NetInf

orchi.1736578

January 2021

Contents

Chapter 1

xDSL - x Digital Subscriber line

1.1 Introduction

DSL is a family of thecnologies that are used to transmit digital data over telephone lines.
DSL service can be delivered simultaneously with wired telephone service on the same telephone line since DSL uses higher frequency bands for data.
The strong point is that it uses the old telephone line.

1.2 ADSL

Asymmetric Digital Subsriber line. Asymmetric because bandwidth and bit rate are greater in DOWNSTREAM than in UPSTREAM.

Two separate frequency bands:

- Upstream → From END USER to the telephone CENTRAL OFFICE
- Downstream → From the CENTRA OFFICE to the END USER

1.2.1 Frequency assignment

So we have POTS(0 - 4KHz), UPSTREAM (25-138KHz) and DOWNSTREAM(138-1104kHZ)

To avoid interference, a gap is left between the POTS and other channels.

In adsl two types of mechanisms can be used to assign the Up and Down channels

- FDM - Frequency Division Multiplexing: ASSIGN each channel its own section of the frequency spectrum

- ECHO CANCELLATION: OVERLAP Upstream and Downstream, so we have to do an operation: the ECO CANCELLATION

1.2.2 ADSL and Cross-Talks

In ADSL exist two kind of cross-talks.

Cross-talk is a phenomenon by which a signal transmitted creates an undesired effect. In ADSL wires share the same cable, so they create interference between them.

The two kind of cross-talks are:

- FEXT: Far-End where trasmitter and riceiver placed in opposite sides of the cable
- NEXT: Near-End where trasmitter and riceiver placed on the same side of the cable

The FEXT cross talk is better than NEXT because there is more attenuation of the error: the further the distance, the more the signal is attenuated. In NEXT the signals from the receiver are softer than those from the transmitter (because they come from far), so there is stronger interference.

To decrease the noise we must decrease the number of twister pairs. Cross-talk tipically increases with frequency.

1.2.3 ADSL Modulation

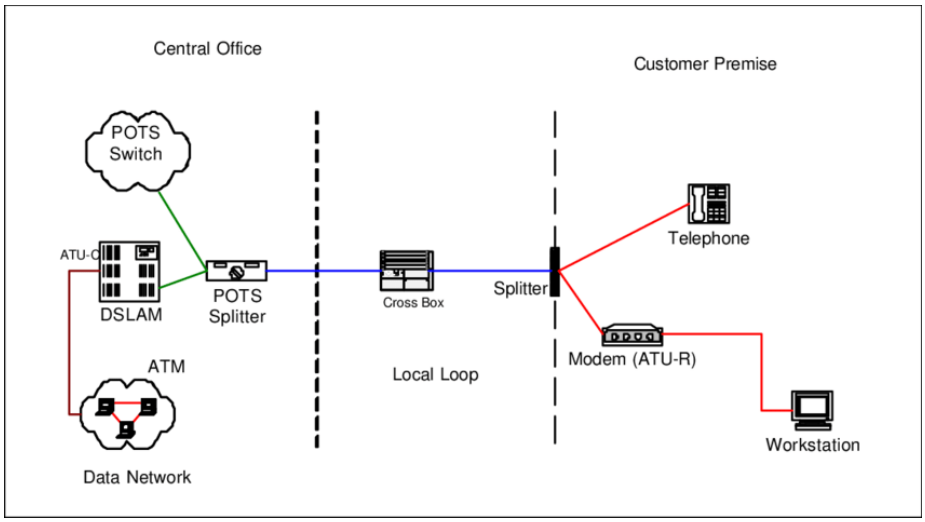
Two method:

- CAP: Carrierless Amplitude and Phase, which need adaptive equalizer
- DMT: Discrete MultiTone, which gives more speed than CAP

DMT uses different carriers at single frequency. The available ADSL bandwidth is divided into very small subchannels.

DMT is better than CAP: attenuation on each sub-band is constant so the use of channel equalizers is not necessary in reception and DMT can dynamically adapt the data rate to the line conditions (ie. SNR)

1.2.4 Architecture

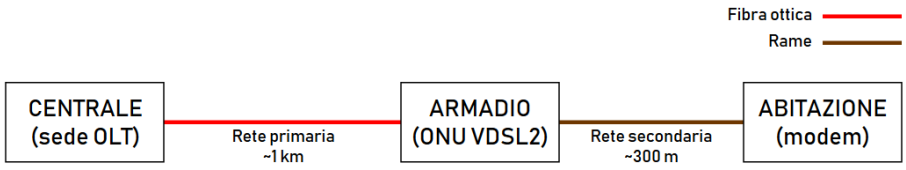


- POTS SPLITTER: A low-pass/high-pass filter
- ATU-R: ADSL Trasmission Unit - Remote.
  It is usually used to interface a single computer (USB or Ethernet interface) or directly integrated with a router to allow LAN access
- ATU-C: ADSL Transmission Unit - Central.
  Network modem (can be integrated into the access node)
- DSLAM: Digital Subscriber Line Access Multiplexer.
  A network device that aggregates multiple DSL lines onto a high-speed channel in order to gain access to the Internet
- CO: Central Office.
  A building to which subscriber home and business lines are connected on a local loop
- Local Loop
  The physical link or circuit that connects from the demarcation point of the customer premises to the edge of the common carrier or telecommunications service provider's network.

See more

1.3 VDSL

Very hight data rate Digital Subscriber Line
The key to fastest bit rate possible is to have the shortest possible length of copper wire and try to use higher frequency band.



ONU: Optical Network Unit: converts the fiber optic signal into the electric signal at the user side and enables reliable fiber optic Ethernet services to business and residential users through fiber-based network infrastructure.

1.3.1 Vectoring

The using of high frequency increase the cross talk problems.
The idea for avoid this problem is close to the principle of echo cancellation.

The DSLAM takes care of the disturbances that the line will receive from the neighbor, so it subtracts the disturbances in advance and the two contributions are compensated by canceling the noise.

To do this we must calculate Anti Signals: send a signal, then give back and shape the change of the original signal.

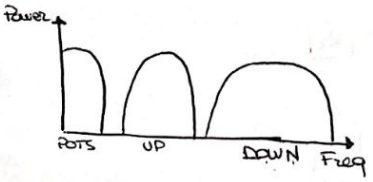
1.3.2 Notes

- Transmit digital data over telephone lines
  Possible thanks to the use of HIGHE FREQUENCY BANDS

- Separate frequency bands (FDM - feq. division Multiplexing)

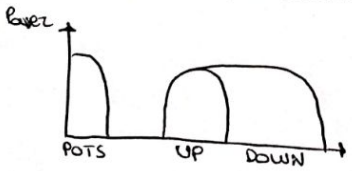
- Two mechanism for assigning UP and DOWN channels

  • FDM - Frequency Division Multiplexing



Assigns each channel its own section of the frequency spectrum

  • ECHO CANCELLETION



Upstream and Downstream overlaps to create a duplex channel, separated by echo cancellation technique

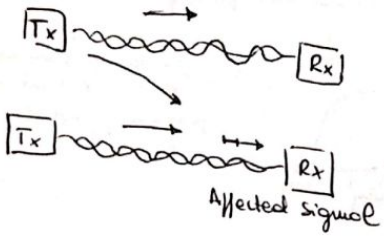
Problems in ADSL is the cross-talk, a phenomenon by which a signal trasmitted creates interference.

↑

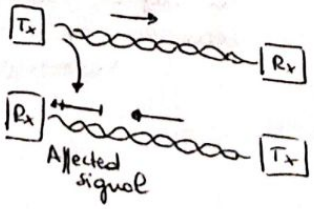
We use (in ADSL) the same cable for more wires

2 types of cross-talk:

- FEXT - Far End, better



- NEXT - Near End, worst



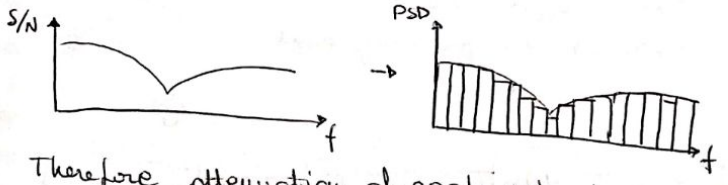
Next is worse because the signal is attenuated in relation to the distance, so the interference is stronger than in NEXT.

ADSL MODULATION:

- CAP – Carrierless Amplitude and Phase
- DMT – Discret Multitone

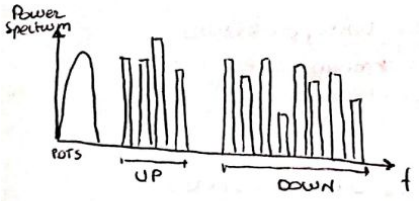
CAP is worse than DMT because on adaptive equalisers, so is slower is needed

DMT instead, divide the available bandwidt in small subchannels



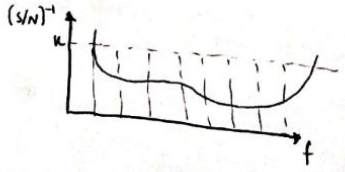
Therefore attenuation of each sub-channel is constant and the use of chanel equalisers is not necessary

Moreover DMT can dynamically adapt the data rate to the line condition.



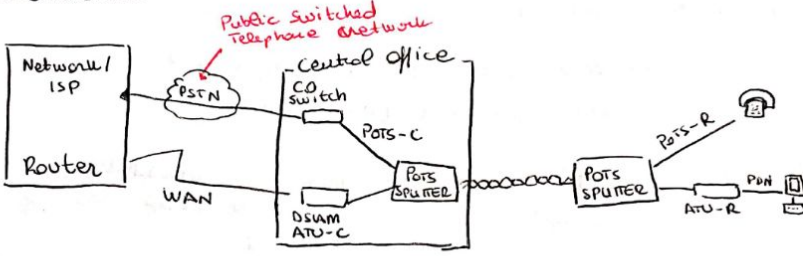
Every tone have QAM modulation

The power for each subcarrier is determinate as the deep of a pool.



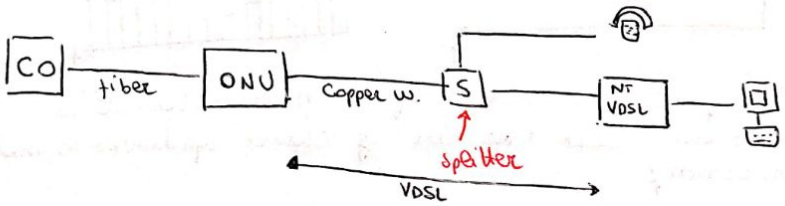
We can deduce the number of bit per simbol to associate to the QAM constellation used in each subchanel

ADSL ARCHITECTURE



VDSL

- To increase the bit rate:
  - Less copper cable
  - Use a higher frequency band



Problems:

Higher frequency ⇒ cross talk problems
neigh. wires interfere with each other

Solution:

VECTORING:

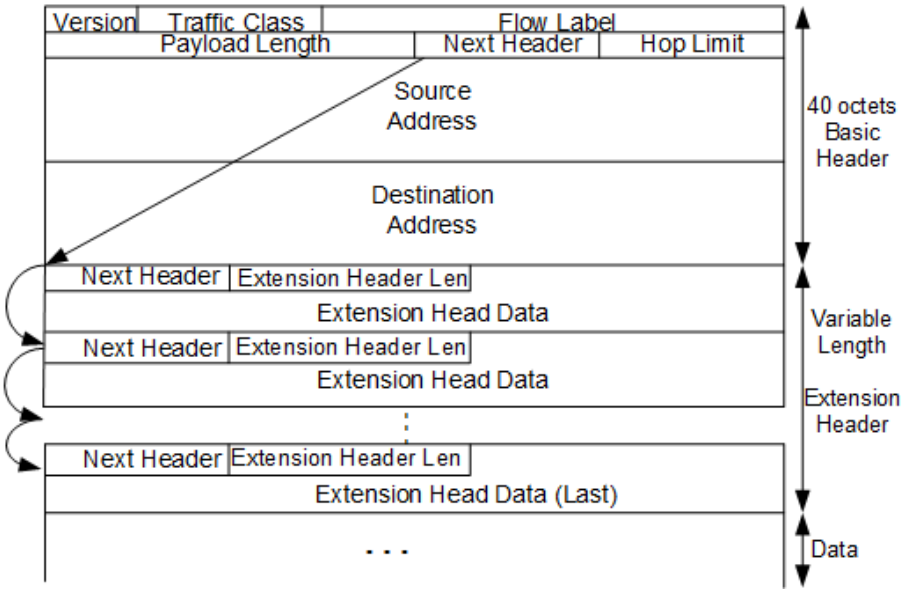
DSLAM subtracts the disturbances (previously measured) first of send the information.

Chapter 2

IPv6

Respect IPv4:

- Expanded addressing capabilities: 128 bits instead of 32 bits
- Header format simplification
- Improved support for extension and options
- Flow labeling capability
- Authentication and privacy capabilities



2.1 Header Format

- Version(4 bits): internet protocol version number = 6
- Traffic Class(8 bits): to manage the traffic
- Flow Label(20 bits): identifier of a flow of packets between source and destination
- Payload Length(16 bits): the size of the payload(the rest of the packet following this IPv6 header) in octets
- Next Header(8 bits): the type of next header. The field can specifies the transport layer protocol used by packet's payload
- Hop Limit(8 bits): replace the time to live field in IPv4, is decremented by one at each forwarding node and the packet is discared if it become 0
- Source Address(128 bits): The address of the sending node
- Destination Address(128 bits): The address of the destination node(If routing header is present may not be the ultimate recipient)

This is the fixed header. We can also have:

- Extension Headers: carries optional internet layer information. The headers form a chain using the Next Header fields(the last indicates the type of the upper-layer protocol header)

These headers aren't processed (inserted, deleted) until the packet reaches the node identified in the destination address field. Moreover must be processed strictly in the order they appear in the packet.

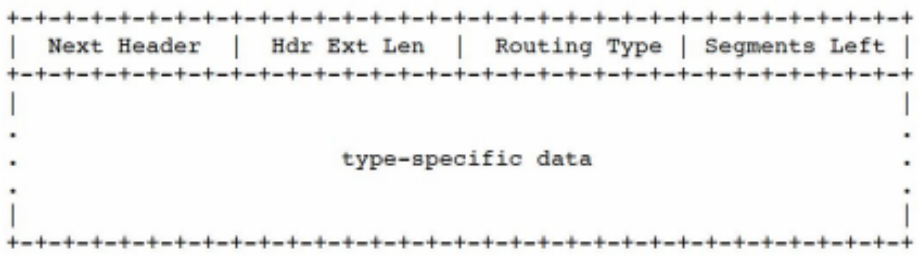
2.2 Extension Headers

The recommended order when are used in the same packet:

1. IPv6 header
2. Hop-by-Hop Options header
3. Destination Options header
4. Routing header
5. Fragment header
6. Authentication header
7. Encapsulating Security Payload header
8. Destination Options header
9. Upper-Layer header

2.2.1 Routing Header

Used in IPv6 source to list one or more intermediate nodes to be 'visited' on the way to a packet's destination.



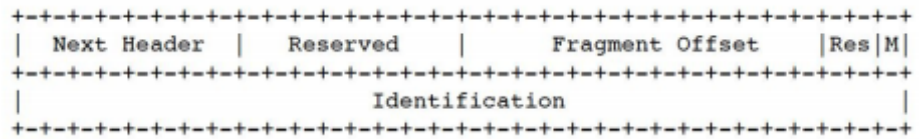
- Routing Type: identifier of a particular Routing header variant
- Segments Left: number of nodes still to be visited before reaching the final destinatio (explicitly listed)

In RH0 (Routing Type header = 0) permits multiple intermediate node addresses and also the inclusion of the same address. This mechanism can create problems: an attacker could be use it to cause congestion along arbitrary remote paths.

2.2.2 Fragment Header

Used in IPv6 to send a packet larger than would fit the path MTU(the minimum link MTU of all the links in a path) to it's destination.
Unlike IPv4 fragmentation in IPv6 is performed only by source nodes.
Pros: less processing, delay and overhead
Cons: security threats, need of path MTU discovery procedure.

To minimize the use of fragmentation IPv6 try to minimize the supported MTU size and allowing only the hosts to fragment datagrams. In IPv6 every link should have an MTU of 1280 octets or greater. (See MTU)
IPv6 nodes should implement Path MTU Discovery in order to discover and take advantage of path MTUs greater 1280 octets. If not implemented IPv6 may simply restrict itself to sending packets no larger than 1280 octecs.



- Fragment Offset: define the offset of the data following this header

- M flag: a bit set to one when more fragmets will follow or 0 if is the last fragment
- Identification: define the fragments which belong to the same packet

2.2.3 Reassembly Fragment Packet

Packets must have the same Source and Destination Address and same Fragment Identification.

Errors:

- Insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first arriving fragment of that packet
  So, reassembly must be abandoned and all received fragments are discarded
- The length of fragment is not a multiple of 8 octects and the M flag is 1
  So the frame is discarded and an ICMP Parameter Problem is sends to the source
- Fragments of a packet are overlapped
  So reassembly of packet must be abandoned and all the received fragments must be discarded

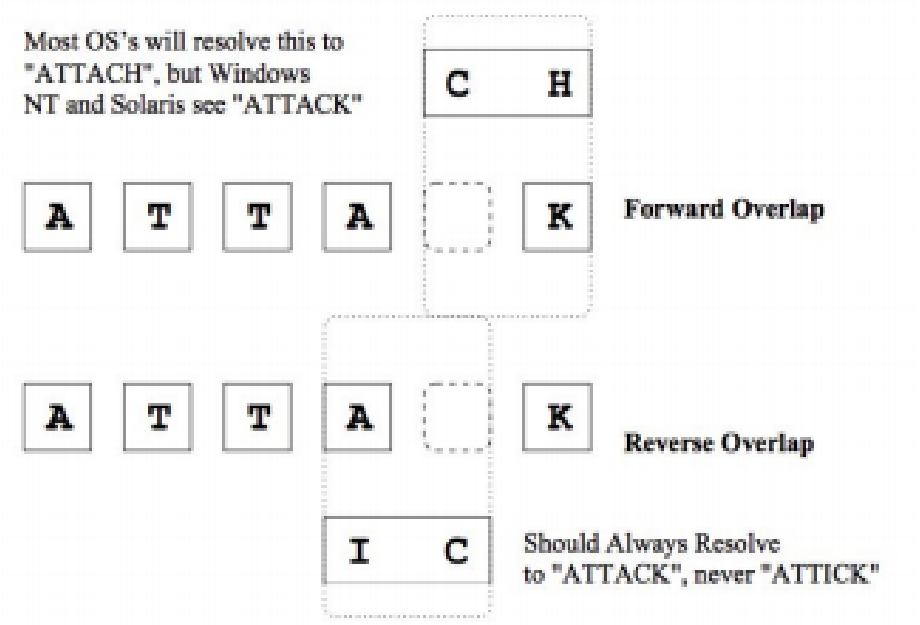
When we have fragmentation overlap we must abandon the reassembly because can be problem to detect a malicious attack (different hosts might generate different packets). Overlapp can occours when fragments of differing size arrive out of order a in overlapping positions.

2.3 PMTUD and Black Holes

Path MTU Discovery, based on ICMP Packet Too Big messages, allows the source to discover the Path MTU.
Black holes (is where the ICMP message doesn't reach the sending host to inform it that it needs to adjust its MTU) occur when the network infrastructure is UP but connection among end devices is DOWN.

2.4 Security Properties

- Eavesdropping: on-path elements can observe the whole packet of each IPv6(stealthily listening to the private conversation or communications of others without their consent)
- Packet insertion: packet from attacker is inject into the network

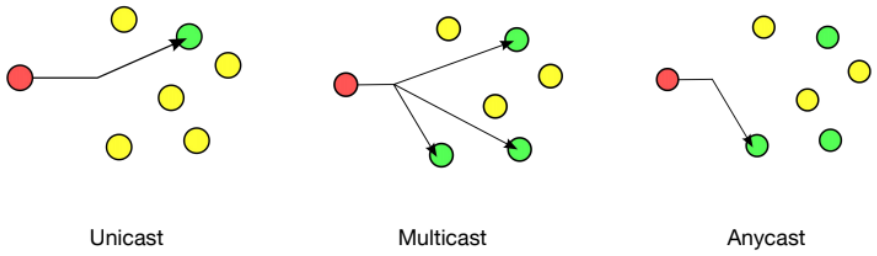


- Packet modification: attacker removes a packet from the wire, modifies it and re-injects it into the network
- Man-in-the-Middle(MITM) attacks: the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other
- Denial-of-Service(DoS) attacks: attacker sends large amounts of legitimate traffic to a destination to overwhelm it

2.5 Types of addresses

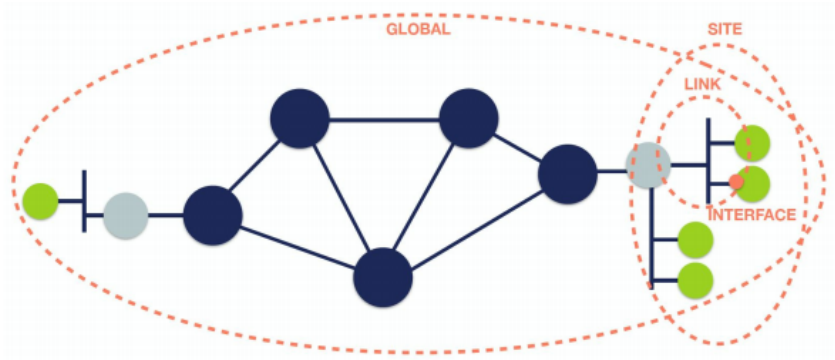
- Unicast - identifies a single interfaces
- Multicast - identifies a set of interfaces that typically belong to different nodes
- Anycast - similar to multicast addresses, except that packets are sent only to one interface, not to all interface(the closest)

The general form for an IPv6 address is x:x:x:x:x:x:x:x with 'x' four hexadecimal digits.
The address Prefix is the costant address and the notation is: IPv6-address/prefix-length, that specifying how many of the leftmost contiguous bits of the address comprise the prefix.



The interface Identifiers in unicast adresses are used to identify interfaces on a link.

Unicast addresses that can be used to implement subscriber access network:
Global Unicast Adresses: is a unique IPv6 address assigned to a host interface. These addresses have a global scope.
Link-Local addresses: allows communication between neighboring hosts that reside on the same link. Link-local addresses have a local scope, and cannot be used outside the link.



2.6 Neighbor Discovery

Nodes use Neighbor Discovery to:

- Determinate the link-layer addresses for neighbors
- Purge cached value that become invalid
- Find neighboring routers

- Keep track of which neighbors are reachable
- Detect changed link-layer addresses

slide 66

2.7 Host Autoconfiguration

Get an IPv6 address for a host:

- Manual configuration
- Stateless autoconfiguration: when site is not concened with addresses host use (SLAAC)
- Stateful autoconfiguration: when site requires control over address assignments (DHCPv6)

SLAAC:
Requires no manual configuration hosts. A hosts generates its own addresses using a combination of locally available information and information advertised by routers:
Routers advertise prefixes(identify the subnets associated with a link)
Interface identifier(uniquely identifies an interface on a subnet).

Lifecycle of a SLAAC address depends on the lifetime of the prefix used to generate it.
Two lifetime for prefixes:

- Preferred lifetime (Preferred address)
- Valid (Preferred or Deprecate address)

When a new host connects to the subnet:

- Generate an IPv6 Link Local address with Duplicate Address Detection to verify the uniqueness of the generated address
- Sends router solicitation to discover routers in the subnet
- Ruoter reply with advertisement containing (optional) the subnet prefix
- With this information the host generate a global unicast IPv6 address

DHCPv6:
slide 87

2.8 Transition Mechanism

Two mechanism to manage transition between IPv4 and IPv6:

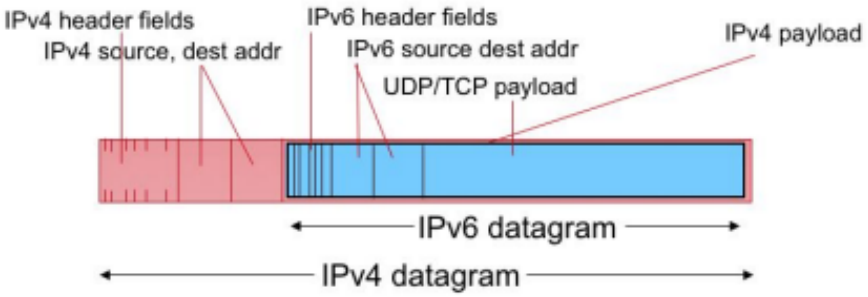
- Dual IP layer (or dual stack): complete support for both IPv4 and IPv6 in hosts and routers (can originate and understand both IPv4 and IPv6 packets)
- Tunneling of IPv6 over IPv4: establishing poin-to-point tunnels by encapsulating IPv6 packets within IPv4

When both devices are dual stacked, the two devices agree on which IP version to use.

Dual Ip Layer Operation/Dual stack:
If you are going to dual stack all of your network devices, the interfaces need both an IPv6 and an IPv4 address.
To remain compatible with IPv4-only nodes by providing a complete IPv4 implementation:

- Address Configuration: nodes may be configured with both IPv4 and IPv6 addresses(ie. DHCPv4 + SLAAC)
- DNS: If a dual-stacked device queries the name of a destination and DNS gives it an IPv4 address (a DNS 'A' Record), it sends IPv4 packets. If DNS responds with an IPv6 address (a DNS 'AAAA' Record), it sends IPv6 packets.

Tunneling:
Provides a way to utilize an existing IPv4 routing infrastructure to carry IPv6 traffic, encapsulating IPv6 datagrams in IPv4 packets. This is done by Encapsulator, that determinant of which packets to tunnel.



Chapter 3

IPSec

A secure network protocol suite that authenticates and encrypts the packets of data to provide secure entrypted comunication between two computer over an IP network.
It support:

- Confidentiality: only sender and reciever should understand message contents (encrypts, decrypts)
- Authentication: sender and receiver want to confirm identity of each other
- Message integrity: sender and receiver want to ensure message not altered
- Access and Availability: services must be accessible and available to users

Two protocols are used to provide security:

- AH - Authentication protocol: designated by the header of the protocol
- ESP - Encapsulating Security Payload: a combined encryption/authentication protocol

3.1 Security Architecture

3.1.1 Security Associations

An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. Security servicies are afforded to an SA for the use of AH or ESP, but not both.

A Security Association is uniquely identified by three parameters:

- SPI - Security Parameters Index
- IP Destination Address

- Security Protocol Identifier (AH or ESP)

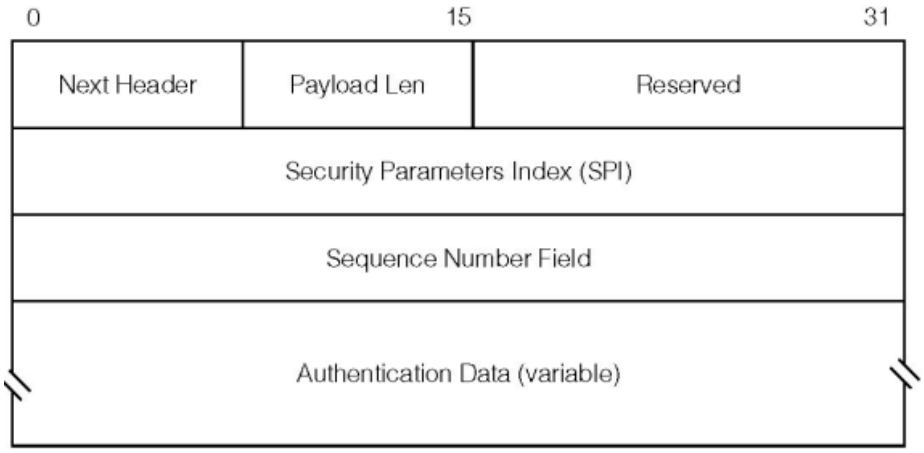
IPSec implementation includes:

- Security Association Database (SAD) that defines the parameter associated with each SA
- Security Policy Database(SPD) that contains entries that defines a subset of IP traffic and points to an SA for that traffic

SA selectors are used to filter outgoing traffic in order to map it into a particular SA

3.2 AH - Authentication Header

Provides support for data integrity and authentication of IP packets.
Enables an end system to authenticate the user and filter traffic accordingly
Prevents and Protects against: Address Spoofing Attacks and Replay Attack



- Next Header(8 bits): the type of header following this header
- Payload Length(8 bits): length of AH
- Reserved(16 bits)
- Security Parameters Index(32 bits): identifies a security association
- Sequence Number(32 bits): increasing counter value
- Authentication Data(variable): contains the Integrity Check Value or MAC for this packet

AH authenticate the entire IP packet, except variable fields on IP header because can be modify by intermediate nodes.

3.2.1 Anti-Replay Service

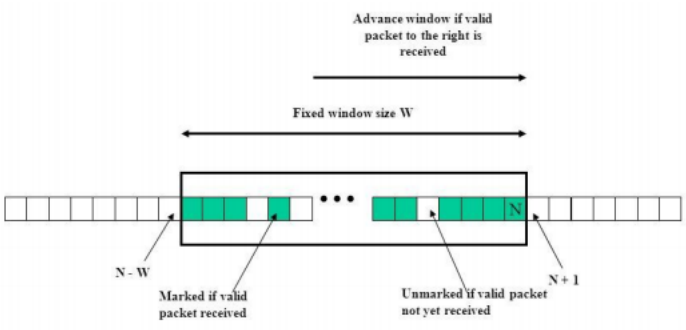
Replay attack: an attacker obtains a copy of an authenticated packet and later trasmits it to the destination.

Sender side:
The Sequence Number field is designed to thwart such attacks

- The sender initializes SN to 0 and each time that a packet is sent on this SA the sender increments the counter and places the value in the SN field
- The sender can't back to zero the SN field. If it reachs the limit of number, the SA terminate

Receiver side:
IP is a connectionless and doesn't guatantee that packets will be delivered in order(or delivered), so the receiver implement a windows of size W

- Received packet falls within the window and is new, and the packet is authenticated:
  - the corresponding slot in the window is marked
- Received packet is to the right of the window and the packet is authenticated:
  - the window is advanced so that this sequence number is the right edge of window
  - the corresponding slot in the window is marked
- Received packet is to the left of the window or authentication fails
  - the packet is discarded



3.2.2 Integrity Check Value

ICV is a message authentication code produced by a MAC algorithm.
Protect information against changes by unauthorized parties and MAC - Message Authentication Code used to provide integrity and authentication of messages (Generates an authenticator with message 'm' and a secret key 'K').

3.2.3 Transport Mode

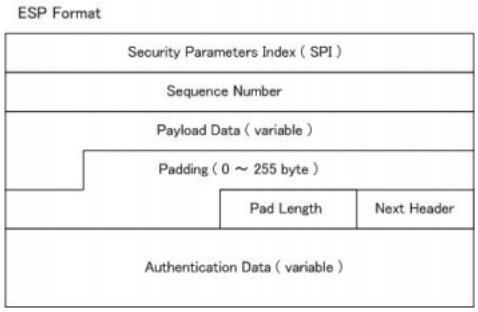
Does not create a new IP header and provides protection for upper-layer protocols.
Authenticates the IP payload and selected portions of IP header.

3.2.4 Tunnel Mode

Creates a new IP header for each packet.
In AH it authenticates entire inner IP packet plus selected portions of outer IP header and outer IPv6 extension headers.

3.3 ESP - Encapsulating Security Payload

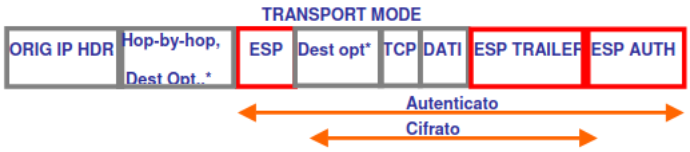
Provides confidentiality services (Can also provides an authentication service).
Authentication differs from AH because it does not cover the external IP header.



- SPI(32 bits)
- Sequence Number(32 bits)
- Payload Data(variable)
- Padding(0 255 bytes)
- Pad Length(8 bits): indicates the number of pad bytes preceding this field
- Next Header(8 bits)
- Authentication Data(variable): contains the ICV computed over the ESP packet minus the Authentication Data field

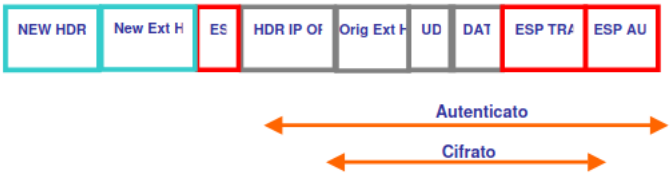
3.3.1 Transport Mode

Does not create a new IP header and provides protection for upper-layer protocols.
Encrypts and optionally authenticates the IP payload but not the IP header



3.3.2 Tunnel Mode

Creates a new IP header for each packet.
In ESP it encrypts entire inner IP packet.



3.4 Combining Security Associations

Individual SA can't implement AH and ESP protocol togheter.
Encryption and authentication can be combined in order to transmit an IP packet that as both confidentiality and authentication between hosts.

3.4.1 ESP with Auth Option

Transport mode: authentication and encryption apply to the IP payload delivered to the host, but the IP header is no protected.
Tunnel mode: authentication applies to the entire IP packet delivered to the outer IP destination address and authentication is performed at that destination.

3.4.2 Transport Adjacency

The inner being an ESP SA and the outer being an AH SA.
In this case ESP is used without its authentication option, the authentication covers more field(include soure and destination IP addresses) but there is more overhead.

3.4.3 Transport-Tunnel Bundle

Inner AH transport SA and outer ESP tunnel SA. Moreover authentication prior to encryption: the authentication data are protected by encryption(nobody can intercept the message) and may be desiderable to store the authentication information with the message at the destination for later reference.

3.5 Key Management

Involves the detrmination and distribution of secret keys.
Two types of key management in IPSec Architecture:

- Manual: system administrator manually configurate each system with its own keys and with the keys of the other communicating systems.
  Is pratical for small environments
- Automated: automated system enables the on-demand creation of keys for SAs.
  Is pratical for large distribution system with an evolving configuration

3.5.1 Oakley Key Determination Protocol

Automated key management protocol, is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security.

3.5.2 ISAKMP - Internet Security Association and Key Management Protocol

Automated key management protocol, provides a framework for internet key management and provides the specific protocol support.

3.6 IKE Protocol

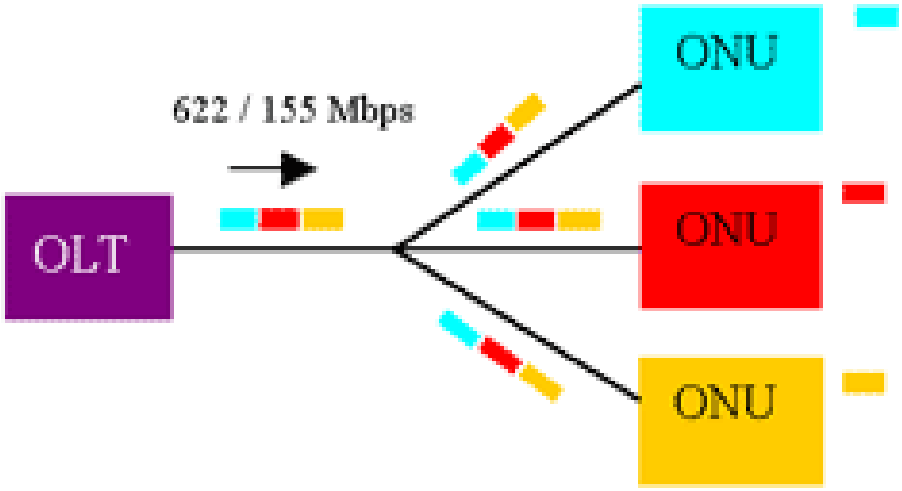
Internet Key Exchange protocol, an hybrid implemetation of the Oakley key exchanges, designed according to the ISAKMP framework.
It works in two phases:

- IKE phase 1 negotiation
  establishes an ISAKMP SA and three shred keys are established
- IKE phase 2 negotiation(quick mode)
  establishes IPSec SAs

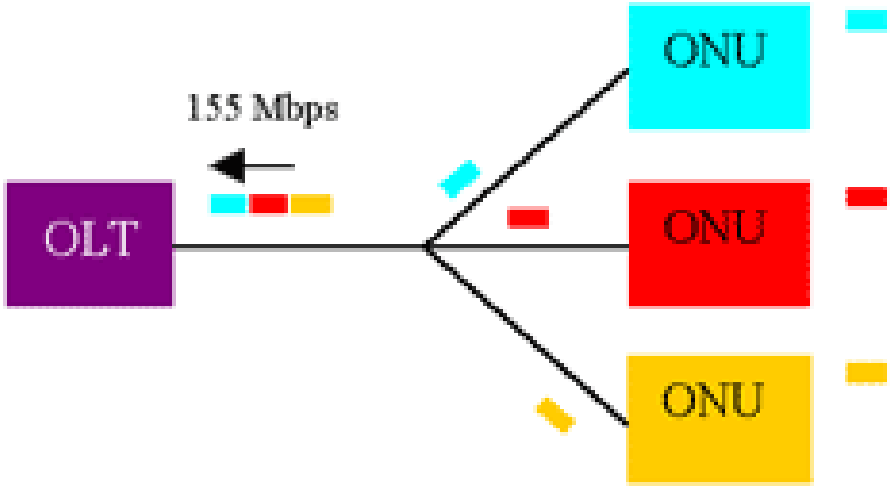
Chapter 4

PON - Passive Optical Networks

A fiber-optic telecommunications technology for delivering broadband network access to end-customers.
Implements a point-to-multipoint topology, in which a single optical fiber serves multiple endpoints by using unpowered (passive) fiber optic splitters to divide the fiber bandwidth among multiple access points.
Is a symmetric technology, so upstream and downstream have the same bitrates.



(a)



(b)

4.1 Advantages and Problems

Splitter is an advantages respect the curb switch:
the curb must convert, amplify and retrasmit the signal, instead the splitter use the same signal.
The problem is that there is a loss of power when the signal is split.

Another problem is that we have to recognize where the right user is to send the signal.

In upstream we have problem of collision and different power of signal.

4.2 Traffic Scheduling

In both side use wavelenght separation, using one wavelength for downstream traffic and another for upstream traffic on a single mode fiber.

Downstream(To the user):

TDM: Time Division Multiplexing scheme

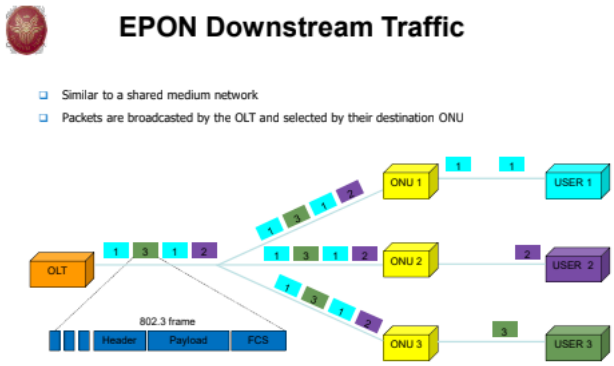
Upstream(To the OLT)

TDMA: Time Division Multiplexing Access
Because the user share the same link, we have to avoid collision.
Because ONU can be in different distance we have problem of power in OLT.
So the OLT use the Automatic Gain Control to adjust 0-1 threshold

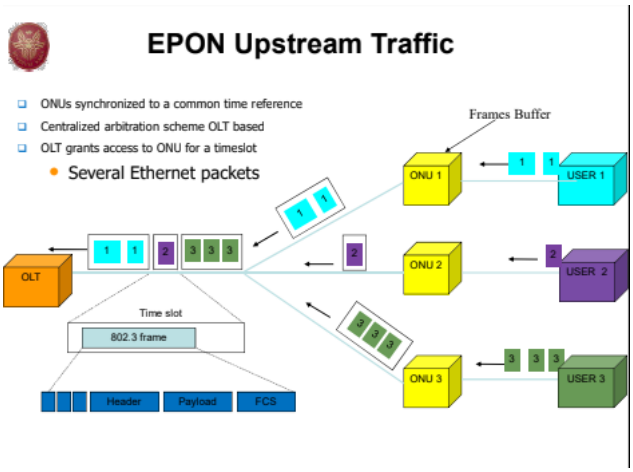
4.3 EPON

A Passive Optical Network which carries Ethernet frames encapsulated in 802.3 standards. It is a combination of the Ethernet technology and the PON technology.

Downstrea: With EPON we know where send the signal, so packets are broadcasted by the OLT and selected by their destination ONU



Upstream:



4.4 WDM-PON

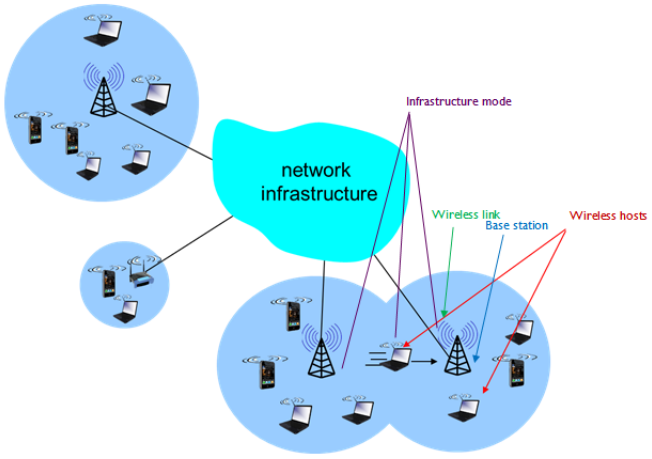
Multiple wavelenghts both in downstream that in upstream: layers and fiber can trasmit contemporary different colors.
Optical router can route the information selecting the color.

Chapter 5

Wireless Access

5.1 Elements of a Wireless Network

- Wireless Host: laptot, smartphone, run applications...
- Base Station: typically connected to wired network is responsable for sending packets between wired network and wireless hosts in its area
- Wireless link: typically used to connect mobiles to Base Station, used as backbone link.
  Link access are coordinate by multiple access protocol
- Infrastructure mode: base station connects mobile into wired network.
  HANDOFF: mobile changes basestation(mobility) providing connection into wired network



5.2 Types of Wireless Network

5.2.1 Ad hoc network

- There isn't Base Station
- Nodes can only transmit to other nodes within link coverage
- Nodes organize themselves into a network: route among themselves

5.2.2 Cellular network

A radio network distributed over land areas called cells.

Wirless link use the CDMA - Code Division Multiple Access that assigns unique code to each user. So, even if all users share same frequency, each of them ha own code to encode data, allowing multiple users to coexist ad trasmit simultaneously with minimal interference

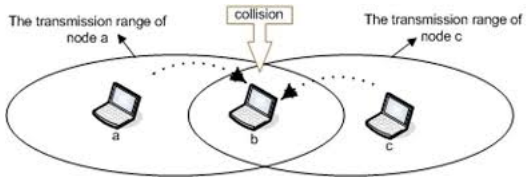
5.3 Wireless Link Characteristics

Different to wired link:

- Decreased signal strength: radio signal attenuates as it propagates through matter (path lost)
- Interference from other sources: other devices use the same spectrum band
- Multipath Propagation: radio signal reflects off objects ground, arriving at destination at slightly different times

5.4 Hidden terminal problem

Not all users are visible to each other. We have collision and to reduce them the



IEEE 802.11 standard provide the CSMA/CA - Carrier Server Multiple Access/ Collision Avoidance MAC protocol.

Sender:

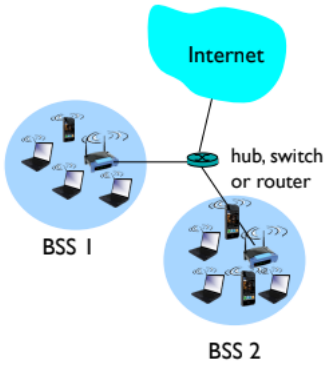
First it listens to dereminate wheter another node is trasmitting or not(with hidden problem is not secure that avoid collision)
If another node was heard, so it wait for a random period of time.
To avoid hidden problem, trasmits small request-to-send(RTS) packets to BS using CSMA
Even if RTS collide there isn't probleme because is a short packets

Base Station:

Broadcasts clear-to-send (CTS) in response to RTS, so CTS heard by all nodes

So the sender, when receive own CTS start to send data, instead other stations defer transmissions for a random period of time.

5.5 LAN Architecture

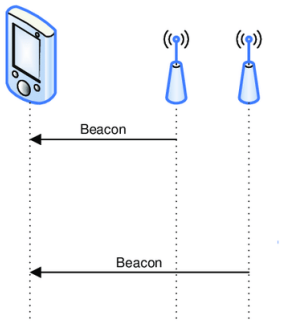


Wireless host: communicate with basestation(Access Point)
Basic Service Set(BSS) or cell: contains wireless hosts and AP

5.6 Scanning for access point

5.6.1 Passive scanning

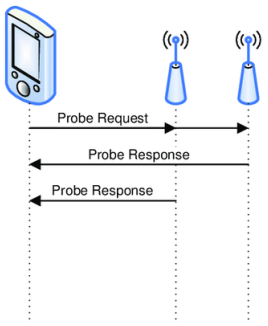
The client listens on each channel for beacons sent periodically by an AP



Passive Scanning

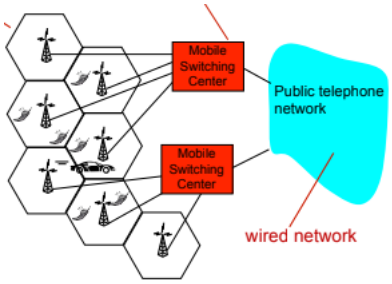
5.6.2 Active scanning

The client trasmits a Probe Request and listens for a Probe Response from an AP



Active Scanning

5.7 Cellular network architecture



Two technique for sharing mobile-to-BS radio spectrum:

- FDMA and TDMA: divide spectrum in frequenxy channels and each channel into time slots
- CDMA: Code Division Multiple Access: there is a code to rebuild the original signal, so the user can trasmit in the same frequency and time. Different users signals arrive at receiver as an unique signal. With the code, it can manage signals for every user

5.8 Mobility

Home network: permanent home of mobile
Permanent address: address in home network, can be used to reach mobile
Home agent: perform mobility functions when mobile is remote
Visited network: network in which mobile currently resides
Care-of-address: address in visited network
Foreign agent: performs mobility function (in visited network)
Correspondent: wants to comunicate with mobile

To approach mobility we can:
let routing handle it: but is not scalable to milions of mobiles
let end-systems handle it.

5.8.1 Registration

1. Mobile go in visited network, so contacts foreign agent
2. Foreign agent contacts home agent

So home agent knows location of mobile.

5.8.2 Indirect routing

Communication from correspondent to mobile through home agent, then forwarded to remote:

1. Correspondent send packets using home address of mobile
2. home agent intercepts packets and forwards them to foreign agent where mobile is located
3. Foreign agent receives packets and forwards them to mobile
4. Mobile replies directly to correspondent

Mobile in this case uses two addresses: Permanent (used by correspondent) and care-of (used by home agent) address.

Triangle routing is inefficent when correspondet and mobile are in the same network.

5.8.3 Direct routing

Correspondent gets foreign address of mobile from home agent and sends packets directly to mobile

1. Correspondent sends the request to the home agent for the foreign address of the mobile
2. Receives foreign address of mobile
3. Correspondent forwards packets to foreign agent, that forwards to mobile
4. Mobile replies directly to correspondent

Overcome triangle routing problem

WIth direct routing we have problem if mobile chages visited network and correspondent have already get care-of-address from home agent.
To avoid this problem first foreign agent is anchored, so data always routed first to anchor FA and when mobile moves new FA arranges to have data forwarded from old FA(chaining)

5.8.4 Handling Mobility

The Mobile Switching Center manages the mobility and there are two element:

- HLR - Home Location Register: database in home network containing permanent cell phone number, profile information and current location
- VLR - Visitor Location Register: database with entry for each user currently in network(could be home network)

When the user receive a call:

1. Call routed to home network
2. Home MSC consult HLR and gets roaming number of mobile in visited network
3. Home MSC forwards call in MSC visited network
4. MSC in visited network completes call trough base station to mobile

5.8.5 HANDOFF

Handoff is the process of transferring an active call or data session from one cell in a cellular networks, necessary for preventing loss of interruption of service to a caller or a data session user.

5.8.6 CELLS

The cells are hexagonal: provides full coverage and permits reuse of pattern, that is to reuse the same frequency at given distance without interference.

With small size of cells th bitrate increase (also the power decrease).

5.9 LTE

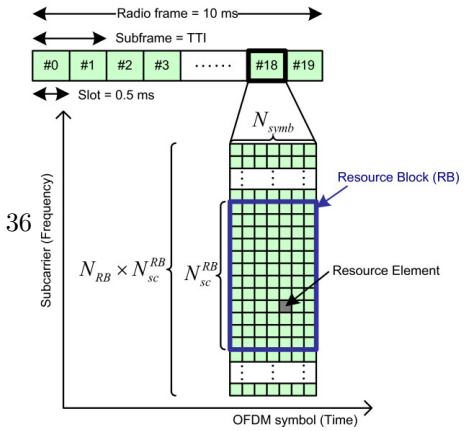
With LTE we increase the datarate, how?

- Using the adaptive modulation and coding
- Using HARQ
- Using higher bandwidths
- Using MIMO and smarth antennas

LTE divide MHz of given bandwidth in Resource Block(pieces)(ie. 3MHz - 15RB)

5.9.1 Adaptive Modulation and Coding

Improve modulation skills with continuos measurament of channel quality, provide different modulation skill.
The Channel Quality Indication (CQI) is required by eNB from UE, so eNB can adapt the modulation according



to the CQI(BPSK,16QAM,64QAM).
With low SNR we obtain low CQI so we use simple modulation, instead with high SNR we obtain high CQI and use better modulation (So higher bitrate).
If the user moves, the CQI changes. For every user is used a different modulation combos.

AMC try to follow the Shannon Limit.

5.9.2 Hybrid Automatic Repeat Request

Is a combination of FEC and ARQ.
FEC - Forward Error Correction: put some extra bit used for detect and correct error
ARQ - Automatic Repeat Request: ask, in case of error, the re-trasmission of signal from the sender

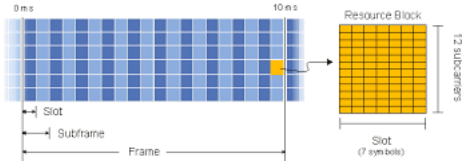
If I'm sure that the channel is good I use only ARQ and not FEC because I don't want to use extra bits, we don't want send bits which are not used.

5.9.3 HARQ with soft combining

If I receive wrong information I combine the same set of data with the new set, so maybe I can try to recover the right information. This mechanism allows not to waste bandwidth.

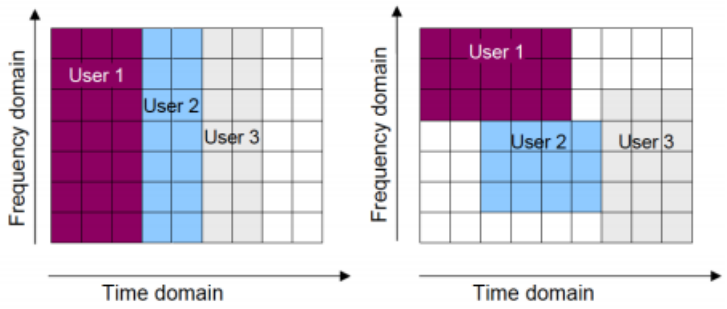
5.9.4 Spectrum flexibility

LTE manage spectrum in a dynamic way. Different bandwidth, different Resource Blocks.
Resource Block is a set of subchannels represented in a set of time slot (equal to 0.5ms) that occupate 180KHz and are managed in differe way in Uplink and Downlink. Overall bandwidth is represent by a matrix.



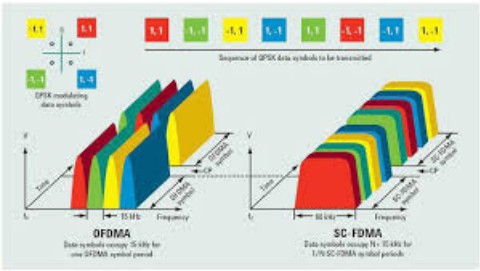
The allocation of the bandwidth is dynamic and specific for the different users:

- Uplink uses SC-FDMA - Single Carrier Frequency Division Multiple Access
  In frequency domain there are different subcarrier. LTE uses this subcarriers all togheter (as a Single Carrier - SC)
- Downlink uses OFDMA - Orthogonal Frequency Division Multiple Access
  Different subcarrier, different user. Divide in both frequency domain and the time domain.



First is SC-FDMA in uplink and Second is OFDMA in downlink

Why this division?
Because in downlink is the eNB that manages the allocation for each EU. Instead in uplink we use time division because it is easier to manage.



More

5.9.5 MIMO - Multiple Input Multiple Output

A way to provide transmission in a system with multiple antennas in output and input. Is an evolution of SISO and MISO.
This mechanism improve the performance of datarate.

Three different modes:

- Transmit diverity(TxD): the same signal in multiple antennas.
  When a signal is trasmitted there are:
  - Direct path
  - Extra paths(reflection). Thanks to MIMO this extra paths are collected by other antennas in the receiver side.

With signal replicas the receiver (Rx) can combine them and increase signal performance (The multiple antennas are in the same receiver!!)

In this case we have a channel with more dimension, so we have a matrix and not a vector.

- Spatial multiplexing(SM)

Transmitter split own data streams in N different flows and parallelize the trasmission. In this case can't be done the diversity gain.

- Beamforming

The signal usually is transmitted in all direction, but if I have different antennas I can combine their transmission so that the resulting signal has a shape(Beam). Is more important because i can concentrate the signal in one direction and avoid interference with another basestation.

5.9.6 Massive MIMO

One antennas with more subantennas that managed different users, provides in the same cells multiple beans.
Improve the capacity.

5.10 LTEA

Thanks to better technologies and use of large bandwidth allow the increase of datarate. LTEA introduce the mechanism 'Cooperation of the basestation'. This is related to Beamforming and is a way to perform frequency reuse. The base stations exchange information with each other
Instead of operate in cells and distance for the reuse of frequency, we operate in beams.

Moreover LTEA can aggregate some bandwidth(Carrier aggregation) to obtain more capacity. This can be done both if different bands of the spectrum are close to each other (easier) and if they are far(harder)