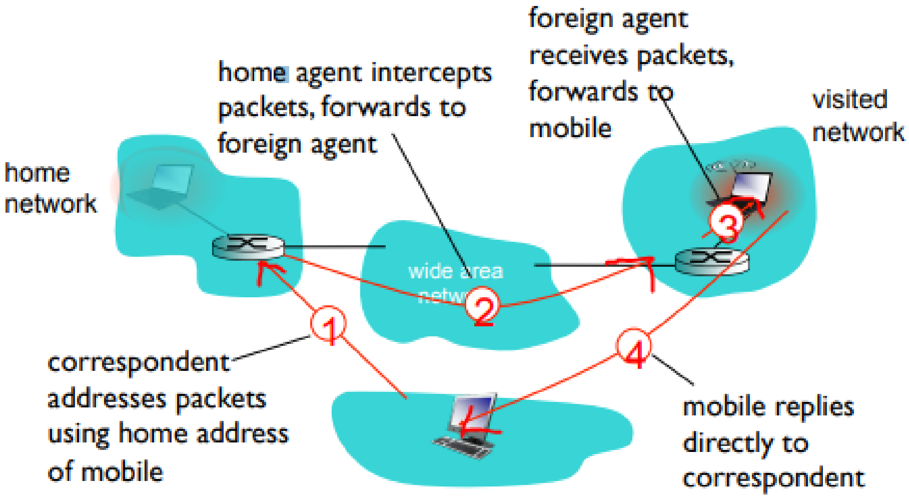
These are the only 2 options due to the fact that a routing table exchange approach is not scalable to million of mobiles equipments. Once the **registration** is done:


wide area network
2
1
foreign agent contacts home agent home: "this mobile is resident in my network"
mobile contacts foreign agent on entering visited network

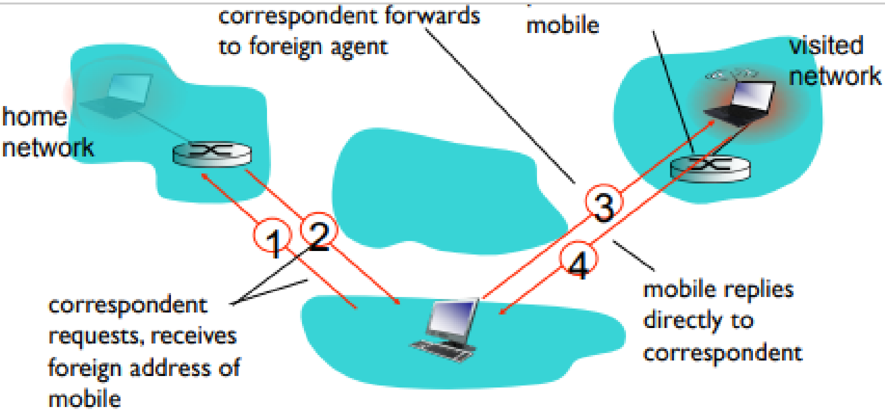
Indirect Routing:
A correspondent (the device who wants to communicate with the mobile device) sends packets to the home network router, it forwards the packets to the foreign agent. The foreign agent forwards it to the mobile equipment. It will replies directly to the correspondent because he knows in advance its "position". This is called indirect routing because the correspondent doesn't talk directly to the mobile, instead the foreign agent is in charge to forward the packets. The mobile has two kind of addresses:

- Permanent address - used by the correspondent
- Care-of-address - used by the home agent

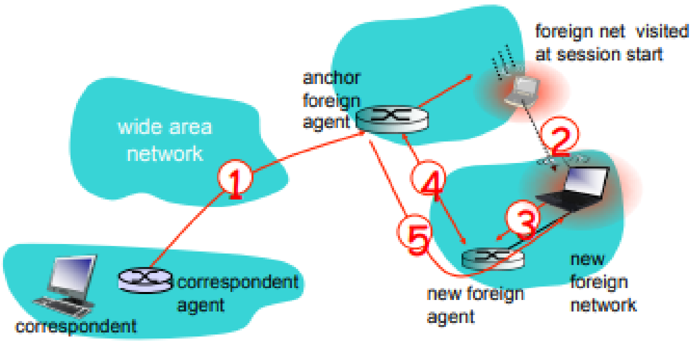
Of course this approach is inefficient when the mobile device and the correspondent are in the same network, because this triangulation is useless. Furthermore, if the mobile changes the network during the communication, the old foreign agent will register as home agent updating the addresses.


home agent intercepts packets, forwards to foreign agent
foreign agent receives packets, forwards to mobile
visited network
home network
wide area network
1
2
3
4
correspondent addresses packets using home address of mobile
mobile replies directly to correspondent

Direct Routing: This approach instead of using an home agent as support, the correspondent asks the foreign address to the home agent and once it get response, directly forwards the packets to the foreign agent.


correspondent forwards to foreign agent
mobile
visited network
home network
1
2
3
4
correspondent requests, receives foreign address of mobile
mobile replies directly to correspondent

In this case the triangulation problem is avoided and it very useful in case mobile and correspondent are in the same network, but some problems can occurs when the mobile changes the network during the communication. In this case we need to use a foreign agent as *anchor* deputy to forwards the packets to the new foreign network.



07_Infrastructures_LTE.pdf

A5 - Noise in digital transmissions and resolution

A channel capacity can be defined as the maximum rate that at which data can be sent through the communication channel. This capacity is limited by the physical structure of the channel and from the presence of noise inside it. due to this fact, the noise (in particular, its power) is the denominator for the SNR (signal-to-noise) ratio. It is useful to get an idea of the quality of the signal.

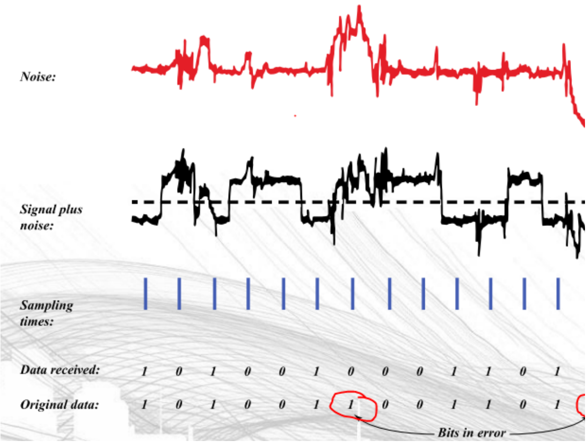
In particular the SNR is computed as follows:

This means that a high SNR ratio is synonymous of high quality of digital signal and as consequences the less installation of repeaters in-between the transmitter and the receiver. Conversely, a low SNR means poor quality of digital signal and the necessity to get repeaters between who transmits and who receives. SNR in general is an upper bound of the achievable data rate and in the Shannon formulation we have that

$$(SNR)_{\text{dB}} = 10\log_{10}\frac{\text{signal power}}{\text{noise power}}$$

$$C = B\log_2(1+S$$

is the capacity with a bandwidth B.


Noise:
Signal plus noise:
Sampling times:
Data received: 1 0 1 0 0 1 0 0 0 1 1 0 1
Original data: 1 0 1 0 0 1 1 0 0 1 1 0 1
Bits in error

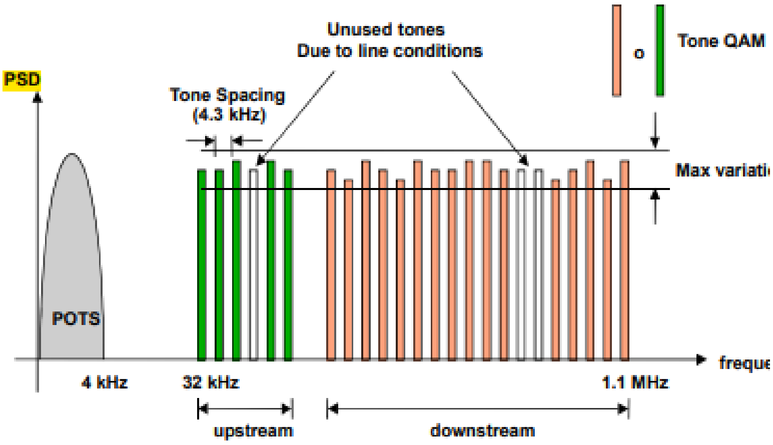
01_TransmissionFundamentals.pdf

A6 - DMT (Discrete multi tone) modulation

In an ADSL system the problem of signal modulation has two "competitors":
Carrier-less Amplitude/Phase (CAP) and **Discrete multi-tone** (DMT) modulations. While the first one is a QAM modulation of a single carrier suppressed before the transmission, the DMT divides the bandwidth in several sub-channels. Discrete carriers (or tones) are used in the center of each data subchannel, they are used to transmit data independently in each subcarrier through a specified QAM modulation.
A multi-carrier modulation is the following idea: Given a spectrum band we divide it in subportions, sub pieces, named **sub carriers.**
These are spaced by 4.3 kHz, it's a sort of frequency division multiplexing, every sub band is at a different frequency.
Some tones are not used at all because in the copper wires of telephone lines you have a rapid decreasing of the SNR. There is a frequency part in the copper wire not useable because of very bad condition.
DMT dynamically adapt the data rate based on the line condition.
Normally each subcarrier is modulated with QAM64, if a subcarrier as noise lines, i use QPSK.
We use as standards:

- Theoretical max upstream bandwidth: – 25 channels X 15 bit/s/Hz/channel X 4 KHz= 1.5 Mbit/s
- Theoretical max downstream bandwidth: – 249 channels X 15 bit/s/Hz/channel X 4 KHz= 14.9 Mbit/s

With respect to the CAP, the DMT doesn't uses adaptive equalizers even if it has peak of power in average.

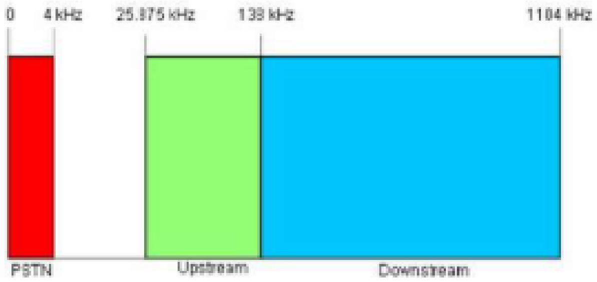


05_XDSL_Family.pdf

band centred in the upstream frequency carrier and another band as for the downstream. A first example of modulation was named carrier-less amplitude phase modulation **(CAP).** Then, **DMT** modulation became the standard due to the fact that is more robust to noise and doesn't requires equalizers.
ADSL uses two separate frequency bands, referred to as the upstream and downstream bands

- The **upstream** band is used for communication from the end user to the telephone central office
- The **downstream** band is used for communicating from the central office to the end user.

With standard ADSL, the band from 25.875 kHz to 138 kHz is used for upstream communication, while 138 kHz –1104 kHz is used for downstream communication



As you can see, the bandwidth is not equally divided between upstream and downstream. This is the reason of Asymmetric DSL (digital subscriber loop). For the voice is used the 0-4kHz band.

05_XDSL_Family.pdf

A9 - What are the key differences of using the old copper wire to provide data (analog voice band modem) and the digital

A voice band modem carries a max of 56 kb/s of digital data. This is because with that modem I perform a digital modulation, my bandwidth is 4 kHz. , if It was the first modem used to transmit emails, ftp etc.. It was very hard, it lasts some years, after a while obviously it was not enough. However the interest was to keep the infrastructure identical to the previous one. So with the ISDN and xDSL the idea was to keep the infrastructure identical to the previous one.

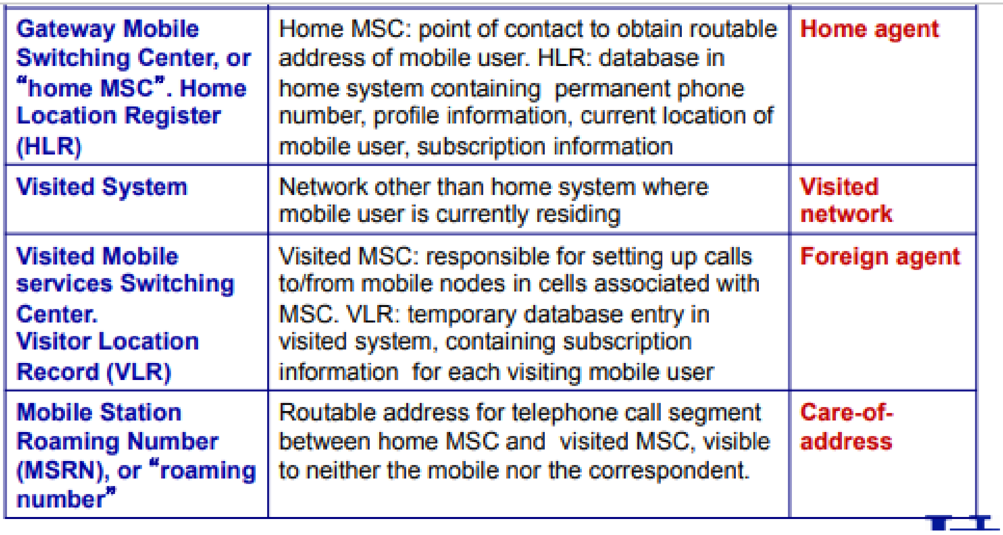
A10 - In the computation of the capacity that a channel can provide both the effetct of the bandwidth and of the SNR are present, discuss how these have an impcat and how they can be managed to imporve the cannel capacity. (= RELAZIONE TRA Bs e Bc e rapporto tra Bs e bitrate) (same as A5)

A11 - Mobility

Mobility in networking **means the possibility of a device to change the network's point of access during a communication**. This is a challenge that in LTE is managed very well. It's important to distinguish from wireless and mobility: a wireless connection can be stationary.

- A mobile wireless user using the same access point has not mobility.
- An example of mobility can be a connection of a car with a gps system : it passes through multiple access point while maintaining ongoing connections.

A key-point of the mobility is the routing: how can i forward packets if i know only the last known position and not the current one? I do with direct and indirect routing. (A4)
To manage the communication there are two technologies: GSM and



Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information	Home agent
Visited System	Network other than home system where mobile user is currently residing	Visited network
Visited Mobile services Switching Center. Visitor Location Record (VLR)	Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user	Foreign agent
Mobile Station Roaming Number (MSRN), or "roaming number"	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	Care-of-address

07_Infrastructures_LTE.pdf

A12 - Fiber technology FTTx

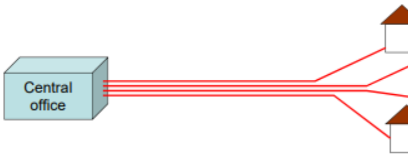
Due to the fact that the majority of users have a copper wired technology, the best current architecture is an installation of the fiber to the central office (CO). Here, a DSL Access Multiplexer has the task of carry connection to the building. But this is one of the worst solutions in terms of efficiency and of course speed connection. What is true is that in the backbone part we have fibers, then or the fiber ends to the central office and the rest goes with a copper based. At the central office there are **Optical line terminals (OLT)**, they provide the fiber toward the end users. There are a plethora of solutions.

Fiber-to-the-x:

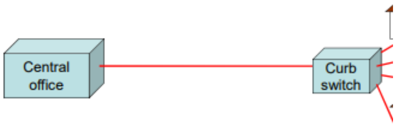
- **FTTH** - Home
- **FTTB** - Building (ending part of this fiber is in the basement of the building)
- **FTTC** - Curb/Cabinet (that are the places where the fiber ends)
- **FTTE, where E** stands for the **exchange** that is the central office, where the exchange in the past was done from a fiber that is always arriving at this central office.

There are 3 topologies for the CO-Building/User path:

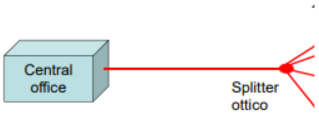
1. A direct connection for each unit, high cost for the digging.

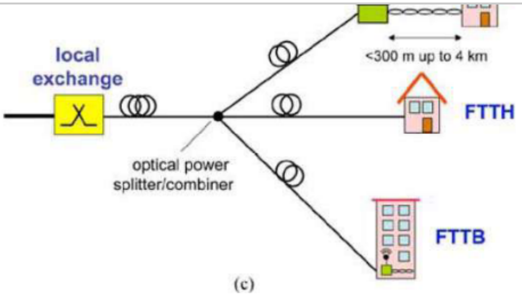


2. Using a curb that is deputy to switch the connection.



3. The usage of a passive optical splitter.





06_Passive_optical_networks.pdf

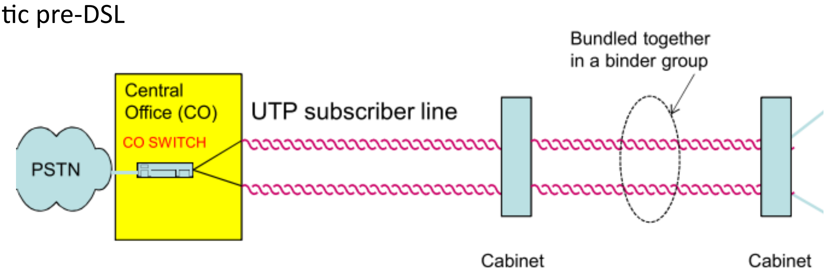
A13 - Differences pre DSL and ADSL

Pre-DSL

In the early 80s, the idea of a digital subscriber line to provide access to an integrated services digital network (ISDN) was initiated

- The initial throughput requirement was 160 kbit/s
- Investigate even higher transmission throughputs approaching T1 speeds
- The project was named High bit rate DSL (HDSL)

Wiring schematic pre-DSL



One of the biggest disadvantages of that technology was the massive cross-talk (NEXT and FEXT) due to the symmetric design.

ADSL

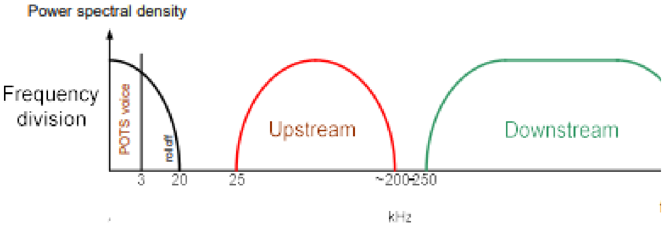
Original market driver: distribution of video on demand (VoD) (failed for this target)

• An ADSL local loop is for the exclusive use of the subscriber, with no contention for bandwidth on that local loop

• ADSL provides for passive transmission of analog voice service (instead, pre-DSL don’t)

• The volume of data flow is greater in one direction than the other (Downstream much bigger than Upstream)

• Providers usually market ADSL as a service for consumers to connect to the Internet in a relatively passive mode – able to use the higher speed direction for the "download" from the Internet but not needing to run servers that would require high speed in the other direction.



Even in ADSL the cross-talk is present, but it’s been reduced with respect to the old technologies.

A14* -subnetting e supernetting

A15* - Local loop

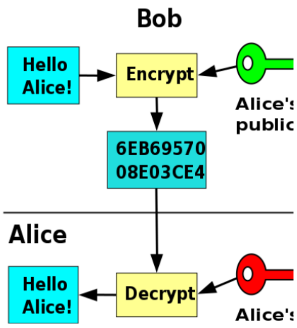
In telephony, the **local loop** (also referred to as a subscriber line) is the physical link or circuit, that connects **from** the demarcation point of the **customer premises to the edge of the carrier** or telecommunications

------------SPAZIANI------------

B1 - Describe public and private key roles in ssh authentication with an example

SSH keys are generated in pairs and stored in plain-text files, consist in two part:

- A private key named *id_rsa* stored on my computer. It is meant to remain secret.
- A public key, usually named *id_rsa.pub* that is placed on the server you intend to log in to. The public key is meant to be shared to everyone who want to use an encrypted language with you. The asymmetry is in the fact that the public key is used to encrypt data and the private key to decrypt them.



Upload the public key to the home directory of the user you would like to log in as --> add public key into a new line inside the user's *authorized_keys file.*

Server creates a challenge that only the owner of the private ssh key will be able to decrypt.

To generate a ssh key use the command ssh-keygen, the key pair is inside the .ssh directory.

B2 - what is netfilter and how it is used to implement firewalls

Netfilter is a framework that provides hook handling within the linux kernel for intercepting and manipulating network packets.

A hook is an entry point within the linux kernel IP networking subsystem that allows packet mangling operations. Packets are intercepted by these hooks, verified against a given set of matching rules and processed as described by an action configured by the user.

Packets can be related to tracked connections in four different so called states: New, Established, Related, Invalid.

Iptables is the frontend of NETFILTER, used to add/remove rules to a chain (mapping of NETFILTER hooks) within a table. Ex: iptables <command> <chain> <table> <match> <target>

Several different tables may be defined. A firewall rule specifies criteria for a packet and a target. If the packet does not match, the next rule in the chain is then examined

If the packet does match then the next rule is specified by the value of the target (option -j): ACCEPT DROP QUEUE RETURN.

Filter is the default table it cointes the built-in chains. INPUT(for packets destined to local sockets), FORWARD(for packets being routed through the box), and OUTPUT(for locally-generated packets).

The following parameters make up a match specification:

- Protocol
- Source address
- Destination address
- Input interface name
- Output interface
- fragment

Ex: iptables -A FORWARD -i eth2 -p tcp --dport 22 -j ACCEPT make it work properly. OSPF falls in the category of the Interior Gateway Protocols, in particular in the sub-category of the Link State Protocols, meaning that every node in the network must know the entire network topology.

OSPF works as follows:

1. Every router advertise its presence to neighbors routers and ”floods” the network with particular messages (**Link State Packets**, LSP) which contains information about the link to which the node is connected to.
2. Every router constructs the network topology a graph) from the LSP received
3. Every router, with the Dijkstra algorithm, builds the ”best path” for every single host.

This will be the router’s routing table

OSPF daemon allows us to specify **cost** for each physical link on a router. The cost is a number greater than zero that has no physical meaning, it’s just relative to the other links cost: a path with a lower cost respect to another will win the race and become part of a router’s routing table.

06_OSPF.pdf

B4 - Remote e local port forwarding

SSH connections can be used to tunnel traffic from ports on the local host to ports on a remote host.

Local

A local connection is a way of accessing a network location from your local computer through your remote host.

First, an SSH connection is established to your remote host. On the remote server, a connection is made to an external (or internal) network address provided by the user and traffic to this location is tunneled to your local computer on a specified port.

This is often used to tunnel to a less restricted networking environment by bypassing a firewall. Another common use is to access a “localhost-only” web interface from a remote location.

To establish a **local tunnel** to your remote server, you need to use the -L parameter when connecting and you must supply three pieces of additional information:

- The local port where you wish to access the tunneled connection.
- The host that you want your remote host to connect to.
- The port that you want your remote host to connect on.

For instance, to connect to example.com on port 80 on your remote host, making the connection available on your local machine on port 8888, you could type:

```
ssh -N -L 8888:example.com:80 username@remote_host
```

Now, if you point your local web browser to 127.0.0.1:8888, you should see whatever content is at example.com on port 80.

A more general guide to the syntax is:

ssh -L *your_port*:*site_or_IP_to_access*:*site_port username@host*

Remote

In a remote tunnel, a connection is made to a remote host. During the creation of the tunnel, a remote port is specified. This port, on the remote host, will then be tunneled to a host and port combination that is connected to from the local computer. This will allow the remote computer to access a host through your local computer.

This can be useful if you need to allow access to an internal network that is locked down to external connections. If the firewall allows connections out of the network, this will allow you to connect out to a remote machine and tunnel traffic from that machine to a location on the internal network.

To establish a remote tunnel to your remote server, you need to use the -R parameter when connecting and you must supply three pieces of additional information:

background before executing and the -N flag, which does not open a shell or execute a program on the remote side.
For instance, to connect to example.com on port 80 on our local computer, making the connection available on our remote host on port 8888, you could type:

```
ssh -f -N -R 8888:example.com:80 username@remote_host
```

Now, on the remote host, opening a web browser to 127.0.0.1:8888 would allow you to see whatever content is at example.com on port 80.
A more general guide to the syntax is:

```
ssh -R remote_port:site_or_IP_to_access:site_port username@host
```

B5 - SSH

SSH is a protocol that allows remote managing over a secured *pipe*. It is a client-server protocol.
Generally, SSH is used to securely acquire and use a remote terminal session. The main features that SSH provides are:

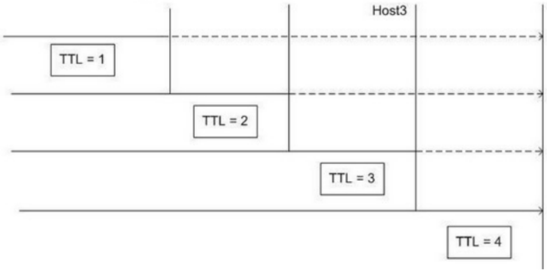
- Authentication
- Encryption
- Integrity

SSH runs over TCP, on the default port 22. When the client starts the session, send a packet to the server specifying the SSH version he supports. Then, the server answers with the SSH version he supports. After this initial handshake, the two exchange each other the encryption algorithms they support. After that, the first that is common to both is chosen. The client and the server now can move forward and authenticate themselves.
The authentication is made as follows: the server sends his public key (a.k.a the fingerprint) to the client. The client is now asked to trust or not trust the server fingerprint. If it trusts the server identity, the client proceeds with authenticating himself. This step can be done with username/password or with an Asymmetric Cryptography.
To authenticate the public and private key, the server can *challenge* the client: the server picks up a random string and encrypt that with the public key of the client. This encrypted value is then transferred to the client through the secured pipe (via the common chosen algorithm). The client decrypts the challenge with his private key and then crypts it again with the public key of the server. Once back, the server decrypts the challenge response: if the response is the same as the random value sent, with a certain degree of probability the client is the one associated with that public key. At this point, the session can start.

07_SSH_basics.pdf

B6 - Describe with an example how tracert (Traceroute) can discover the path taken from a packet directed to a specific destination

This command exploit the fact that every packet has a TTL field which is X when the packet leaves the NIC. Every hop decrease by one the TTL field. When the TTL reaches 0, the host that expired the TTL sends back to the sender an ICMP error packet. The packet contains the IP address of the host who expired the TTL. By sending packets with TTL starting from 1, tracert can discover the path taken from the packets to reach a particular destination.



B7 - Advantages and disadvantages of ip static and dynamic routing

Static Routing Advantages

- Easy to implement in a small network.
- Very secure. No advertisements are sent, unlike with dynamic routing protocols.
- It is very predictable, as the route to the destination is always the same.
- No routing algorithm or update mechanisms are required. Therefore, extra resources (CPU and memory) are not required.

Static Routing Disadvantages

- Suitable only for simple topologies or for special purposes such as a default static route.
- Configuration complexity increases dramatically as the network grows. Managing the static configurations in large networks can become time consuming.
- If a link fails, a static route cannot reroute traffic. Therefore, manual intervention is required to re-route traffic.

Most of the problems of **static routing** can be reconducted to:

- ***Scalability*** because as network increases in complexity, configuring every single router for every single path can be a tough task, in particular if you want to take into account the different path costs in a redundant network.
- ***Reliability*** because if a link goes down, the network cannot failover a redundant link automatically.
- ***Heterogeneity*** because the network can be composed of different router made by different vendors with different OSs, meaning that the sysadmin must be able to configure them all.

Dynamic Routing Advantages

- Suitable in all topologies where multiple routers are required.
- Generally independent of the network size.
- Automatically adapts topology to reroute traffic if possible.

Dynamic Routing Disadvantages

- Can be more complex to initially implement.
- Less secure due to the broadcast and multicast routing updates.
- Additional configuration settings such as passive interfaces and routing protocol authentication are required to increase security.
- Route depends on the current topology.
- Requires additional resources such as CPU, memory, and link bandwidth.

Rule: Once we have a routing protocol, we can abstract from how it is implemented and develop platform independent architectures, solving heterogeneity issues.

Find: A good routing protocol must discover failures and react properly, solving reliability issues.

Bring: the routing protocol must provide control messages to other nodes using the same protocol to exchange informations (e.g. subnets advertisement), solving scalability issues.

Bind: the routing protocol must guarantee connectivity all over the network nodes with the minimum amount of overhead.

OSPF Is one of the most spread dynamic routing protocol.

06_OSPF.pdf

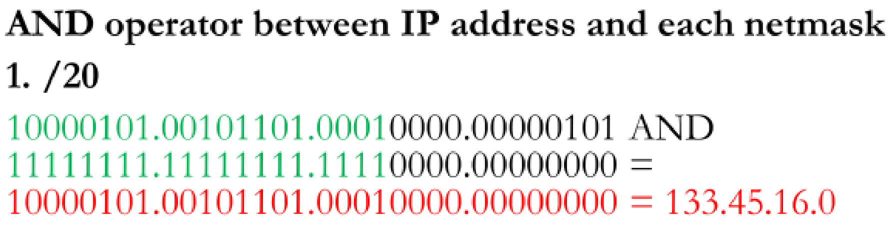
B8 - What are the fields of an ip routing table and how they are used to

- Metric

We can consider Hops as the routers along a packet's path during its travel from a source to a destination. In a network, the next hop is the next possible destination for a packet.
Next hop is an IP address (an entry in a routing table belonging to a router), which specifies the next closest/most optimal router in its routing path.
Every single router maintains its routing table with a next hop address for each network destination.

1. When a packet arrives at Router A, this router consults its routing table in order to find the best path towards the packet destination
2. Router A forwards the message to the interface specified by the routing table (best metric)
3. When the packet arrives a router directly connected to the destination network, its routing table indicates that the destination network is directly connected, so the router modifies the packet with the destination host MAC address and delivers the frame to the host

When a packet arrives a router interface, its IP destination address is not a network_id, but a host_id. In a routing table we have only the network_id, not the host_id of ALL HOSTS of ALL NETWORKS!!! We just need to find out what is the network_ID starting by an IP address and by the netmask
3 STEPS:
1. Convert both IP Address and Netmask into the equivalent binary
2. Make the logical AND operator between the IP Address and the Netmask
3. Convert the result into decimal -> We find the Network_ID



AND operator between IP address and each netmask

1. /20

10000101.00101101.00010000.00000101 AND
11111111.11111111.11110000.00000000 =
10000101.00101101.00010000.00000000 = 133.45.16.0

B9 - VPN

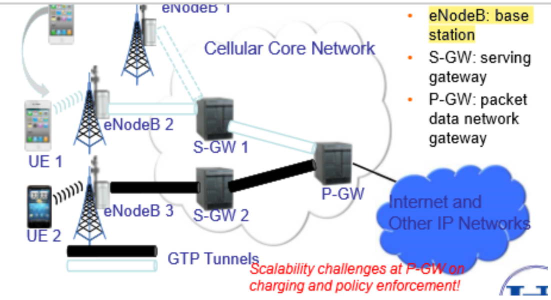
VPNs allow you to create a secure, private network over a public network such as the Internet. They can be created using software, hardware, or a combination of the two that creates a secure link between peers over a public network. This is done through encryption, authentication, packet tunneling and firewalls.
Running a virtual private network over the Internet raises an easily forgotten issue of reliability. Let’s face it: the Internet isn’t always the most reliable network, by nature. Tracing a packet from one point to another, you may pass through a half-dozen different networks of varying speeds, reliability, and utilization—each run by a different company. Any one of these networks could cause problems for a VPN. Generally, VPN is better than SSH because an SSH tunnel doesn’t offer all the benefits of a VPN. Unlike with a VPN, you must configure each application to use the SSH tunnel’s proxy. With a VPN, you’re assured that all traffic will be sent through the VPN (you don’t have this assurance with an SSH tunnel). With a VPN, your operating system will behave as though you’re on the remote network

---------------------Extra---------------------

E1 - SDN Mobile

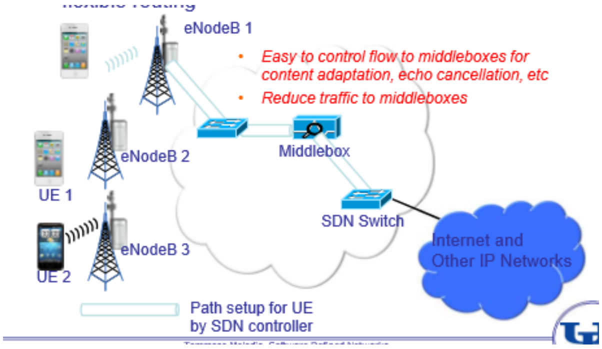
CellSDN

First of all we have to discuss the LTE infrastructures problem:



- eNodeB: base station
- S-GW: serving gateway
- P-GW: packet data network gateway

Scalability challenges at P-GW on charging and policy enforcement!


eNodeB 1
eNodeB 2
Middlebox
UE 1
SDN Switch
eNodeB 3
UE 2
Internet and Other IP Networks
Path setup for UE by SDN controller

- *Easy to control flow to middleboxes for content adaptation, echo cancellation, etc*
- *Reduce traffic to middleboxes*

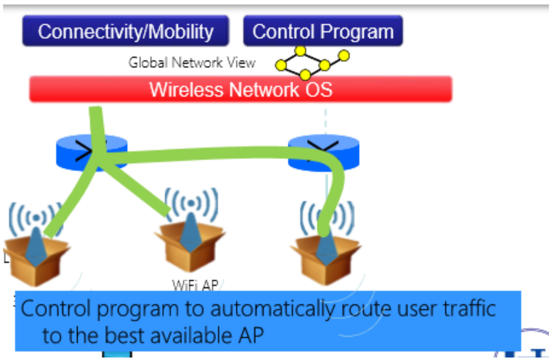
So, the new architecture is made of:

- A centralized control plane with a MiddleBox
- A SDN Switch (to satisfy traffic policies)

The SDN control plane has the faculty to manage all the previous generation of mobile telecommunication infrastructures (LTE-A,3G,2G…), so it can easily decide which is better in specifical cases. The CellSDN architecture is similar to a generic SDN with multiples networks OS and a slicer connected to the real hardware through OpenFlow and (Business)Applications through API's.

OpenRadio

Is the architecture devoted to know all informations about flows of traffics, quality of signal, management of the packets and so on, it has the task to know the details of the network (a global network view). This is the Open Radio architecture



Control program to automatically route user traffic to the best available AP

The OpenRadio AP's(access points) are cheap

SoftRAN : Software Defined RAN (Radio Access Network)

In LTE i have the RAN very simple. UE--->AN through radio waves.

These are the disadvantages of LTE-RAN:

- Distributed control plane
- Tight coordination becomes infeasible with density
- Huge demands on the backhaul network
- Inefficient radio resource management
- Hard to manage in a dense network

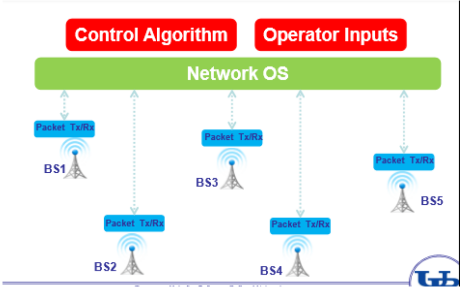
With SoftRAN i have 3 steps:

1. Connect to a single station
2. Assign resource blocks (time-and-frequency slots) to each flow
3. Assign transmit powers to be used for each resource block

This is smart and powerful but can suffer of interference: if power used by

- Coordinating handovers critical

So, as requirements, Radio Resource Management needs to be tightly coordinated.



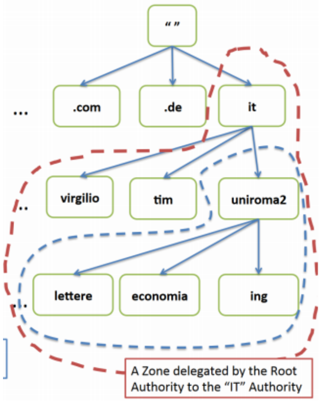
SoftRan Architecture

The advantages of this technology are:

- Efficient use of wireless resources
- Global view on interference and load
- Simplified network management
- Plug-and-play control algorithms

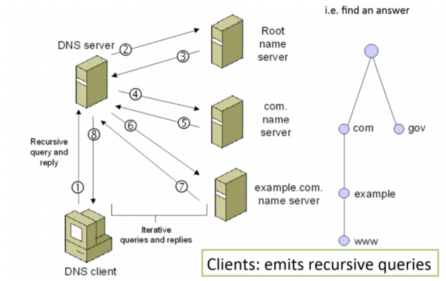
E2 - DNS

A Domain Name Server is a Server devoted to get the correct address of a certain domain. For example, if a certain domain (example.com) is signed in a DNS and my console is connected to that DNS, if i digit example.com instead of its ip, i reach the site without problems. Basically, a dns is a database containing indexed domains, another view is a inverted-tree-based tree. Where from the root, each level of the tree is a level of the dns and each node is a particular domain. Every subtree is a subdomain that *delegate* the domain to the root (Authority) of that subtree.



A Zone delegated by the Root Authority to the "IT" Authority

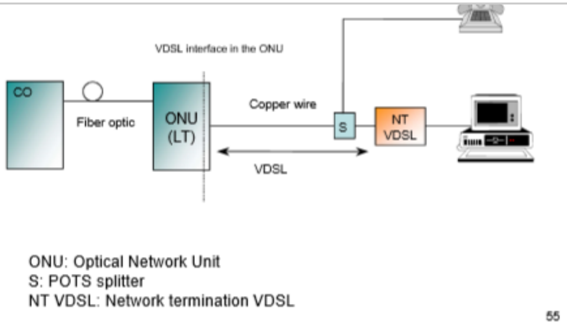
The Configuration of the dns is Master-Slave. The master send iterative queries to the slave ones and they reply with the subdomain that they have. These queries are sent from the user via a so called: Recursive query.



Clients: emits recursive queries

VDSL

It exploit the max performance that a copper wire can offer. The idea is also to have the smallest length of copper wire.


VDSL interface in the ONU
CO
Fiber optic
ONU (LT)
Copper wire
S
NT VDSL
VDSL
ONU: Optical Network Unit
S: POTS splitter
NT VDSL: Network termination VDSL
55

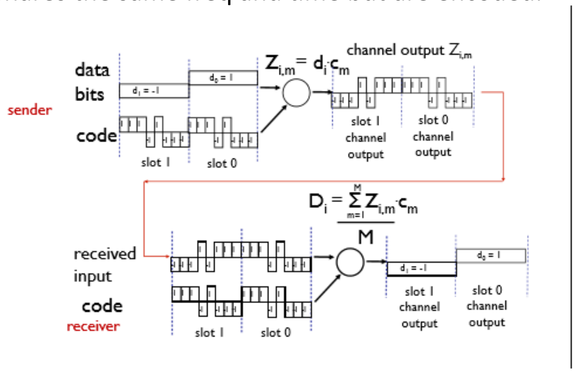
SO, now the ONU and CO are in the same place and is connected through fiber optic. then, from that point starts the copper wire. A VDSL Problem is the crosstalk. It is resolved with the vectorizing, generating an anti-signal built synching the devices signals.

SS7

Is a standard used to manage the communication over the network. It is deputy to routing, managing of the traffic, congestion control, data base queries. It sets the *how* the communication is trasmitted. Also ss7 is famous to be a very weak protocol and easy to permit a MITM attack.

CDMA

the protocol that uses a code for each user. Instead of FDD or TDD, all users shares the same freq and time but are encoded.



802.11 (The Wi.Fi)

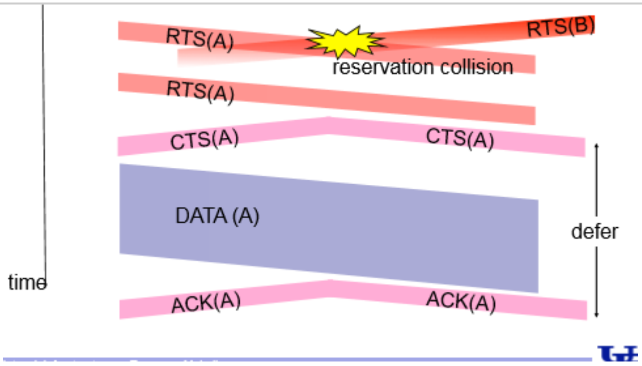
- *passive vs active* scanning:

A device has to find the best AP. It can do with an active (it’s the device to scan the area in search of the ap sending requests to them) Or passive (The AP’s send the requests and the device replies) approach.

CSMA/C(ollision)A(voidance) : is an upgrade of the protocol that solves the collisions.

It waits a difs time; if the channel is free then send data, else waits a rnd time then tramsmits the data. if the receiver doesn’t replies with an ack, then increases the timer.

The receiver once received the data, send the ack after a sifs.



LTE

3G++, Mobility and so on...

The previous generations had CDMA, here the things changed are:

1. Adaptive Modulation and Coding (AMC)
2. Hybrid ARQ (HARQ)
3. Spectrum flexibility: OFDMA and SC-FDMA
4. MIMO Transmission

1 -*Adaptive Modulation & Coding (AMC)*

Based on the data rate of the communication, the modulation changes.
if low -->QPSK
if high-->64QAM

2 - *Hybrid ARQ*

Procedure to manage the errors. Soft combining:

- Combination of FEC and ARQ (FEC: correct a subset of errors) - (ARQ: if still error detected)
- Works at PHY layer but controlled by MAC layer
- If the received data has an error then the Receiver buffers the data and requests a re-transmission from the sender

There are two main soft combining methods in HARQ: Chase combining and Incremental redundancy

3 - *Spectrum flexibility: OFDMA and SC-FDMA*

- The uplink (from UE to eNB) uses SC-FDMA (Single Carrier Frequency Division Multiple Access). each sub-carrier contains information of ALL transmitted symbols.

- The downlink (from eNB to UE) uses OFDMA (Orthogonal Frequency Division Multiple Access) allocates user in time and frequency domain. each sub-carrier only carries information related to one specific symbol.

4 - *MIMO Transmission*

Multiple Input Multiple Output are smart antennas. It can be SingleUser (Good experience for user) or MultipleUser(Good management of 2+ users simultaneously).

structure:

- Spatial multiplexing
- Beamforming (Adaptive or switched)
- Single stream transmit diversity

LTE-ADVANCED

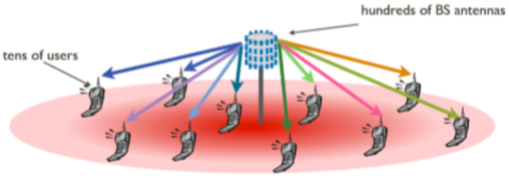
4G

1. Carrier aggregation
2. Enhanced MIMO (FD) ---> then Coordinated MIMO
3. Relays
4. Machine-to-Machine communication (M2M) ---> then Device-to-Device (D2D)
5. Heterogeneous Networks (HetNets)

- This is crucial to increment throughput (up to 1Gbps) because i get more bandwidth.
- Lower interference and mobility improvements
- Load balancing
- Low energy

2 - *Enhanced and Coordinated MIMO’s*

-V1: A simple evolution of previous mimo. Dynamic SU/MU-MIMO Switching, better beamforming, in general is optimized version of old mimo.
-V2: Full dimension (FD) mimo: accurate 3d beamforming
-V3: Massive mimo: every station has a huge number of antennas

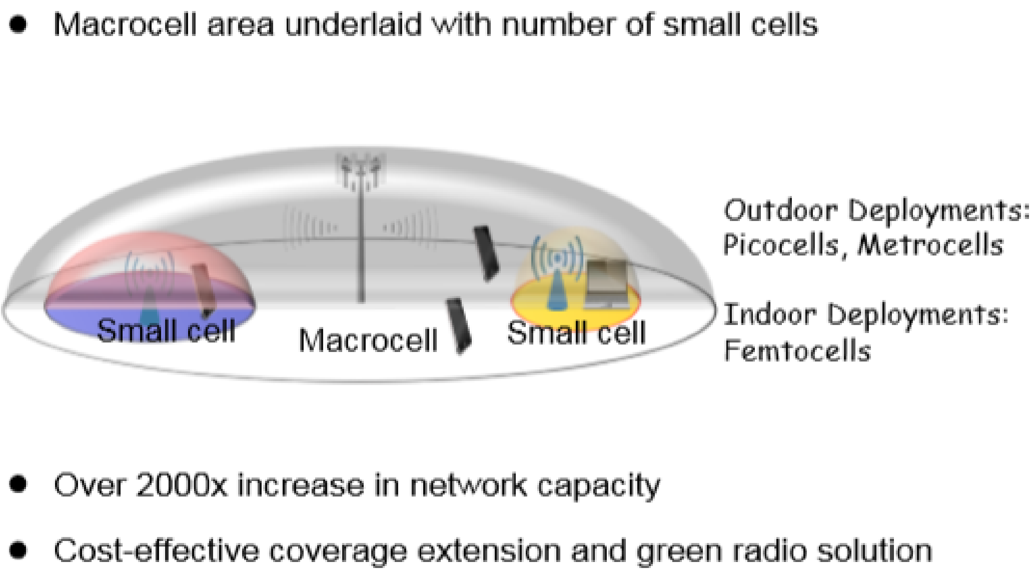


-V4: Coordinator MIMO: UEs at the cell-edge can communicate with several cell sites, both for the DL and UL. A sort of distributed system.

3- *Relays*
Basic relays used to forward the traffic to the “father” Mimo. That actually does the communication.
They are placed in far places and with them more user are reached. (Rural zones)

4 - *Machine to Machine comm. and Device to device*
M2M is a system that is based on the cellular infrastructes to communicated between smart things.
D2D instead is an Ad-hoc system built with the same puropose. Obviously D2D better than M2M but much expensive.

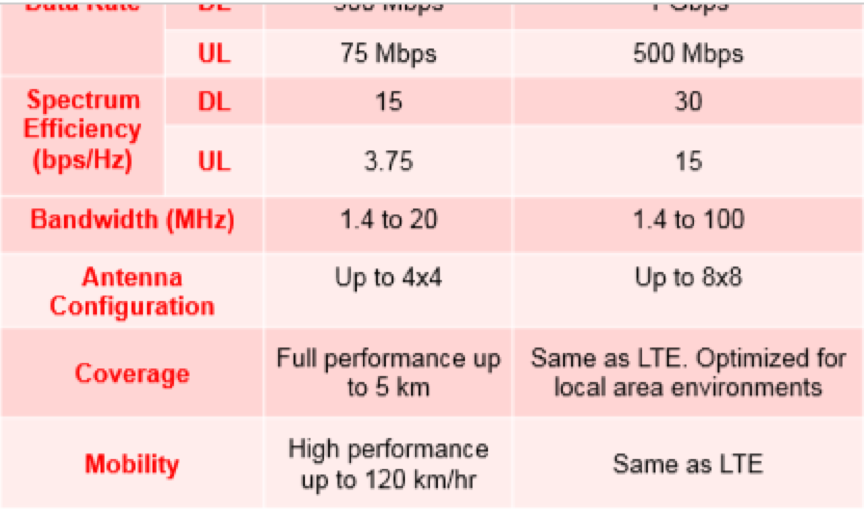
5 - *Heterogeneous Networks*



- Macrocell area underlaid with number of small cells

Small cell
Macrocell
Small cell
Outdoor Deployments: Picocells, Metrocells
Indoor Deployments: Femtocells

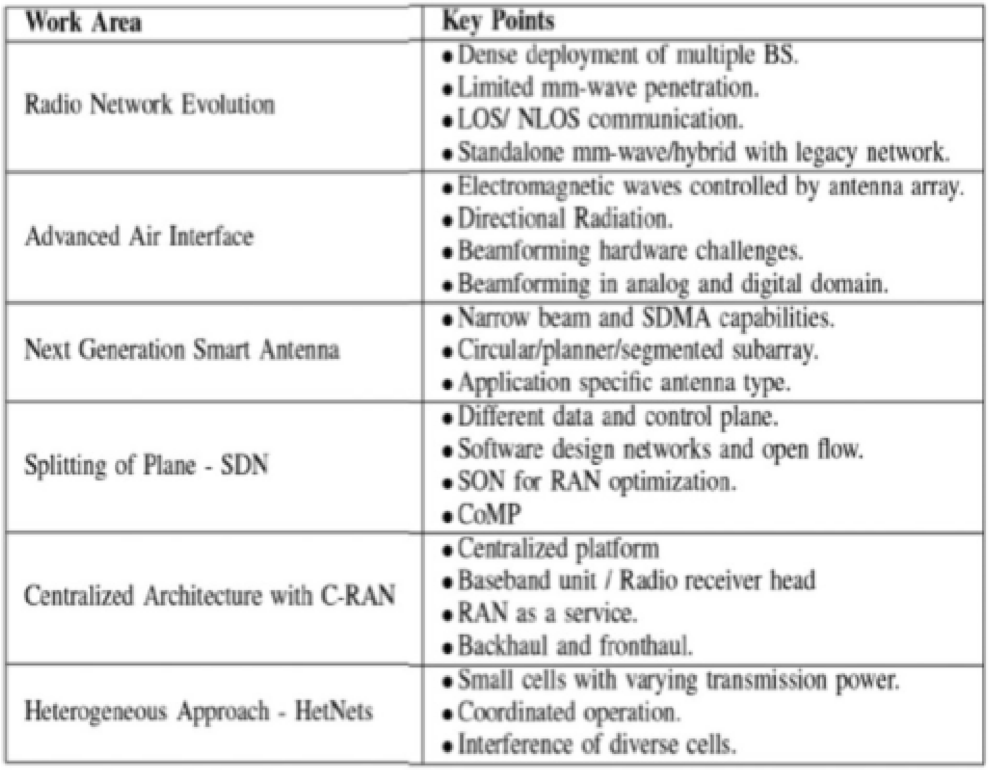
- Over 2000x increase in network capacity
- Cost-effective coverage extension and green radio solution



Data Rate	DL	300 Mbps	1 Gbps
	UL	75 Mbps	500 Mbps
Spectrum Efficiency (bps/Hz)	DL	15	30
	UL	3.75	15
Bandwidth (MHz)		1.4 to 20	1.4 to 100
Antenna Configuration		Up to 4x4	Up to 8x8
Coverage		Full performance up to 5 km	Same as LTE. Optimized for local area environments
Mobility		High performance up to 120 km/hr	Same as LTE

5G

5G wireless networks lies in exploring unused, high mm-wave band.
The propagation and penetration of mm-wave signal in outdoor environment is quite limited
ultra dense deployment is necessary in areas requiring high data rates.
Small cell sizes (at the order of 100-200 m)



Work Area	Key Points
Radio Network Evolution	• Dense deployment of multiple BS. • Limited mm-wave penetration. • LOS/ NLOS communication. • Standalone mm-wave/hybrid with legacy network.
Advanced Air Interface	• Electromagnetic waves controlled by antenna array. • Directional Radiation. • Beamforming hardware challenges. • Beamforming in analog and digital domain.
Next Generation Smart Antenna	• Narrow beam and SDMA capabilities. • Circular/planner/segmented subarray. • Application specific antenna type.
Splitting of Plane - SDN	• Different data and control plane. • Software design networks and open flow. • SON for RAN optimization. • CoMP
Centralized Architecture with C-RAN	• Centralized platform • Baseband unit / Radio receiver head • RAN as a service. • Backhaul and fronthaul.
Heterogeneous Approach - HetNets	• Small cells with varying transmission power. • Coordinated operation. • Interference of diverse cells.