Linux Day Torino
26 ottobre 2024

Come funziona la rete?

Massimo Nuvoli

Mi presento

- Architetto di Sistemi
- Lavoro per me stesso, Progetto Archivio SRL, Dicobit
- Trainer certificato in ambiente tecnico

e …

- Co-fondatore di Adenda SRL (CTO)
- Co-fondatore di Aibeex SRL (CTO)

  Provider di infrastrutture di rete, con il primo datacenter innovativo a Torino

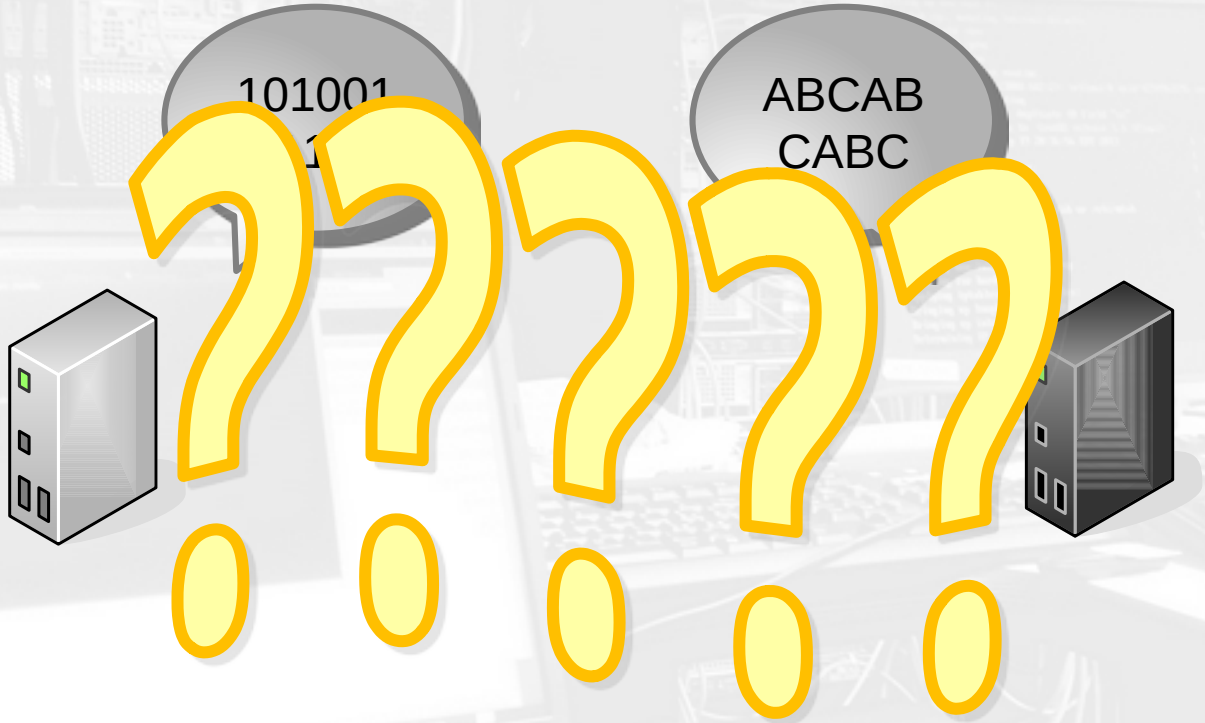

ma anche...

Introduzione al networking

- basi della comunicazione
- connessione fisica
- connessione logica
- connessione tra reti
- reti “speciali”

Basi della comunicazione

Basi della comunicazione

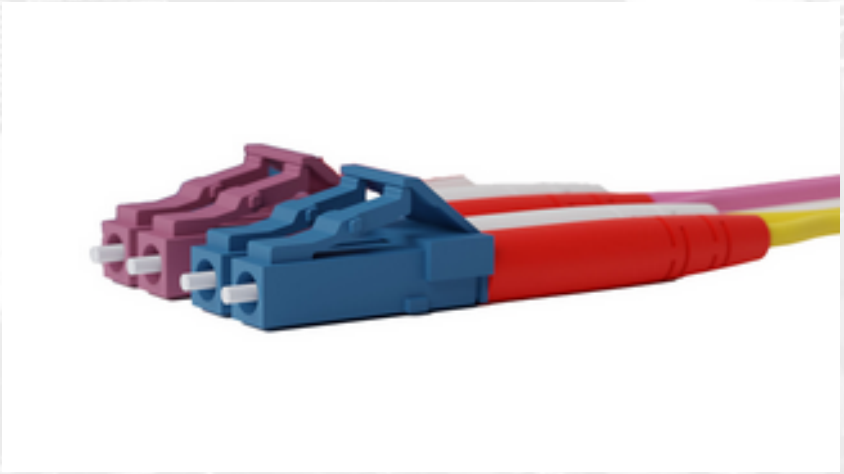


Scomporre per semplificare

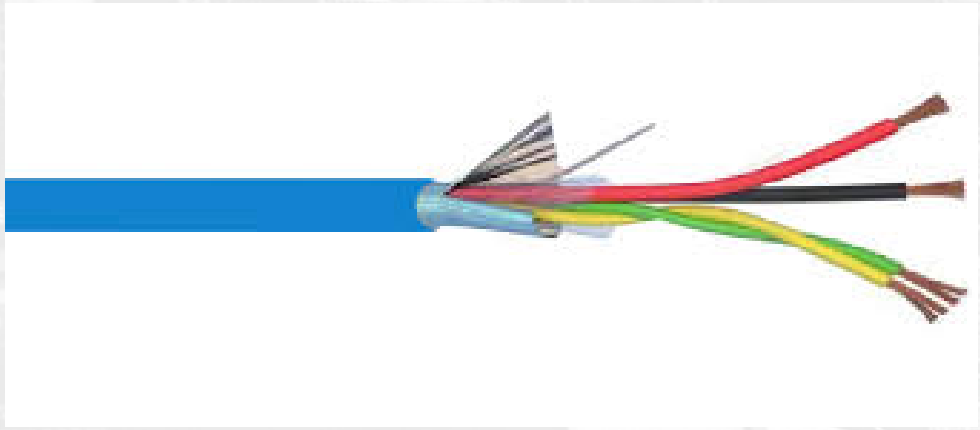
Connessione Fisica

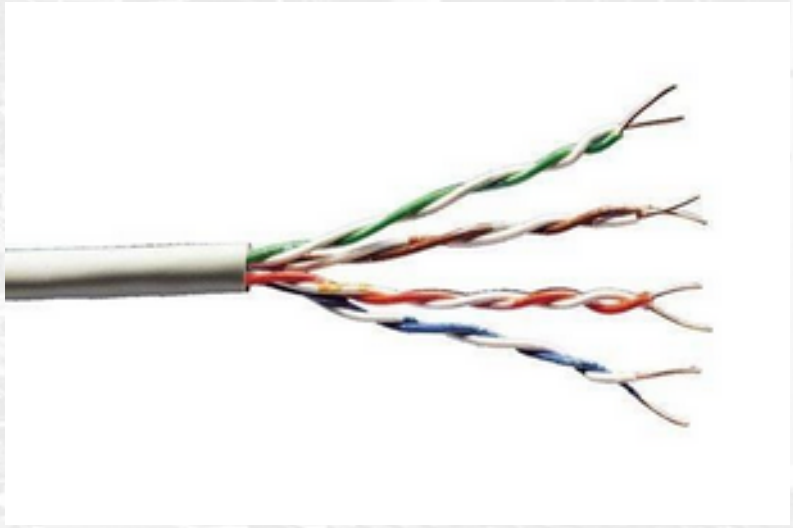
- cavi
- connettori
- fili
- ma anche “onde radio”
- la luce
- meccanica
- etc.. etc..

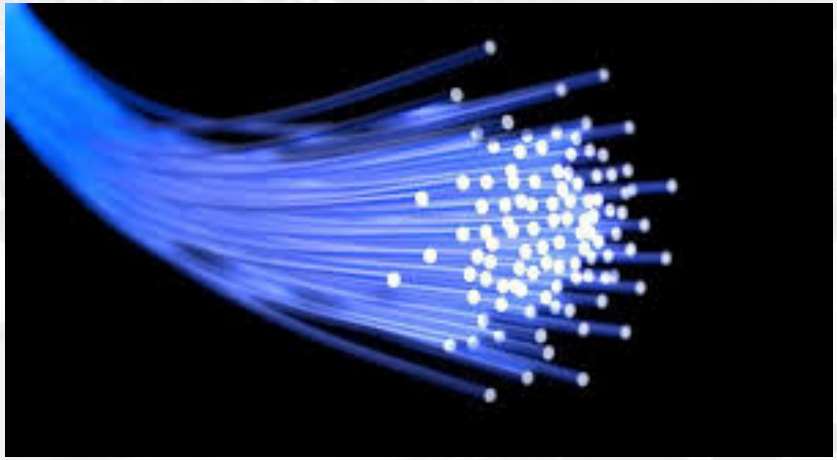
Connessione Fisica



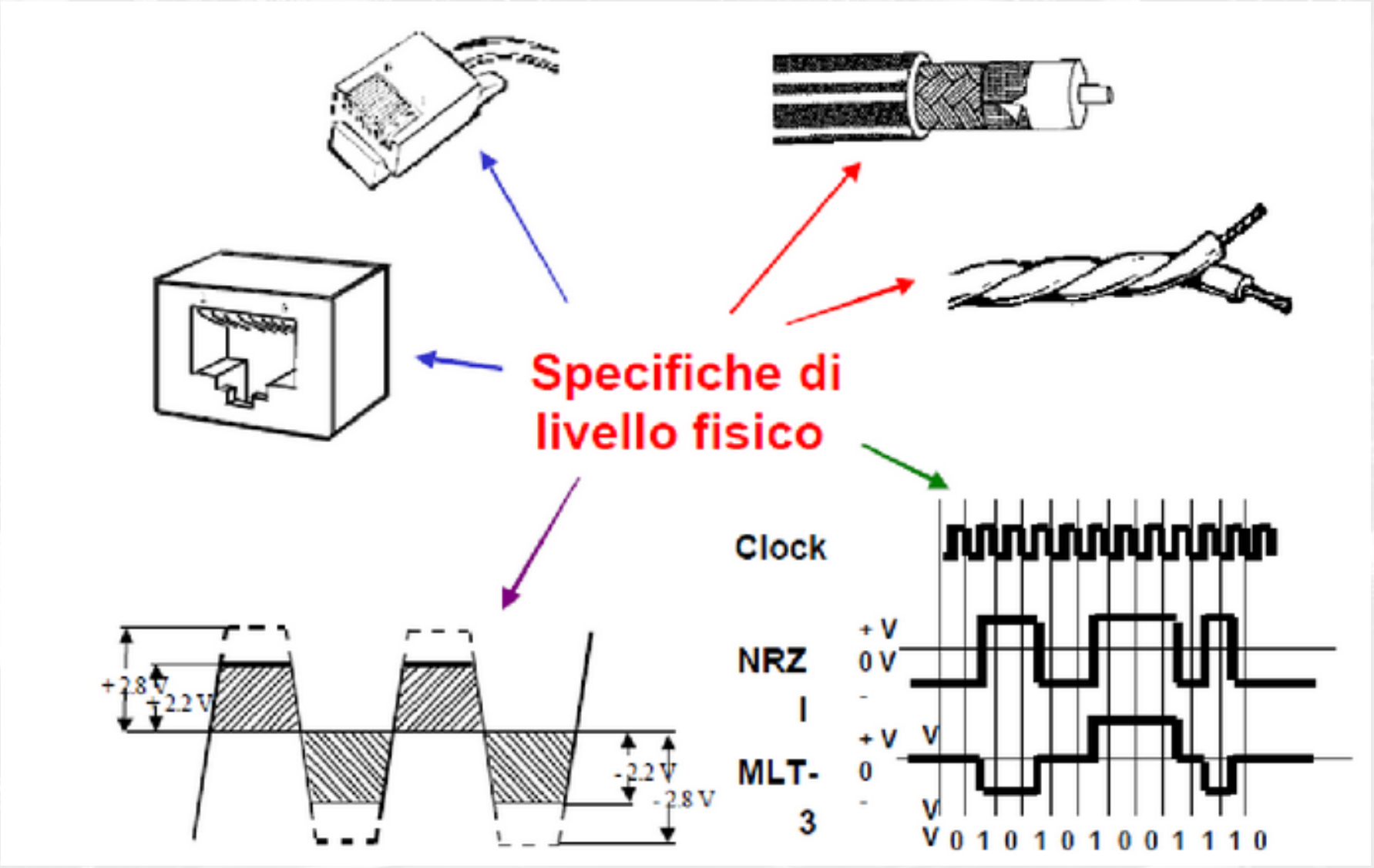
Connessione Fisica



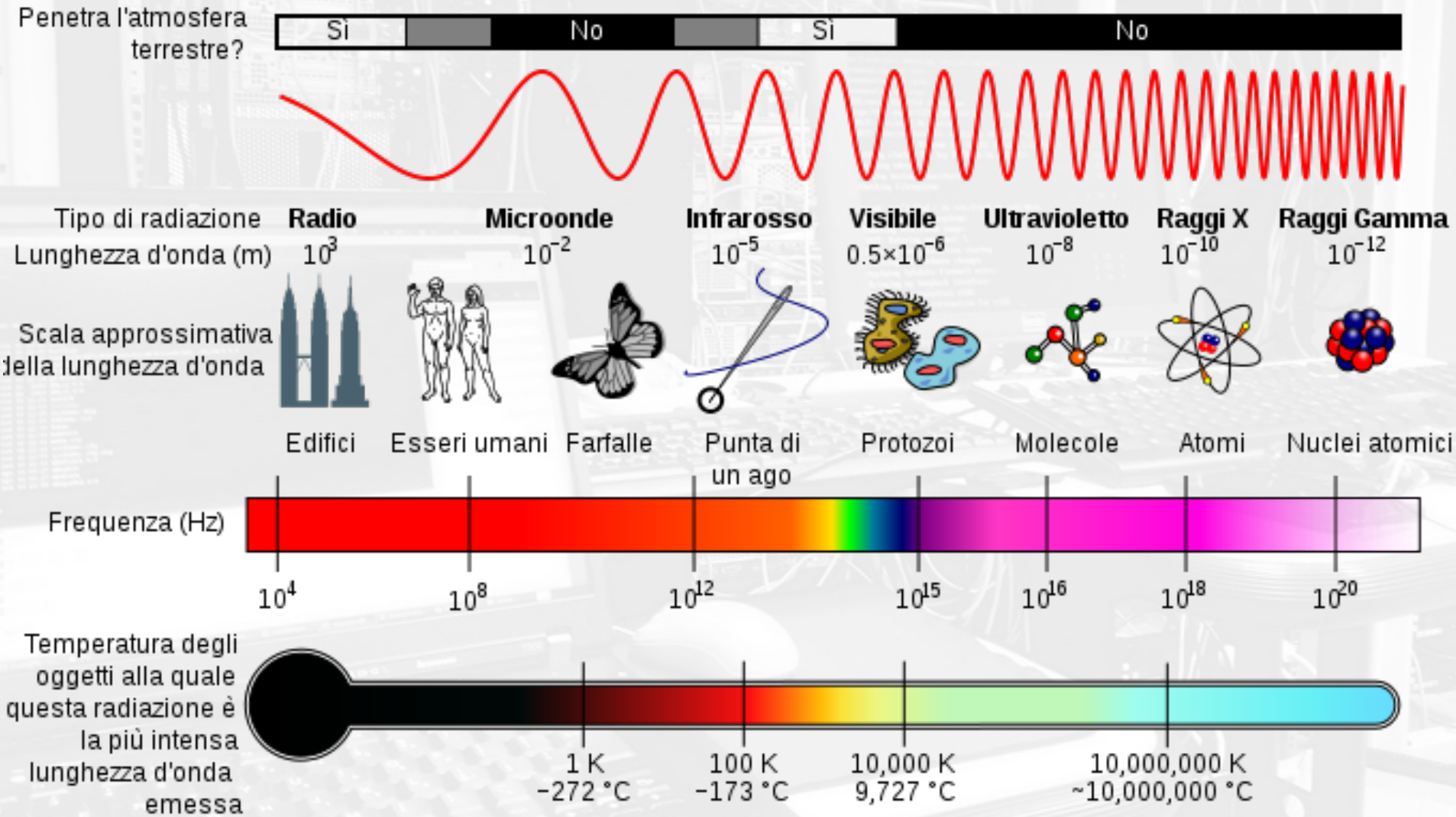




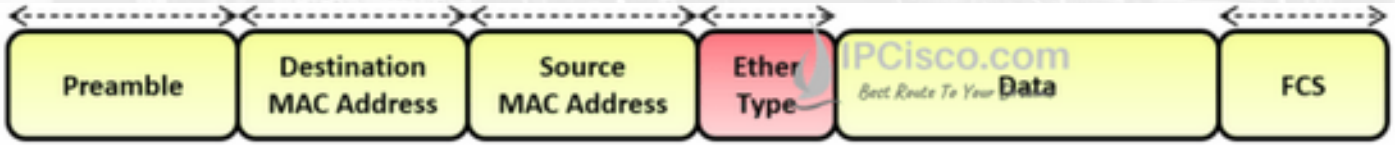
Connessione Fisica



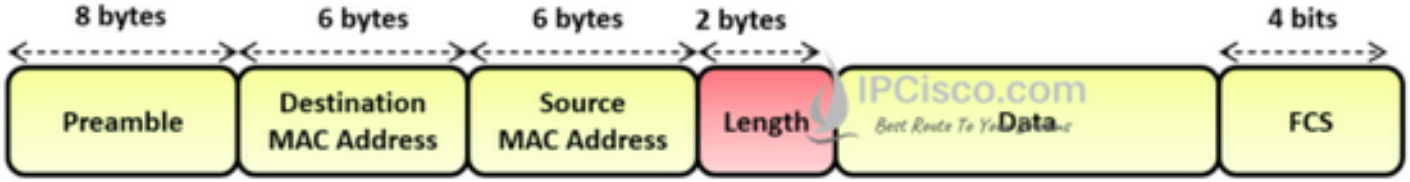
Connessione Fisica



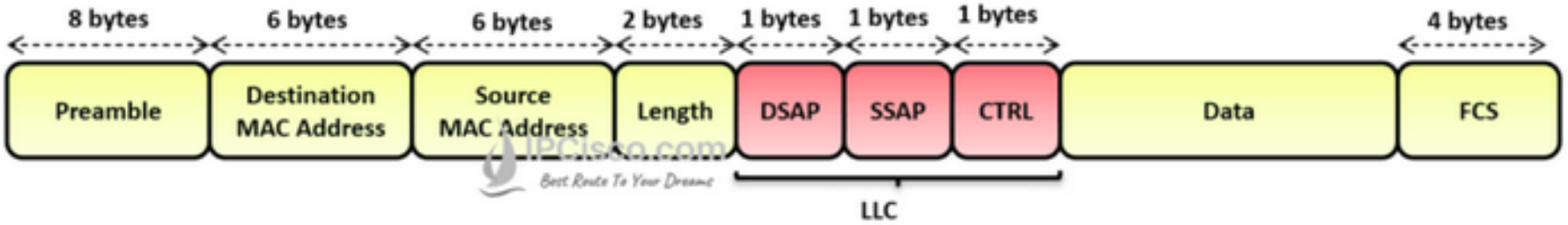
Collegamento Dati Cavo



IEEE 802.3 Frame

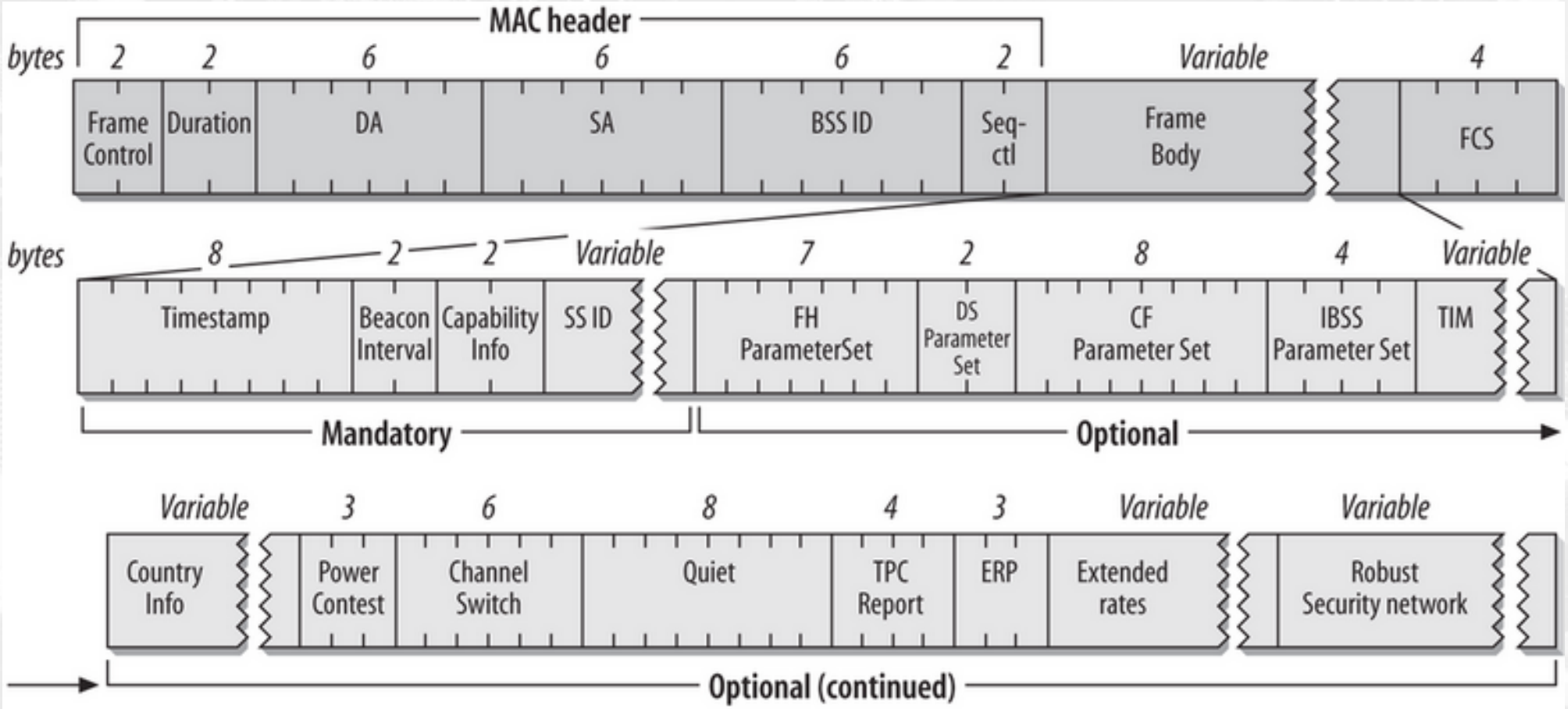


IEEE 802.3 Frame with LLC

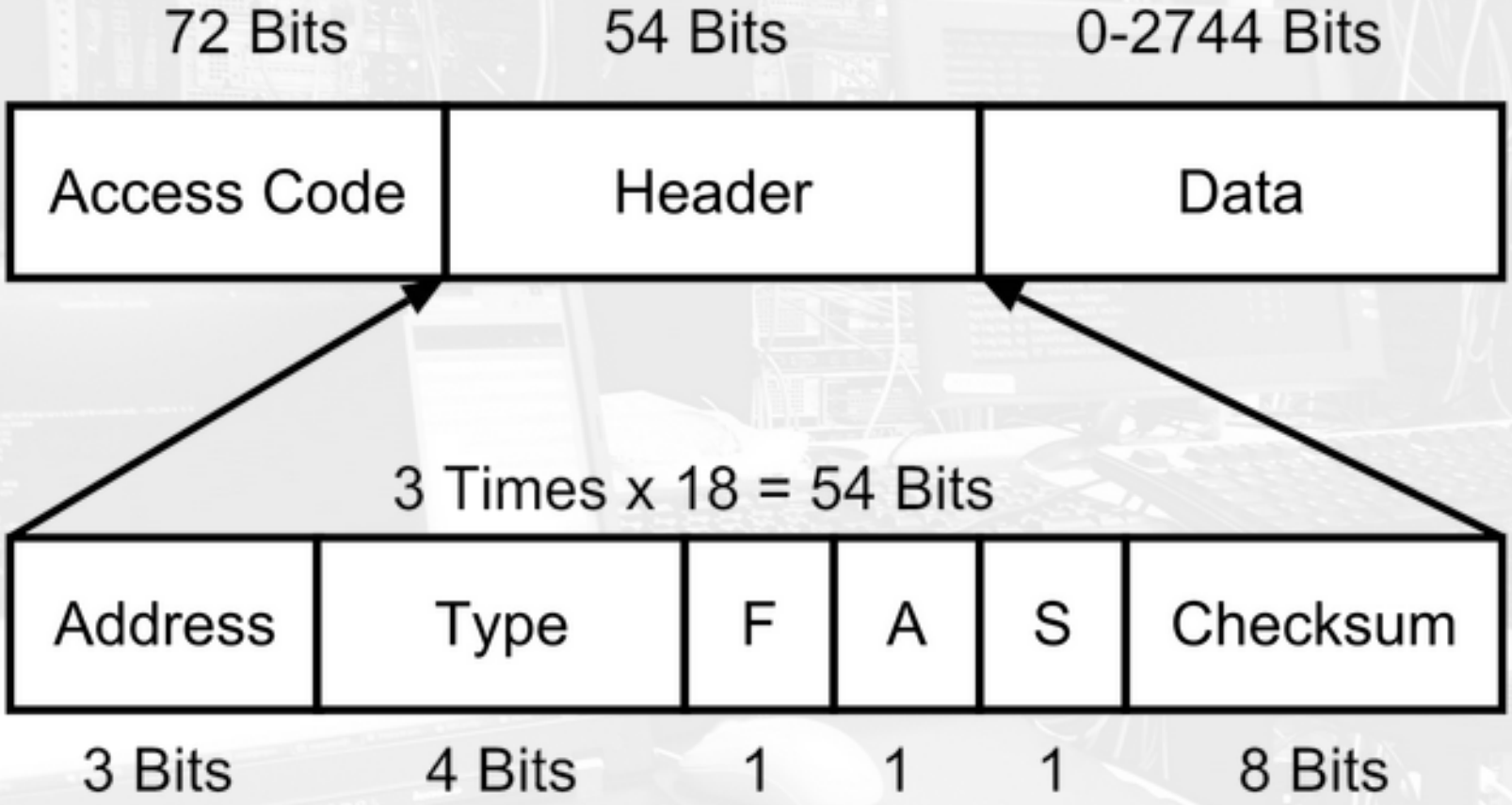


IEEE 802.3 Frame with LLC/SNAP

Collegamento Dati Wireless



Collegamento Dati Bluetooth



Bluetooth Frame Format

Chi determina la velocità della connessione?

- La velocità della connessione dipende prima di tutto dal livello L1
- Subito dopo si va su L2, dove possono intervenire tutti i meccanismi possibili, ma esiste una sola grande verità, in un dialogo tra macchine l'unica che può intervenire sulla velocità è quella che trasmette

Rete → Mac Address

- Indirizzo fisico di ogni punto di rete
- Notazione Esadecimale
- 1 2 3 4 5 6 7 8 9 0 A B C D E F
- XX:XX:XX:XX:XX:XX
- Vale solo per Ethernet e affini
- Gli id di altri mezzi sono differenti!!!
- Lo spazio è diviso per “vendor” ed è già “pieno” (tecnicamente 2^48 ma data la suddivisione in OUI e in multicast/unicast e local o global)

MAC-ADDRESS

- FF:FF:FF:FF:FF:FF

  é l'indirizzo di broadcast che raggiunge “tutti” coloro che sono collegati sulla rete

- Il mac address è diviso in due parti

  AA:AA:AA e BB:BB:BB

  AA:AA:AA si chiama OUI e rappresenta l'azienda o organizzazione a cui appartiene il MAC

  BB:BB:BB è il NIC e rappresenta l'identificativo univoco (per quel OUI) di ogni singola scheda di rete

- Una parte degli OUI è riservata agli OUI locali e una parte agli OUI “multicast”

MAC-ADDRESS e sicurezza

- Sebbene sia frequente l'uso del MAC-ADDRESS per rendere sicura una rete non va fatto
- Cambiare l'indirizzo fisico di una scheda di rete è strafacile
- In alcuni casi (ad esempio per aumentare la privacy) viene fatto di proposito per impedire la tracciabilità anche del dispositivo hardware

Saliamo di un livello, IP

- Con la rete che è in grado di comunicare a livello L2 possiamo iniziare a scambiarci messaggi ma succederebbe solo all'interno della rete stessa, e con indirizzi “che dipendono dall'hardware”
- Per ovviare e per aumentare l'astrazione ecco che si passa ad utilizzare un protocollo che si chiama “Internet Protocol”
- Ha il compito di indirizzare ed instradare i pacchetti anche in ambiti più complessi della rete locale

IPv4 e IPv6

- Oggi vedremo prevalentemente IPv4 ma esiste anche una versione aggiornata che si chiama appunto IPv6
- Rispetto IPv4 IPv6 permette di indirizzare più dispositivi e di creare reti più complesse, con minore difficoltà
- La “logica” di funzionamento è praticamente identica, ma essendo fisicamente incompatibile l'implementazione di IPv6 è totalmente distinta rispetto a quella di IPv4, tecnicamente si dice “dual stack” ovvero nulla della rete IPv4 viene utilizzato per IPv6 (e viceversa) con le dovute eccezioni

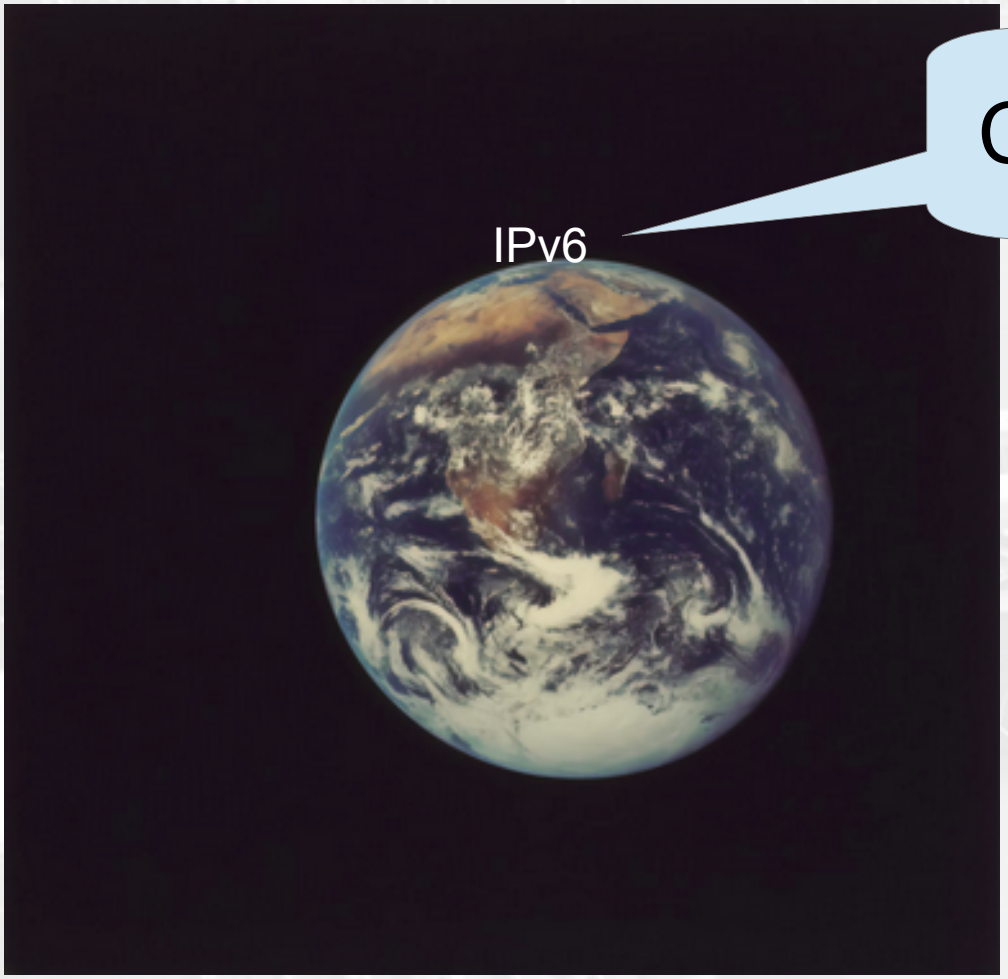
IPv4

- Gli indirizzi IPv4 sono composti da quattro numeri che vanno da 0 a 255 (questo perchè sono 8 bit)
- Il numero massimo di indirizzi possibili è quindi pari a 2^32 ovvero circa 4,3 miliardi di indirizzi
- In realtà molti di questi vanno “persi” per motivi disparati, indirizzi riservati, indirizzi di rete, indirizzi particolari etc. etc. etc.
- Il protocollo IPv4 ha 43 anni (1981) ed è uno dei protocolli più diffusi, più utilizzati e più sicuri a livello mondiale, lo dimostra la sua età
- Da tempo gli indirizzi pubblici IPv4 sono terminati e si spinge per l'adozione su larga scala del successore IPv6

IPv6

- Gli indirizzi IPv6 sono composti da 128 bit
- Il numero massimo di indirizzi possibili è quindi pari a 2^128 ovvero circa 3,4 * 10^38 indirizzi
- Il protocollo IPv6 è anche lui vecchiotto, ha 36 anni (1988) ma la sua adozione è stata ostacolata da differenti problematiche, per poi tornare in auge a seguito della fine della disponibilità degli indirizzi pubblici IPv4
- Considerando la totale superficie della terra esistono 0,000007 indirizzi IPv4 per metro quadro, mentre esistono circa 655 triliardi di IPv6 per metro quadro.

IPv6



IPv4 nel dettaglio

- Indirizzo composto da quattro numeri da 0 a 255
- L'indirizzo è composto da due parti, una che è la rete una che è l'indirizzo del dispositivo nella rete
- Tecnicamente si contano i bit nella prima parte dell'indirizzo per la rete, i restanti saranno i bit dell'indirizzo locale
- Per indicare questa cosa si scrive la “maschera” della rete ovvero ad esempio 255.255.255.0 che sono 24 bit a 1, i restanti 8 saranno gli indirizzi della rete locale

IPv4 nel dettaglio

Binary Mask	Prefix Length	Subnet Mask
11111111 00000000 00000000 00000000	/8	255.0.0.0
11111111 10000000 00000000 00000000	/9	255.128.0.0
11111111 11000000 00000000 00000000	/10	255.192.0.0
11111111 11100000 00000000 00000000	/11	255.224.0.0
11111111 11110000 00000000 00000000	/12	255.240.0.0
11111111 11111000 00000000 00000000	/13	255.248.0.0
11111111 11111100 00000000 00000000	/14	255.252.0.0
11111111 11111110 00000000 00000000	/15	255.254.0.0
11111111 11111111 00000000 00000000	/16	255.255.0.0
11111111 11111111 10000000 00000000	/17	255.255.128.0
11111111 11111111 11000000 00000000	/18	255.255.192.0
11111111 11111111 11100000 00000000	/19	255.255.224.0
11111111 11111111 11110000 00000000	/20	255.255.240.0
11111111 11111111 11111000 00000000	/21	255.255.248.0
11111111 11111111 11111100 00000000	/22	255.255.252.0
11111111 11111111 11111110 00000000	/23	255.255.254.0
11111111 11111111 11111111 00000000	/24	255.255.255.0
11111111 11111111 11111111 10000000	/25	255.255.255.128
11111111 11111111 11111111 11000000	/26	255.255.255.192
11111111 11111111 11111111 11100000	/27	255.255.255.224
11111111 11111111 11111111 11110000	/28	255.255.255.240
11111111 11111111 11111111 11111000	/29	255.255.255.248
11111111 11111111 11111111 11111100	/30	255.255.255.252
11111111 11111111 11111111 11111110	/31	255.255.255.254
11111111 11111111 11111111 11111111	/32	255.255.255.255

IPv4 indirizzi “speciali”

- In ogni “sottorete” ci sono due indirizzi speciali:
  - uno che identifica la rete stessa, con la parte di indirizzo finale tutta a zero.
  - uno che identifica tutti gli indirizzi della rete stessa e si chiama broadcast, con la parte di indirizzo finale tutta a 1
- Esempio:
  - 192.168.1.5/24 (255.255.255.0) ovvero
  - rete 192.168.1.0
  - broadcast 192.168.1.255

IPv4 ma ci sono anche le reti “speciali”!

- indirizzi zero → 0.0.0.0/8
- indirizzi ip privati 10.0.0.0/8
- indirizzi localhost 127.0.0.0/8
- indirizzi link local 169.254.0.0/16
- indirizzi per documentazioni ed esempi 192.0.2.0/24
- indirizzi ip privati 192.168.0.0/16
- indirizzi ip multicast 224.0.0.0/4
- indirizzi ip riservati 240.0.0.0/4

IPv4 indirizzamento sottoreti

- in ogni dispositivo possono essere indicati degli indirizzi di rete ed i corrispettivi indirizzi a cui devono essere “girati”
- Saranno quindi delle coppie di indirizzo rete/indirizzo IPv4
- ad esempio 0.0.0.0/0 → 192.168.0.1 indica che la rete deve essere girata verso il 192.168.0.1
- la rete 0.0.0.0/0 si chiama “default” ed è la rete più grande possibile, il 192.168.0.1 si chiamerà gateway, in questo caso default gateway
- In caso di più rotte prevale l'indirizzamento di quella più piccola, ovvero quella che ha l'indirizzo di rete più grande.

IPv4 indirizzamento sottoreti

- Se il mio ip è 192.168.1.21/24 e il mio gateway è il 192.168.1.1 qualsiasi indirizzo che io cerco di raggiungere al di fuori della mia rete 192.168.1.0/24 dovrà passare dal gateway stesso.
- Si... ma come faccio a raggiungere il gateway, ne manca un pezzoooooo

IPv4 ARP

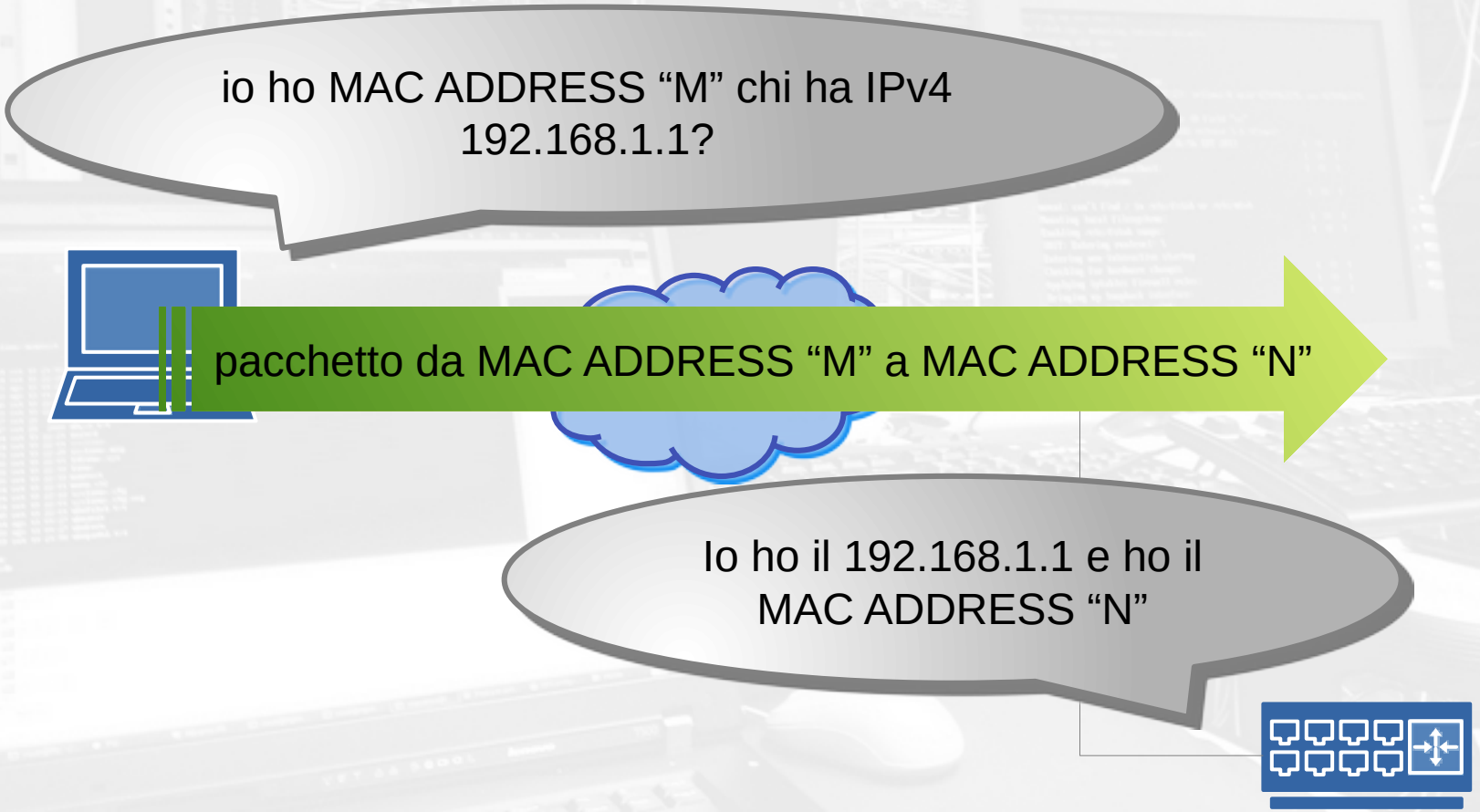
- Prima ci siamo fermati agli indirizzi MAC fisici delle schede di rete, come si passa dall'indirizzo IPv4 al MAC?
- Usando il protocollo ARP (Address Resolution Protocol)

  un dispositivo chiede alla rete locale “chi ha l'indirizzo ip?” e il dispositivo che quell'indirizzo ip risponde “io!”
- A questo punto mettiamo tutto insieme...

IPv4 esempio ARP

- Un dispositivo con MAC ADDRESS “M” e indirizzo 192.168.1.22/24 vuole contattare il gateway che ha indirizzo 192.168.1.1/24 e MAC ADDRESS “N”
- Alzerà la mano tramite ARP e chiederà: “chi ha l'indirizzo 192.168.1.1?”, il gateway risponderà “io! comunicando il proprio MAC ADDRESS “N” al dispositivo.
- A questo punto e solo questo potrà viaggiare un pacchetto a livello L2 da “M” a “N”
- Ovviamente succederà l'identica cosa al contrario!

IPv4 esempio ARP



IPv4 ip “automatico”

- Ma se io collego un dispositivo in rete, come faccio a fare si che si configuri da solo?
- Ci sono due metodi:
  - DHCP
  - APIPA
- Il funzionamento dei due è radicalmente differente, per semplicità saltiamo APIPA che assegna indirizzi locali del tipo 169.254.0.0/16 basandosi solo su “evitiamo il conflitto” da evitare come la peste

IPv4 APIPA

- Automatic Private IP Address (indirizzi Local Link)
- Assegna un indirizzo IPv4 in modo pseudo casuale
- Prima di utilizzare l'eventuale indirizzo casuale viene fatta una richiesta ARP per evitare un conflitto
- Se vi è un conflitto si riparte con la generazione dell'indirizzo casuale e quindi ARP
- Con APIPA non viene assegnato nè il DNS nè il gateway, quindi sono indirizzi locali

IPv4 APIPA quello che non vuoi

- Quando ci sono impostati DHCP e/o indirizzi IP statici ma andando a vedere l'indirizzo è APIPA allora siamo nei guai
- Significa che c'è un conflitto o qualcosa che non va
- Lo fanno solo i sistemi operativi che sono abilitati
- Ad esempio NON lo fa GNU/Linux se non specificamente indicato.
- Lo standard teoricamente evita APIPA se è possibile utilizzare indirizzi IPv4 validi.

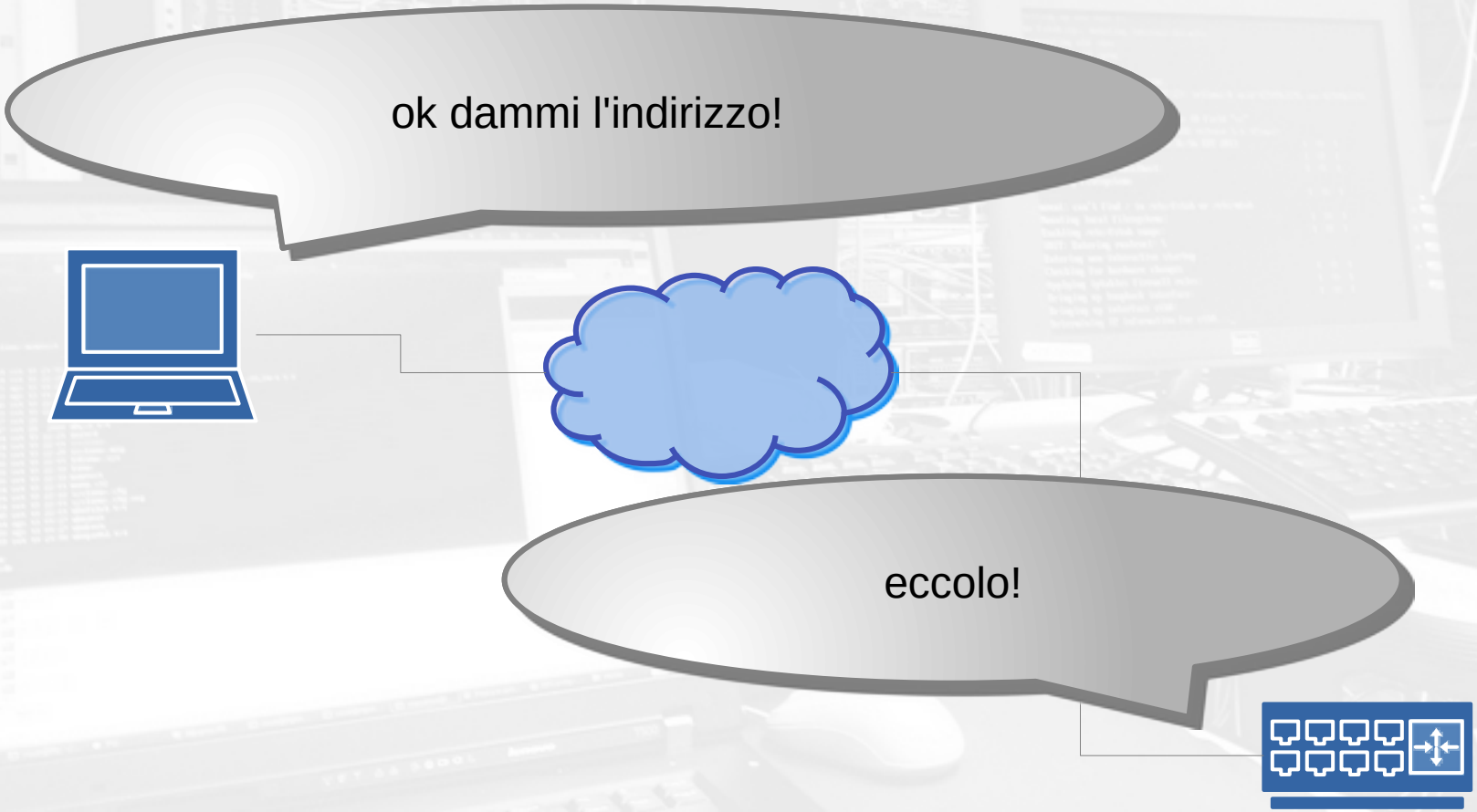
IPv4 DHCP (parte 1)

- Dynamic Host Configuration Protocol
- E' un protocollo client-server, ovvero c'è da qualche parte nella rete un “server” che eroga il servizio e i client lo contattano per avere quello che serve
- Il client usa un messaggio di tipo “broadcast” richiedendo alla rete “chi ha un indirizzo da darmi?” questo si chiama “discover”
- Il server vede la richiesta e risponde “Io!” dando i parametri al client, questo si chiama “offer”

IPv4 DHCP (parte 2)

- A questo punto più di un server DHCP potrebbero aver dato risposta al client (è previsto), per cui il client ancora una volta deve mandare un messaggio al server DHCP richiedendo l'indirizzo ip, questa si chiama “request”
- Solo a questo punto il server DHCP risponde con un messaggio di tipo “ack” che significa acknowledge. passando al client tutti i dati della configurazione aggiornata
- Periodicamente il client richiede al server DHCP l'indirizzo e il server DHCP deve rispondere sempre con “ack”, in questo modo gli indirizzi non sono assegnati permanentemente

IPv4 esempio DHCP



IPv4 DNS

- Si ma perchè io scrivo “www.google.it” e tutto magicamente funziona?
- Esiste un protocollo client-server anche per la risoluzione dei nomi ovvero per convertire il nome “www.google.it” in un indirizzo IPv4 pubblico valido, ad esempio 142.251.209.35
- Questo server DNS viene configurato o assegnato dal DHCP (non in APIPA ad esempio)
- Vale sia da IPv4 a nome che viceversa, non è obbligatorio che nome → IPv4 → nome, può essere differente

IPv4 DNS

```
massimo@hei:~$ host www.google.it
www.google.it has address 216.58.204.227
www.google.it has IPv6 address 2a00:1450:4002:415::2003
massimo@hei:~$ host 216.58.204.227
227.204.58.216.in-addr.arpa domain name pointer mil07s18-in-f3.1e100.net.
227.204.58.216.in-addr.arpa domain name pointer lhr48s22-in-f3.1e100.net.
227.204.58.216.in-addr.arpa domain name pointer par21s06-in-f227.1e100.net.
227.204.58.216.in-addr.arpa domain name pointer par21s06-in-f3.1e100.net.
massimo@hei:~$
```

server HTTP/HTTPS

- Quando avvio il browser e apro una pagina http o https cosa succede?
- tramite il DNS il client identifica l'indirizzo IPv4 del sito da contattare
- farà una richiesta in chiaro (http) o crittografata (https), il server risponderà con una pagina inziale, nel cui contenuto possono essere presenti altri contenuti da scaricare, il browser continuerà a richiedere ogni cosa al server per visualizzare la pagina

ping ovvero ICMP ping

- Esistono dei protocolli usati per la diagnostica
- Il comando “ping” utilizza il protocollo ICMP
- Serve per verificare la raggiungibilità di un indirizzo IPv4

ping ovvero ICMP ping

```
massimo@hei:~$ ping 192.168.195.1
PING 192.168.195.1 (192.168.195.1) 56(84) bytes of data.
64 bytes from 192.168.195.1: icmp_seq=1 ttl=64 time=2.85 ms
64 bytes from 192.168.195.1: icmp_seq=2 ttl=64 time=44.6 ms
64 bytes from 192.168.195.1: icmp_seq=3 ttl=64 time=2.53 ms
^C
--- 192.168.195.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.528/16.648/44.565/19.740 ms
massimo@hei:~$
```

Cosa fa lo switch?

- Agisce a livello L2, quindi soli MAC-ADDRESS
- Con 802.11q anche VLAN
- Serve solo a permettere ai vari dispositivi di dialogare tra di loro

Cosa fa il router?

- Il router puro fa solo L3
- I router di casa hanno molte funzionalità, anche L2, quindi fanno da router, switch, spesso hanno l'access point
- Il compito del router è di fare dialogare tra di loro le varie reti locali
- Il termine utilizzato per identificare la rete comprendente lo switch e i dispositivi connessi è “dominio di collisione”


DOMANDE?

per contattarmi:

maxnuv@linux.it