Networks and Cybersecurity

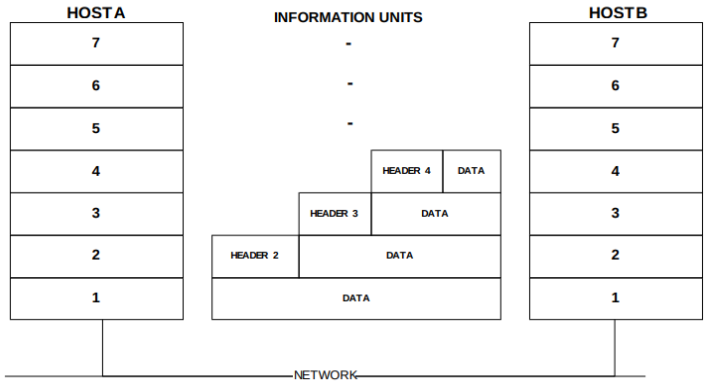
Network architectures: Ring, Star, Bus
Standardization authorities

- ISO International Organization for Standardization (ISO)
- IEEE Institute of Electrical and Electronic Engineers {e.g. IEEE 802.3}
- IANA Internet Assigned Numbers Authority

Communication mode: Synchronous communication, Asynchronous communication
Connection mode: Point-to-point communication, Multipoint communication
Communication options: simplex, half-duplex, full-duplex
Interface types: DTE (Data Terminal Equipment), DCE (Data Communication Equipment)
Services can be:

- **connection-oriented:**
  - Creation of a connection; Data transfer/exchange; Release of the connection.
- **Connectionless**:
  - Sending/transfer of data without establishing a connection among the communication nodes

Communication options: unicast, multicast, broadcast, anycast, geocast
An anycast network try to connect to multiple hosts, but after the first connection the communication will be between out host and the first that catch the connection.
A reliable service is a service that guarantee that all data is correctly sent to the due recipient.
Usually a confirmation message (ACK acknowledgement) is sent from the destination node.
Reliability introduces an overhead that may be considered undesirable.



Physical layer
Cabling standards: ANSI: EIA/TIA 568 and TSB36 e TSB40 ,ISO/IEC DIS 11801.
Multiport Transceivers is the device that allow fiber connection.
Datalink layer
it guarantees to its upper layer a link without errors.
Error detection (checksums, parity bits, CRC) Error correction (e.g. Hamming code)

Data integrity:
it can use parity (VRC, BCC, SRC) that check the parity of bits, there is a bit that determinate it.
CRC is based on a polynomial division between data and a polynomial generator that is a prime number, the reminder of the division will be an unique number valid for all n digits integer number. It will appended at the end of the frame. (XOR between bits, if 1,1 or 0,0 = 0 else 1)

```
ABCDEFGHIJKLMNOP
11000010000000000
100011101
---------
010011001
 100011101
 ----------
 000101111
    100011101          (*)
    ---------
    001100101
      100011101
      ---------
      010001001
       100011101
       ---------
       000001111 = 0x0F
ABCDEFGHIJKLMNOP
```

The verification is valid if the same operation give reminder equal 0, the generator is known by both hosts.
Errors detection: it use hamming code, it use bits of control and bits of message.
Datalink has 2 sub-layer, LLC (Logical link control) and MAC (Media Access Control). The MAC layer allows to manage different standard

to avoid collision (CSM/CD), and manage the abstraction of physical layer to LLC. it sends data to LLC that elaborate data providing service for upper layers.
PPP is the protocol used for communication in LAN and WAN, LCP(Link control protocol) is used to negotiate any point-to-point.
The maximum size of a packet in PPP is 1500 byte, equal to Ethernet, minimum frame size of 64 bytes.
CSMA/CD it is a protocol used to manage collisions.
CS: Carrier sense→ each nodes listen the network for activity.
MA: Multiple Access→ the network is shared among all nodes.
CD: Collision Detection → even during transmission the components are actively listening on the network to detect collision. In case a collision is detected:

- The node detecting the collision send a jammer signal that resets the all network.
- Each node recovers connectivity after a random interval.
- Each node listen to the network.
- The transmitting node re-transmits data if no activity is detected, otherwise it waits

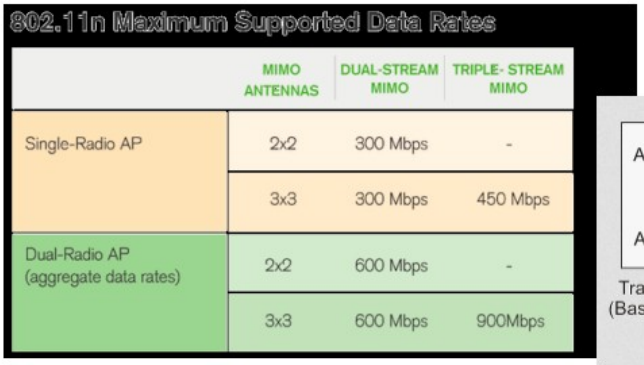
When a packet is received the card checks the 2 bytes:

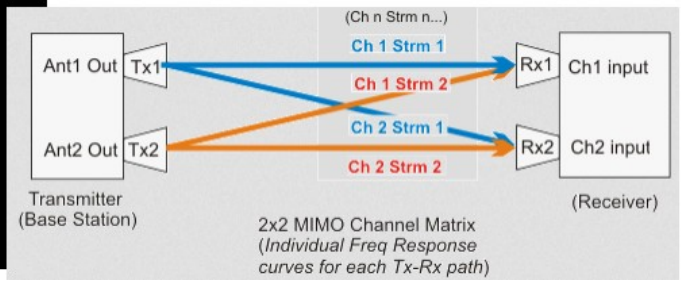
- content > 1500 : Ethernet packet
- content < 1500 : 802.3 packet, the protocol type is encapsulated in the information handled by the LLC level.

Type field) that contains the value **0x0800** to identify the encapsulated protocol as IP
The NIC sends the frame, led by a preamble, which is a leading bit pattern used by the receiver to correctly interpret the bits as ones and zeroes.
Token Ring networks:
it operates at 16 Mbps, IEEE 802.5
Working principle:

- When a machine wants to communicate it has to wait for free token, as soon as the machine gets a free token it loads the token with data.
- The clearing process is expected to be done by the machine that originates the token, that will therefore empty it.
- Other machines have to wait for the token to be free to communicate, however they can reserve the token to use it when it will be free.

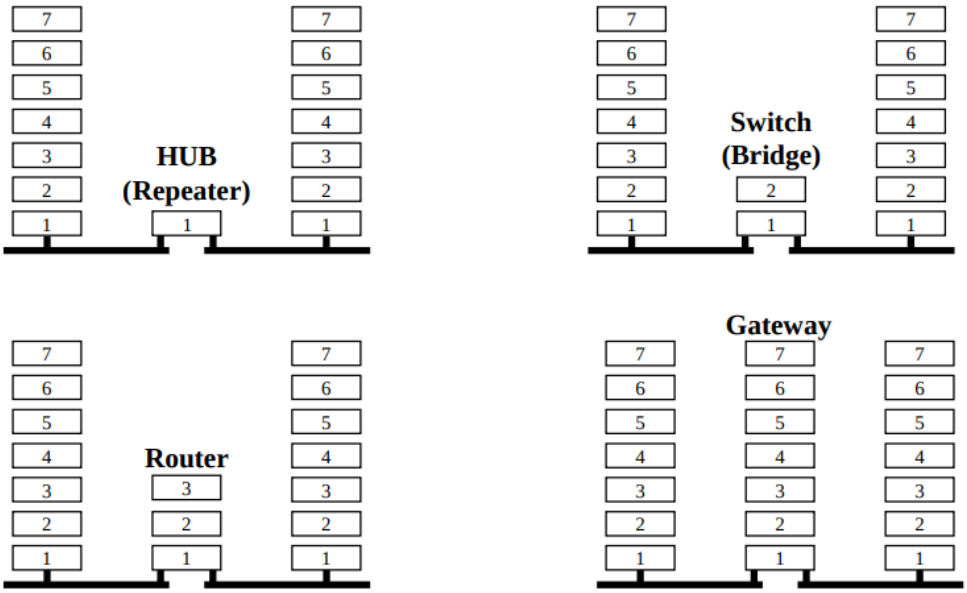
WIFI 802.11n
Standards of security: WEP - Wired Equivalent Privacy,WPA - Wi-Fi Protected Access, WPA - Wi-Fi Protected Access 2 (WPA + AES 128 bit)
MIMO: Multiple Input, Multiple Output. Wireless communication use this protocol to allow multi host connection with different frequencies.





ATM (Asynchronous Transfer Mode)

it is not an IEEE-Standard. It is switch-based. It has dedicated capacity it support 25, 155,622 Mbps or 2.4 Gbps. Cell-Based with 53 byte cells, that are fixed the difference with frame is that in frame transmission size can be different packet per packet in cell based it always cell's default size.
It negotiate service connection with: end-to-end connections or virtual circuits.



At level 2 devices use MAC address, it is an address composed by 6 byte. The first 4 bytes indicates the manufacturer of the nic the remain identify the nic, unique code for every nic.
Example: 00-2B-8C-42-5A-F1, switches base their "routing" on MAC address. Some switches allows to have some extra functions like VLAN, QoS …

VLAN IEEE 802.1Q

A virtual local area network (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer.
VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and deployment.
VLAN add a level in the frame, after mac addresses composed by the following fields

- Tag protocol identifier (TPID)
  - 16-bit field, set to **0x8100** to identify the frame as IEEE 802.1Q-tagged frame. Located at the same position as the EtherType field in untagged frames, thus used to distinguish the frame from untagged frames.
- Tag control information (TCI)
  - A 16-bit field containing the following sub-fields:
  - Priority code point (PCP)
  - A 3-bit field which refers to the IEEE 802.1p class of service and maps to the frame
    priority level. Different PCP values can be used to prioritize different classes of traffic.
- Drop eligible indicator (DEI)
  - A 1-bit field. (formerly CFI[b]) May be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion.[6]
- VLAN identifier (VID)
  - A 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal

values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs.

The connection between 2 switches, is called trunk.

Network Partitioning

Network ip is always even and broadcast ip is odd, broadcast ip is the last ip and network is the first; gateway for convention is the first available ip.

…	/…	…	…
255.255.254.0	/23	512	510
255.255.255.0	/24	256	254
255.255.255.128	/25	128	126
255.255.255.192	/26	64	62
255.255.255.224	/27	32	30
255.255.255.240	/28	16	14
255.255.255.248	/29	8	6
255.255.255.252	/30	4	2

Loopback ips are local-host ips, 127.0.0.0, 127.0.0.1,…

There are some classes of ips used for private, thus they can't be used to connect networks cross internet.

A(10.0.0.0-10.255.255.255) .../8

B(172.16.0.0.0-172.31.255.2555)../12

C(192.168.0.0-192.168.255.255) .../16

A device can act on LAN through 2 parameters: IP address, subnet mask.

To communicate outside the LAN it must have default gateway(Router) address in the IP configuration.

Routing

There are 2 types of routing:

- **Static routing**: each route is manually added, programmed and maintained on each routers
- **Dynamic routing**:

  it use routing table and update that continuously.

  The optimization of routing path is based on 2 principles:
  - Distance vector: metric system to calculate the path, number of hop, or number of networks between 2 end nodes
  - link state:it operates taking into account the current state of the path: bandwidth, link state such as delay and network congestion

Some switches can work at level 3 but they are not able to connect wan like routers.

Routers are "slow" machines. Its possible setup a PC as router.

Network protocols (not IP)

- Routing protocols, e.g. OSPF, RIP, …
- Network protocols, IP protocol:
- IPv4
  - Address Resolution Protocol (ARP)
  - Internet Control Message Protocol (ICMP)
  - IPv6

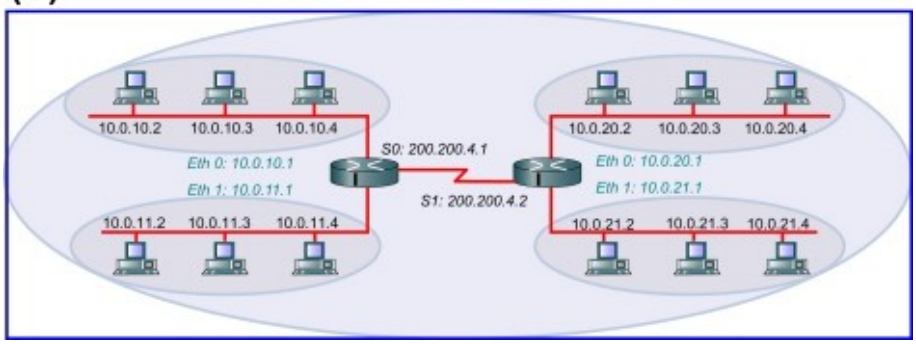
  Routing:
  - Static

- Dynamic (RIP…)

(A)

Learned	Network Address	Hop	Interface
C	10.0.10.0	0	Eth0
C	10.0.11.0	0	Eth1
C	200.200.4.0	0	S0
R	10.0.20.0	1	S0
R	10.0.21.0	1	S0

(B)



Routing can be grouped in a bigger network (geographical routing)
0.0.0.0/0 all networks. Routing table must contains only optimized paths, I put paths that have the same metric.
For RIP protocol 16 is infinite, network is offline. In the table we could put a backup paths.
Routing algorithm get data and optimize routing tables. Routing tables are based on network status.
RIP learns routes sending messages in the network and adds new routers that missed in the routing table. It starts from known networks.

Routing topology

every router interface must be on at least 1 network.
An interface can have multiple ips.
In static routing you must maintain all routers in the network, if you edit something you must change every router that reflect that change. Static routing must be used only for special cases.
Use dynamic routing! It uses routing tables. **Routing algorithm must be simple.**

- **Adaptive routing**: it search the shortest path using Dijkstra algorithm , measuring the cost called metrics expressed in hops.
- **IGRP**: *Interior Gateway Routing Protocol*: (CISCO propriety protocol)it bases on distance vector with additional metrics on network status. IGRP is used for bigger network. Maximum number of hops 255, RIP was 15. It uses and equation based on bandwidth, load and delay to calculate metric.

Metric =[K1*Bandwidth+(K2 * Bandwidth)/(256-load) + K3*Delay] *[K5/(reliability) + K4]
The default constant values are K1 = K3 = 1 and K2 = K4 = K5 = 0.

- **OSPF**: *Open shortest path first* this algorithm works on areas. And the management in the areas is specific for the areas. This is the way how internet works. It is open source.
  The protocols based on the link state have a complete vision of the network topology and its status (unlike distance vector that is limited to hop count).
  The protocol acquires information on the near link states and forwards it information to the other nodes using the algorithm link state broadcast

- **EIRGP:** Enhanced Interior Gateway Routing Protocol: protocol based on combination of distance vector and link state information. It is an evolution of IGRP, max hop:224

Feature	RIP	IGRP	OSPF	EIGRP
Algorithm	Distance vector	Link state	Link state	Both distance vector & link state
Metric	Hop count	Based on delay, bandwidth, channel occupancy and reliability of the path.	Routing based on on bandwidth delays, throughput and RTT	Bandwidth, load, delay, hop count and reliability
Maximum no. of hops	15/16 hops is considered to be infinity	Maximum 255 (default 100)	Depends on the size of routing tables	Maximum 255
Subsystem segmentation	Autonomous system is treated as single subsystem	No segmentation of the autonomous system (AS)	Breaks the autonomous system in areas	System is not divide in areas
Proprietary/Open	Open	Proprietary	Open	Proprietary

An autonomous system is a system that internally managed the networks independently and use *internal router* they can use different routing algorithm from border routers. The communication with outside is managed by border routers.

Exterior router

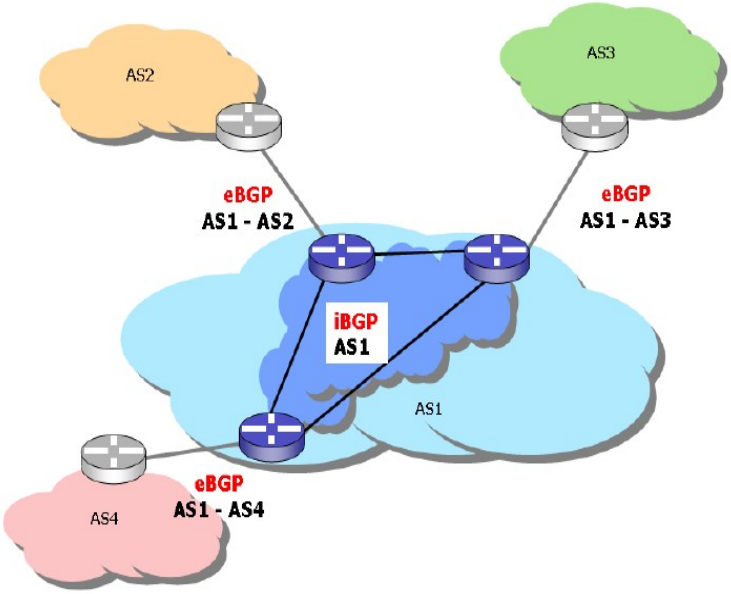
it is a router that communicate with outside for the opposite network, thus for internal router the router that communicate with external is border router for external networks the border router is called external router.

Intradomain routing

- Distance vector:RIP
- Link state:OSPF
- Hybrid: IRGP, EIRGP

Interdomain routing

- EGP:Characterized by 3 main features:
  - Neighbor acquisition
    - Verifies if there is a agreement to be neighbor.
  - Neighbor reachability:
    - Monitor neighbor connection.
  - Network reachability:
    - Exchange the information of the network.
- BGP (eBGP, iBGP):
  communications are reliable, errors detection is delegate at transport layer, the exchanged information is



- **CIDR classes**
  - **External BGP** sessions (eBGP), these connection
  - **Internal BGP** sessions (iBGP), these connection

Inside an autonomous system could

ARP

Address Resolution Protocol
Ethernet code type: **0x0806**
It does not provide mechanisms to authenticate responses.
The host sending a request trusts that the response will come from the legitimate owner of the IP address.
Keeps tracks of the response in cache.
Avoid using ARP before sending any packets. ARP entries are deleted after a due time.

ICMP
Internet Control Message Protocol
it is encapsulated directly into the IP, delivery is not guaranteed. It is used by many programs such as ping and trace-route.
ICMP data change OS by OS.

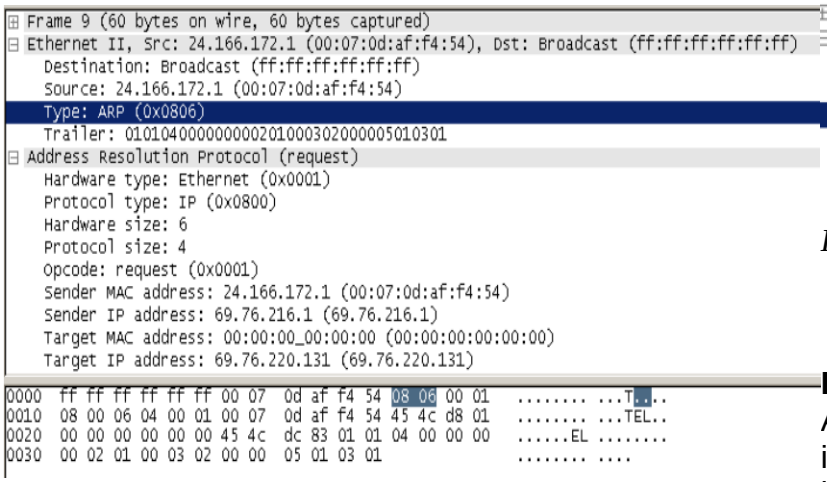


Figure 1: ARP

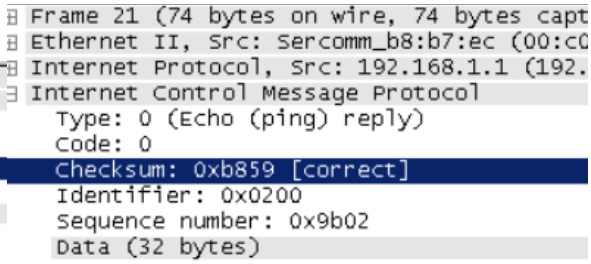
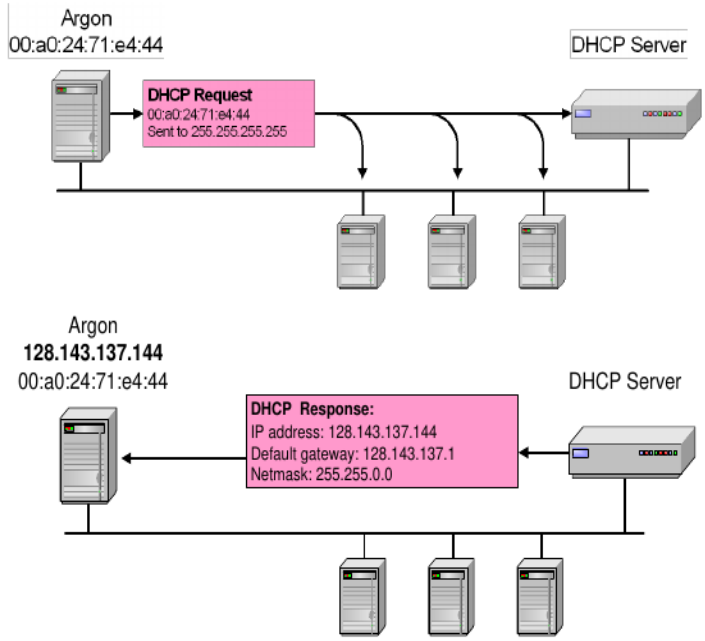


Figure 2: ICMP

IPv4
Address: it identifies a network interface (not a node) it has 4 byte of length. Address composition a.b.c.d

IPv6
high speed networks have fixed header length, another thing that has been removed is controls(checksum). The subnet-mask is removed.
This type of network improve the flow of the network, thus high speeds.
If transfer fails you must receive again the data, no problems because you have high speed network.
Devices can have multiple IPs

DHCP
it needs to assign dynamically the IP to the DTE.
It is a server. It can use reservation we can reserve ip for a defined MAC address.
It doesn't support multiple address for an interface. It cannot propagate



Dynamic IP assignment
3 protocols:
- RARP
- BOOTP
- DHCP

today only dhcp is used
bootp allows the boot of a machine
It assign ip to the machine, it detect
DHCP's ip has an expire date.
DHCP Messages

Note	Message Tyoe
Find DHCP server	DHCPDISCOVER
after response client can use ip	
Response to client, it is response of discover	DHCPOFFER
	DHCPREQUEST
	DHCPDECLINE
	DHCPACK
Sended by server if ip is already use	DHCPNAK
It need for renew the IP, it's sent when we are at 50% of ip's life	DHCPRELEASE
	DHCPINFORM

Transport level

The protocol has 8 bit in the package.

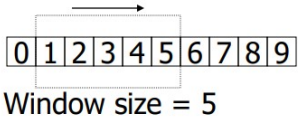
- **UDP User Datagram Protocol** IP field value=17
- **TCP Transmission Control Protocol** IP field value=6

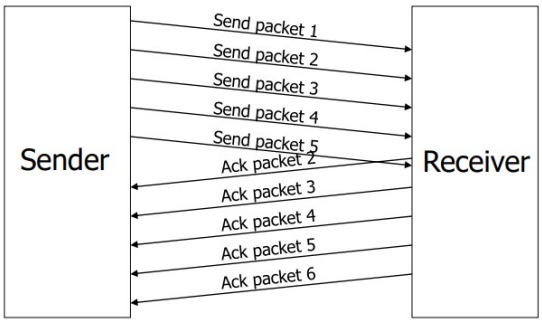
UDP is not reliable protocol, useful if we can allow packages missed. The protocol leaves the tasks to the applications if data is arrival order is correct, if data actually arrived a the destination, if data are not duplicated

TCP: sequence number needs to build the message in the right sequence acknowledgment number it represents the next package expected. Tcp if data are not receive properly, they will be resend.

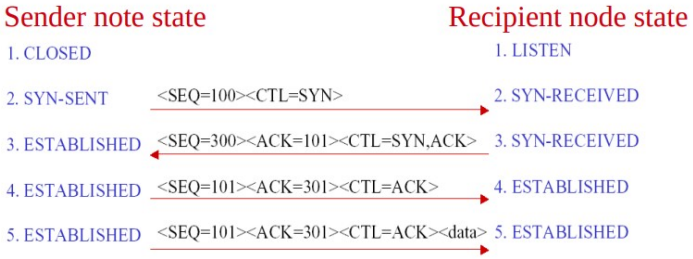
It use ACK to confirm right data.

- **Sliding Window**





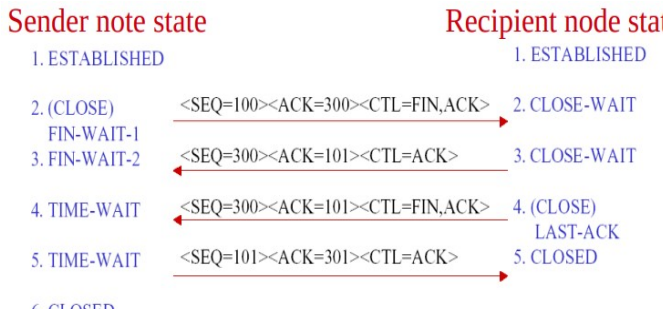
Open connection in TCP

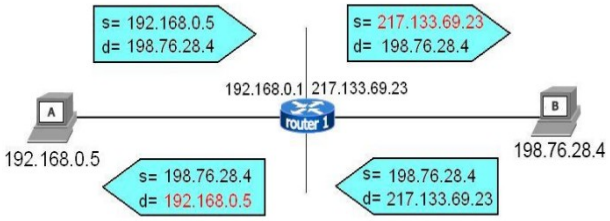


Through SYN request we create a session and when we open a connection, the connection is called **socket.**

A socket is formed by: ipHost:port ipLocal:port

Close connection





The first 1024 ports are reserved for standard server services, **but there are also server port over 1024**.
Networking address translation (NAT) it is a technique used to send data through internet, it uses a public ip to communicate outside of the network.
If I communicate with outside the other side doesn't see my private ip, but it read that request come from my router, the response will arrive to my router and it will route it to my device.
Port forwarding allow the exposition of a service to the internet, it says: if someone request something on public ip on a determinate port, route the request to the machine that provide that service.
A good practice is isolate servers from LAN (DMZ)
There are different types of NAT.
PAT or NAPT is NAT variation based on the used port number (Network Address and Port Translation).
If there are communication problems it is used NAT trasveral, STUN, ICE, TURN.

Security

Security components

- Reliable system architectures
- Data and information backup
- Firewalls
- Intrusion detection and prevention
- Virus and malware protection
- Encryption
- Authentication and authorization
- System's hardening: setup system properly, make system resilient
- Sandboxing
- VPN
- Auditing and assessment
- Monitoring and system control

Adequate contracts and SLAs (service level agreements), make contracts with other companies that provide external services.
all systems have errors, keep always informed.
USE redundant hardware components (HHD, Fans, Power Supply)→all these components have mechanical components in addition to electronic components.
UPS are hardware that allowed power continuity in case of blackout, can manage server power-off.
put disks in mirror, using RAID0, 2 disks put together 2 disks and see as once, no backup, not safe!!.

RAID

RAID=Redundant Array Of Inexpensive Disk
RAID1: 2 disks first as operative the second as backup , RAID 5 use n-1 disks for storage and the remain as backup, redundant is only 1 disk, if more than 1 disk breaks RAIDs stop working to avoid Spare Disk 1 disk as backup of RAID.
RAID 1 and 5 are used for the safety.
it's used for load balancing and fail over configuration.

Is very useful have hot-plug components.

Backup

know which data have to backup, how often, how long I keep backup(retention).
Do recovery test; backup can't save always from cryptolocker malware if properly set.
Recovery point Objective(RPO) represents the point in time where data is lost.
Recovery Time Objective (RTO) is very important estimate the downtime of the systems due to a data recovery.
It can be incremental or complete. It a good practice program backups

Firewall

there are 2 firewalls

- Network
- Personal

it separate LAN from public internet,
Firewall governs flow of data into and out of a LAN.
Firewall can manage DMZ networks.
DMZ is a zone where outside can access, we put here webserver for example. It is a network and it is managed by firewall.
Port forwarding is managed by firewall, it can route requests based on socket from outside inside firewall networks.
Firewall are based on rules.
A firewall protects a network if:

- is updated
- is well configured
- rules are correctly programmed
- all the traffic go through firewall

A firewall is just rule driven application.
It simply applies the programmed rules.
State full inspection firewall can put rules on all layers of OSI/IP stack, is useful to manage users
Note:
Mail server must be in the LAN, for law. Webserver with web mail will do proxy.
Mail client use mail proxy, it is like a webmail server but use smtp and imap protocol to communicate with client.

Intrusion Detection System: It listens network traffic and check If there are suspect actions, and alert if finds it. Port scanning is easy to detect because an user try connection to different services in a short time. (SNORT)

Intrusion Prevention System: It needs a firewall and edit rules to face attacks. It is not more used because it risks to lock services easily.

Cryptography

Symmetric key:

this type of encryption is faster, less complex, than public key.

Public key:

There are 2 keys a public key visible by everyone and a private key known only by user.
Sender send to User: Public key encrypt →User decrypt with his private key.
With symmetric key there is a problem of authenticity of origin.
Throw certification authority (C.A.) it certificates our identity and our activities in the communications.
Computer recognizes C.A. of certificates and if it knows the entity it considers it secure else it alert us that the certificate is not valid.

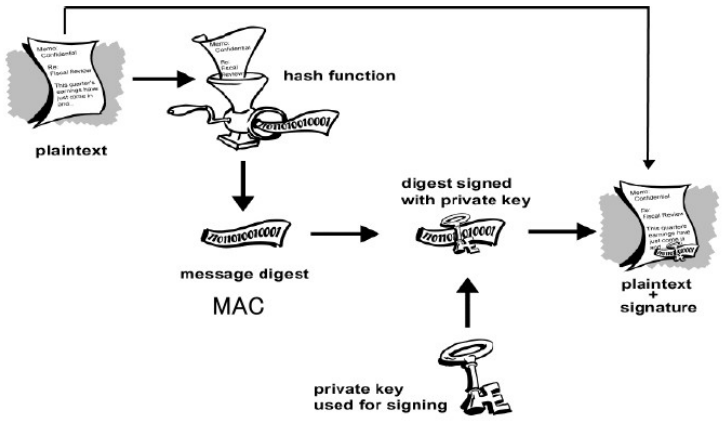
Key length

if the length of a key is long it is securer but it is longer to calculate.
Symmetric keys has short keys, asymmetric(public key) has long keys.
Symmetric is not adequate to manage multiple users.

Public key are slow.
Https mix symmetric and public keys, uses public to create communication channel then it use symmetric keys.

Hash functions

An hash function is a function that given an input it return a string that not permit go back, only one direction.
MD5 (vulnerable), SHA-1 and SHA-256 more secure.
To hack an hash we could create collision, giving random strings since we found the match.
Hash are used also for file integrity.



digital signature doesn't give confidentiality but certificates the origin and the integrity.
Receiver check the hash message with received message+signature.

Authentication and Authorization

There are 3 forms of credentials:

- something to have: Smartcard, token
- something to know: password, PIN
- something you are: fingerprint, retina scan, biometric information

Use 2 factors authentication is more secure.
Password should be:

- at least 8 mixed characters and numbers
- change periodically
- have timeout of attempts.

Authorization is the process when someone is authenticated.
Token are based on series number, server start from series number and an algorithm calculates the code generated by token. If token has a button there is a list of code that server expect that token generates.
Token are:

- highly accurate
- portable
- some are transferable
- all are revocable
- management systems may be expensive and complex

Biometric sensors are less accurate because of they are analogical measures, less accurate.
Typing characteristic it associates how you write something

VOIP

Transmission technology

Transport of signals via transmitting media.

Exchange technology

Supply of a transmission path between terminals by variable coupling of transmission mechanisms.

Terminal technology

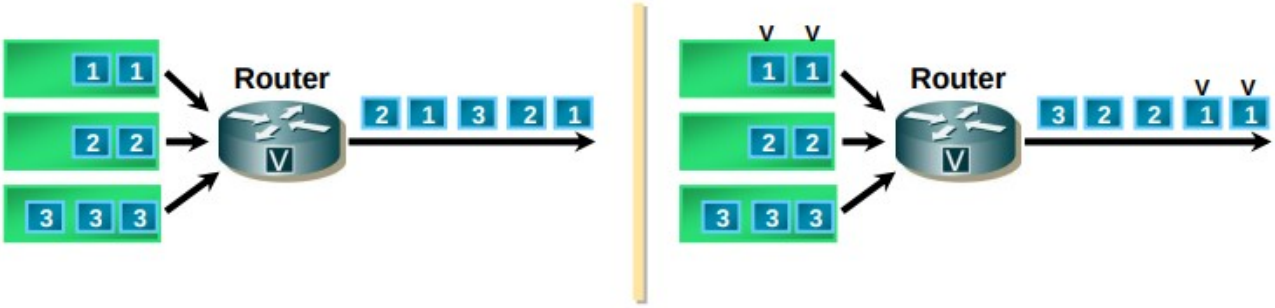
Technical mechanisms with the telecommunications participant: Input, data and signal preparation for the purpose of the transmission and switching, plus genuine rendition of the entered data if possible.

The sum of delay budget is given by the sum of: **fixed delay + variable delay**
analog ITU telephone channel, frequency 300 - 3400 Hz, range 3100 Hz, highest occurring frequency 3400 Hz
Scanning rate ITU-recommended sampling rate for PCM telephone digitization f A = 8 kHz
Scanning period T A = 1/f A = 1/8000Hz = 125 µs
The probably most important keywords concerning ISDN are:

- end to end digital connection
- integration of multiple services (voice-, data-, video-, multimedia transmission) • standard terminal interface: • S-Bus • 4 wire bus (3,4,5,6)

Summary of the steps sampling - quantization – coding

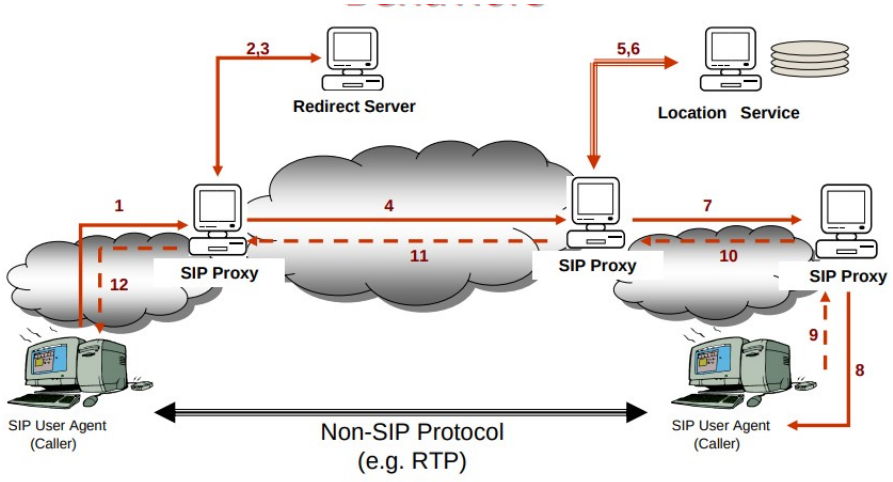
Telephone network components
SSP: Service Switching Point STP: Service Transfer Point SCP: Service Control Point
G.729 with 8 kbps we have the best quality,, needs 20 MIPS.
The compression is made using **vocoders**, that create the model of the voice.
Waveform coders works based on maths principles.
Hybrid coders works with both previous techniques and they have best quality.
Loss of packets
the quality of a call is determinate by the number of packets received.
The latency is acceptable only if the delay is in the range 0-150ms and 400 for intercontinental communication. Frames has delay.



Are present when the input data flow is higher than the output data flow capacity.
Possible solution: queuing with priority.
De-jitter: allows to have a constant delay between packets.
Delay Budget = Fixed Delay + Variable Delay
VOIP technology
SIP
it is an application layer signaling control protocol. It is the core protocol for initiating managing and terminating sessions in the internet.
To call someone we have to know internet address.
Example something@domain2.domain1
we have 2 agents:

- User Agent Client: UAC
  - initiates SIP requests
  - Acts as the user's calling agent
- User Agent Server: UAS
  - receive requests and return responses
  - Acts as the user-called agent

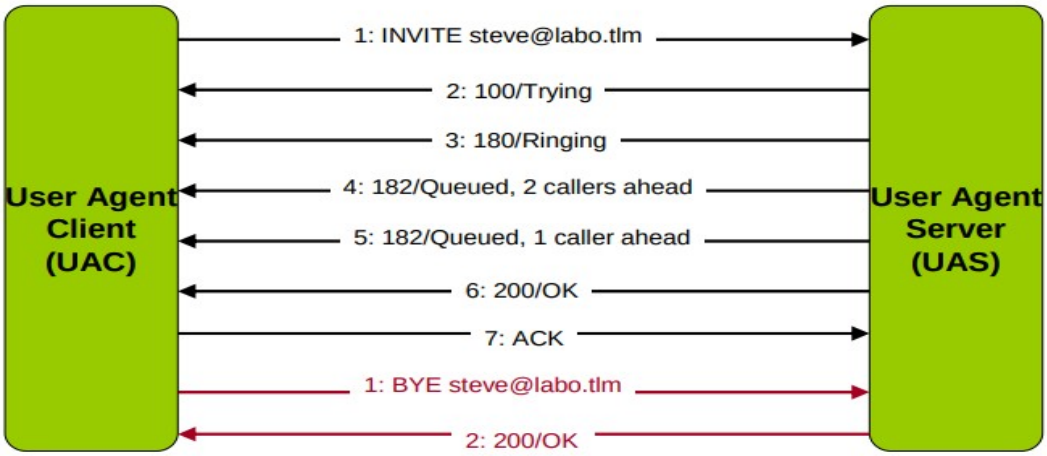
SIP port: 5060



-

The call works on RTP, secure version SRTP.
Red part are SIP requests/respones.

if we use few portion of band we doesn't have interference problems.



Security added section
Sandboxing
In IT: security mechanism to separate domains, where restricted environment is created and in which certain functions are prohibited • used in both PC and mobile environments • used when executing untested code or untrusted programs • e.g.: Unix implements two core sandboxes: at process and userid level • benefits in security: web navigation, test of new software, isolation of scratch space on disk and memory, limitation to network accesses, to inspect the host system or to I/O devices.
The 10 GOLDEN rules of security

- Error-free systems don‘t exist, systems can only be error tolerant.
- We shall always investigate the origin of the problems.
- Reduce manipulation errors through internal or external training.
- Limit as far as possible the possibility of misuse of the infrastructures.
- Perform periodical risk analysis and inform people accordingly.
- Define clearly how infrastructures shall be used and motivate these guidelines.
- Everybody shall accept the security rules.
- Security policies shall be motivated, not be based on drawbacks.
- The management is responsible for the security culture in a company.
- Satisfied employees are the best guarantee for quality & security

Network added section
Token Ring: per comunicare é necessario attendere un token libero (rete ad anello con passaggio del testimone), alternativaall'ethernetinizialmente token vuoto che percorre il cerchio, poi una determinata macchina lo prende e scrive il destinatario, la macchinadestinatarialolegge lo segna come letto e lo rimanda al mittente che avrà il compito di liberare il token. nel pacchetto token abbiamostart delimiteraccesscontrol end delimiter

Useful commands

Valid for MS WinNT system, Win2K, WinXP and following.

C:> ipconfig -all (systems: WinNT, Win2K, WinXP, Vista, ···)
C:> winipcfg (system WIN9x)
C:> ping 193.5.153.13
C:> tracert www.mit.edu
C:> arp -a
C:> netstat -an
C:> netstat -e
C:> netstat -r
C:> nslookup www.dti.supsi.ch

ifconfig ··· (UNIX systems)
traceroute ···

Show routing table on windows: netstat -r
arp command return the known devices
tracert command return routers that packet through
netstat -e return which port are listening

netstats -n Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
Netstats -a Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
Nslookup return domain information

FRAME STRUCTURE

Tabella riassuntiva formato frame

Layer 2
ethernet

8 byte	6 byte	6 byte	2 byte	46 -1500 byte	4 byte
Preambolo	Indirizzo destinazione	Indirizzo sorgente	Tipo frame	Dati	CRC

Layer 3
IP

32 bit

4-bit version	header length	8-bit TOS	16-bit total length
16-bit identification		3-bit flag	13-bit fragment offset
8-bit TTL	8-bit protocol	16-bit header checksum	
32-bit source address			
32-bit destination address			
options (if any)			
data			

20 byte header

Layer 4
UDP - TCP

0 — 32 bit — 31

16-bit source port	16-bit destination port
16-bit UDP length	16-bit UDP checksum
Data	

8 byte

0 — 32 bit — 31

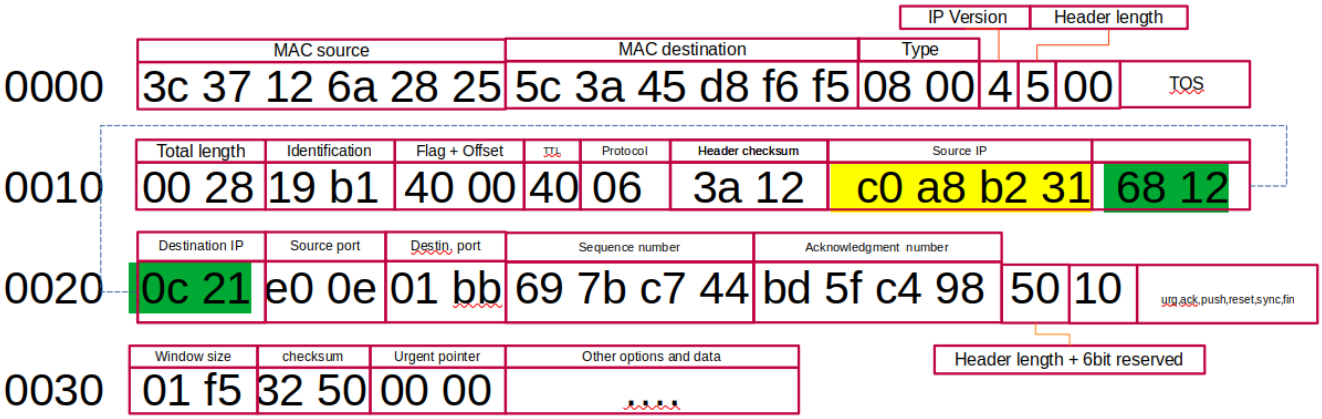
16-bit source port								16-bit destination port	
32-bit sequence number									
32-bit acknowledgment number									
Header length	6-bit reserved	URG	ACK	PSH	RST	SYN	FIN	16-bit window size	
16-bit TCP checksum								16-bit urgent pointer	
options									
data									

20 byte

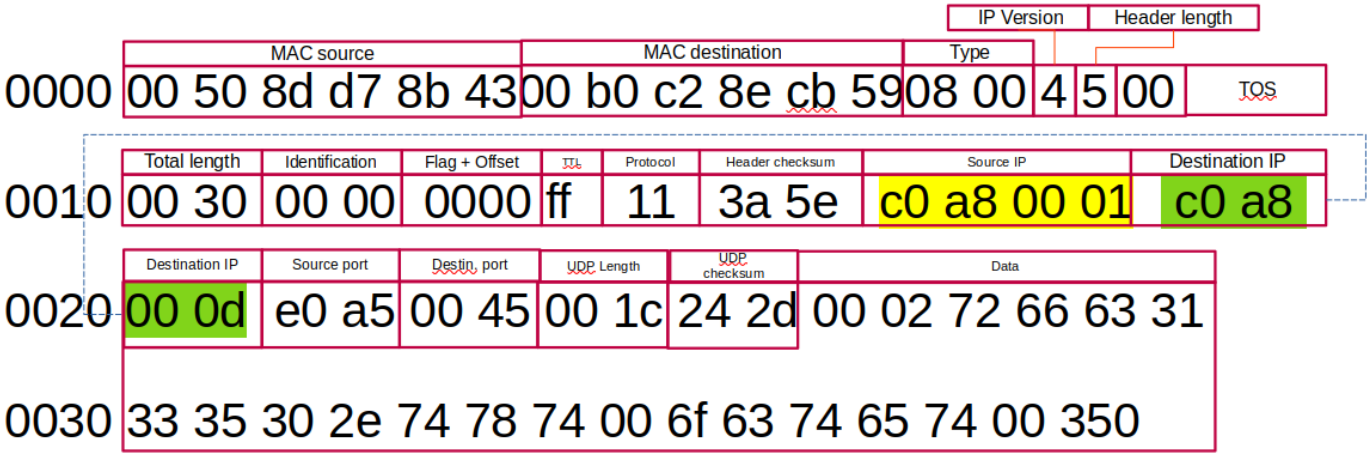
General

	IP Version	Header length																			
	MAC source						MAC destination						Type								
0000	5c	3a	45	d8	f6	f5	3c	37	12	6a	28	25	08	00	4	5	00	TOS			
	Total length		Identification		Flag + Offset		TTL	Protocol	Header checksum		Source IP				Destination IP						
0010	00	54	00	00	00	00	74	01	90	31	8e	fa	b4	a3	c0	a8					
	Destination IP		(some bytes if there are options, other protocols and data) this is ICMP.....																		
0020	b2	31	00	00	bc	b0	00	01	00	05	64	2a	b4	62	00	00					
0030	00	00	60	e9	0b	00	00	00	00	00	10	11	12	13	14	15					
0040	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25					
0050	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35					
0060	36	37																			

TCP



UDP



Lista Acronimi

ARP:addres resolution protocol, invio del messaggio in broadcast a tutti i dispositivi nella rete, chiedendo15 chi a l'indirizzoipchecerco,tuttiloignoreranno tranne la macchina con l'ip interessato
ANSI:American National Standards Institute
ATM:asynchtonous transfer mode, BGP:Border gateway protocol
BOOTP: BOOtstrap Protocol l'host puo' configurare i parametri ip a boot time
DNS:Domain Name System
DTE:(data terminal equipement)qualsian^si dispositivo che svolge la funzione di sorgente o destinazione di una cominicazionedati DCE(datacomunicatione equipement), attrezzatura di comunicazione. EIA:Electronic Industries Association
EIGRP:Enhanced Interior Gateway Routing Protocol: protocollo basato sulla combinazione di vettore di distanza e link stateinformation,max224 hop evoluzione di IGRP

EGP:exterior gateway protocol:primo protocollo usato per comunicare., caratterizzato da acquisizione dei vicini, monitoraggiodei
vicini,scambio di info
FTP: file transfer protocol, necettita di 2 porte per funzionare, TCP 20 per il trasferimento dei file, **TCP** 21 per il controllo. il protocollosicuroéSFTP. FDDI: fiber distributed data interface
IPv4:32 bit 2^23 bit
IPv6:128 bit per lo spazio di indirizzamento,esadecimale
ISO:International Organization for Standardization(ISO), es:OSI model
IEEE:Institute of Electrical and Electronic Engineers
IAB: Internet Architecture Board {e.g. TCP/IP, SNMP}
IETF: Internet Engineering Task Force (The IETF is supervised by the Internet Society Internet Architecture Board (IAB)
IANA:Internet Assigned Numbers Authority
ITU-T: International Telecommunication Union Telecommunication Standardization Sector, also known by its old name CCITTICMP: Internet control message protocol, protocollo per la diagnostica di base delle reti, ad esempio la raggiungibilità di unhost ecc. essoprevede una serie di codici di controllo (0 destination network unrichable, 1 destination host unrichable, 2 detination protocol unrichable,3destination port unrichable,...), usato da ping(testare raggiungibilità e latenza, echo request ed echo replay) e traceroot(serveatracciareilcammino dei pacchetti, da un host A ad un B, per ogni host /router ci dà l'indirizzo IP dell'intermediario e ci ridà l'IP), il protocolloICMPdeveessere abilitato altrimenti non si ricevono risposte. IMAP:(internet message acess protocol) consulta la casella mail direttamente dal server
IGMP:Interior Gateway Routing Protocol: supporta più metriche per ciascun percorso: larghezza di banda, carico di linea, ritardi eaffidabilità;Numero massimo di hop: 255, Nasce per superare la limitazione del protocollo RIP (hop massimo: 15) Protocollo proprietario(CISCO)LLC:logical linck control
NAT:network adress traslation, traduzione dell'ip locale in un ip publico,per permettere la circolazione su internet, a livello4ceinpiùilnumero di porta e viene aggiunto il PAT(port addres traslation)o port forwarding.
RARP:reverse address resoluton protocol, simile al arp, manda una richiesta ad un ip , associato ad uno specifico mac address
SLIP:serial line internet protocol, considerato il protocollo point-to-poit d'origine per il traffico **TCP/IP, a**dotta un particolarecaratteredifine0x0C, protocollo specificato in RFC(max 1066 bytes) **TFTP:Trivial File Transfer Protocol (TFTP)** è un protocollo di trasferimento file di livello applicativo molto semplice, con le funzionalità di basedel FTP
WLAN WEP:wireless equivalent privacy, usa RC4 encription per la sicurezza CRC-32 per l'integrità
WPA:WIFI protocol acess, criptato con RC4. 128 bit key 48 bit d'inizialization vector
WPA2:WPA+AES(advance encryption standard) 128bit