

# CORSO AVANZATO DI INFORMATICA E ROBOTICA

## LEZIONE 9: Reti e Internet

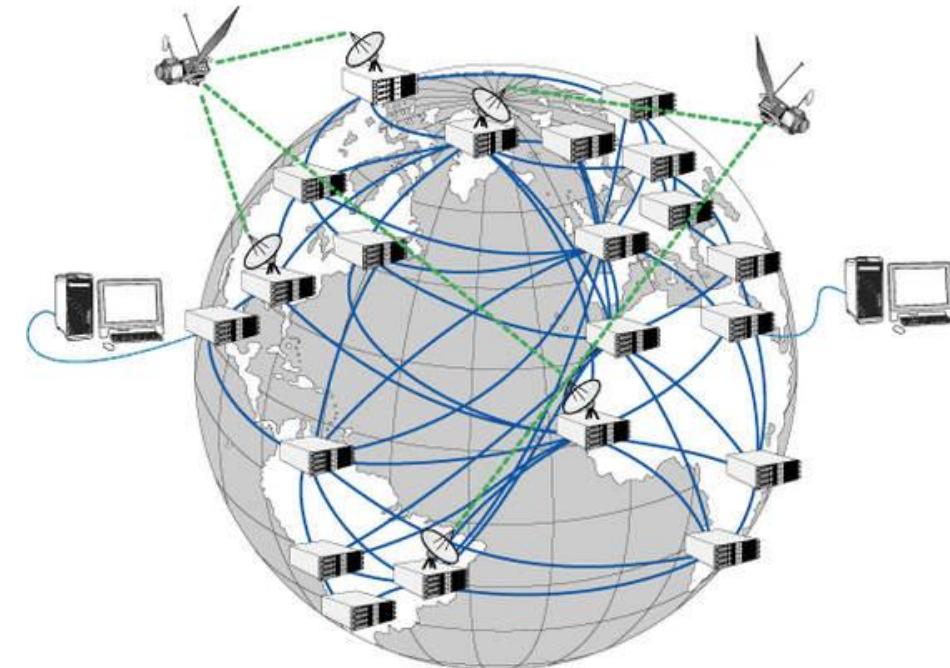
# Reti

01

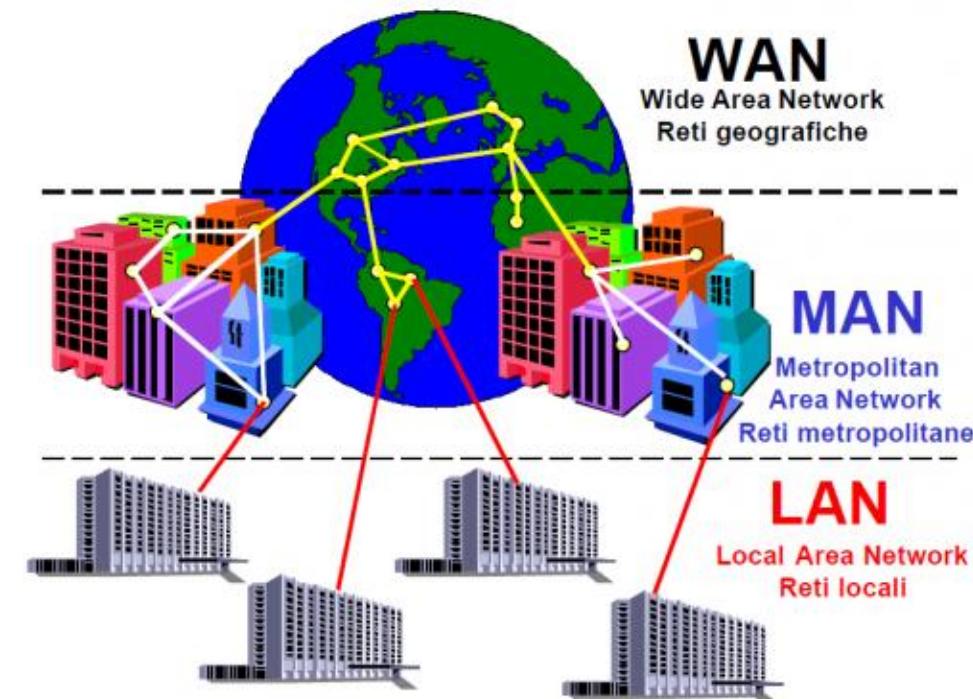
# Cos'è una rete?

Una **rete informatica** è un insieme di **dispositivi elettronici autonomi** (computer, server, smartphone, stampanti, sensori, microcontrollori, ecc.) **interconnessi** tra loro allo scopo di:

- scambiarsi **dati**
- condividere **risorse** (file, stampanti, connessioni Internet)
- cooperare nell'esecuzione di **servizi** e applicazioni



L'elemento chiave è la comunicazione: una rete esiste solo se i dispositivi possono **trasmettere e ricevere informazioni** seguendo **regole comuni**, dette **protocolli**.



# Componenti fondamentali di una rete

- **Nodi (host)** - i dispositivi collegati alla rete

Ogni nodo è identificato da:

- un indirizzo fisico (MAC)
- uno o più indirizzi logici (IP)

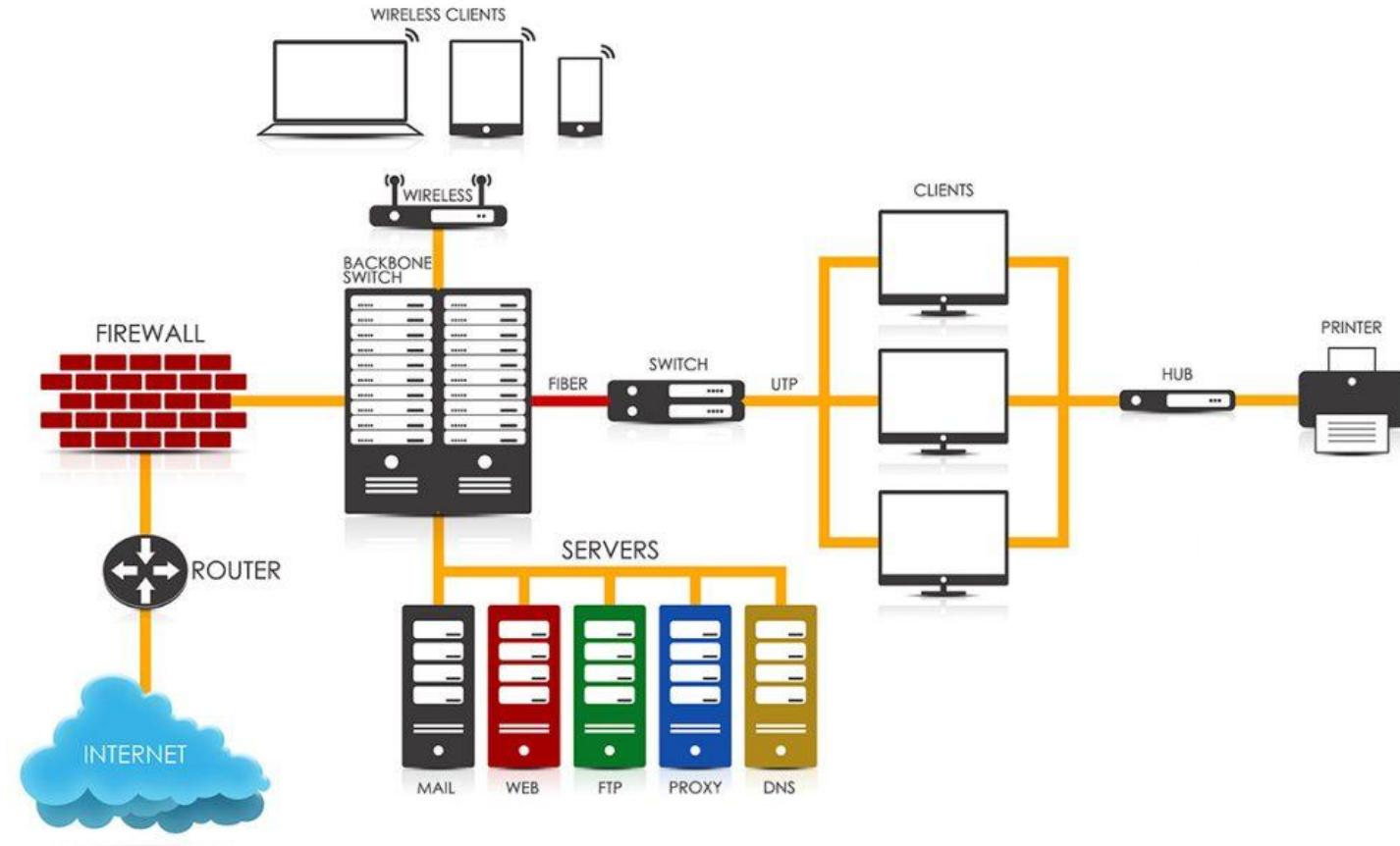
- **Mezzi trasmissivi** - il mezzo fisico o logico

attraverso cui viaggiano i dati

- Cablati (doppino, fibra ottica, ethernet)
- Wireless (wifi, 5G, ...)

- **Dispositivi di rete**

- **Switch**: collega dispositivi all'interno della stessa rete locale
- **Router**: collega reti diverse tra loro
- **Access Point**: fornisce accesso wireless
- **Firewall**: controlla e filtra il traffico

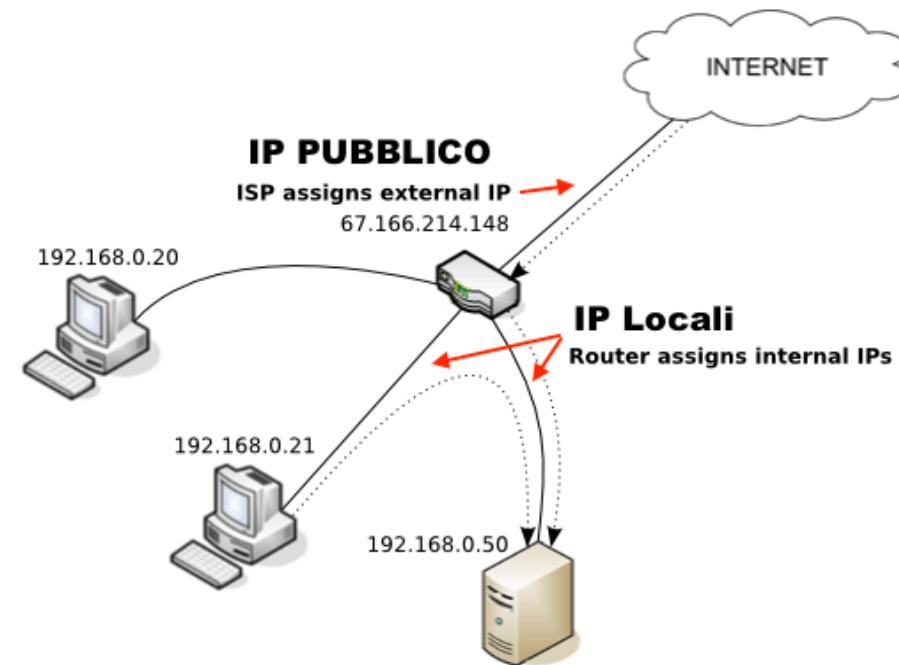


# MAC address & IP address

Per comunicare, ogni dispositivo deve essere **identificabile**.

Qui entrano in gioco due concetti fondamentali:

**MAC address e IP address.**



## MAC address: l'identità fisica

Il **MAC address** è:

- un codice univoco **a livello mondiale**
- assegnato alla **scheda di rete**
- non cambia (salvo spoofing)
- funziona **a livello locale**
- scritto in forma esadecimale  
(es. A4:5E:60:1F:9C:22)

È come il **numero di telaio di un'auto**: identifica l'hardware, non la posizione.

## IP address: l'indirizzo logico

L'**indirizzo IP** identifica **dove si trova** un dispositivo in una rete e:

- **può cambiare** nel tempo
- **dipende dalla rete** a cui sei collegato
- esistono IPv4 e IPv6:  
Esempio IPv4: 192.168.1.25  
Esempio IPv6: fe80::1234:5678:9abc:def1

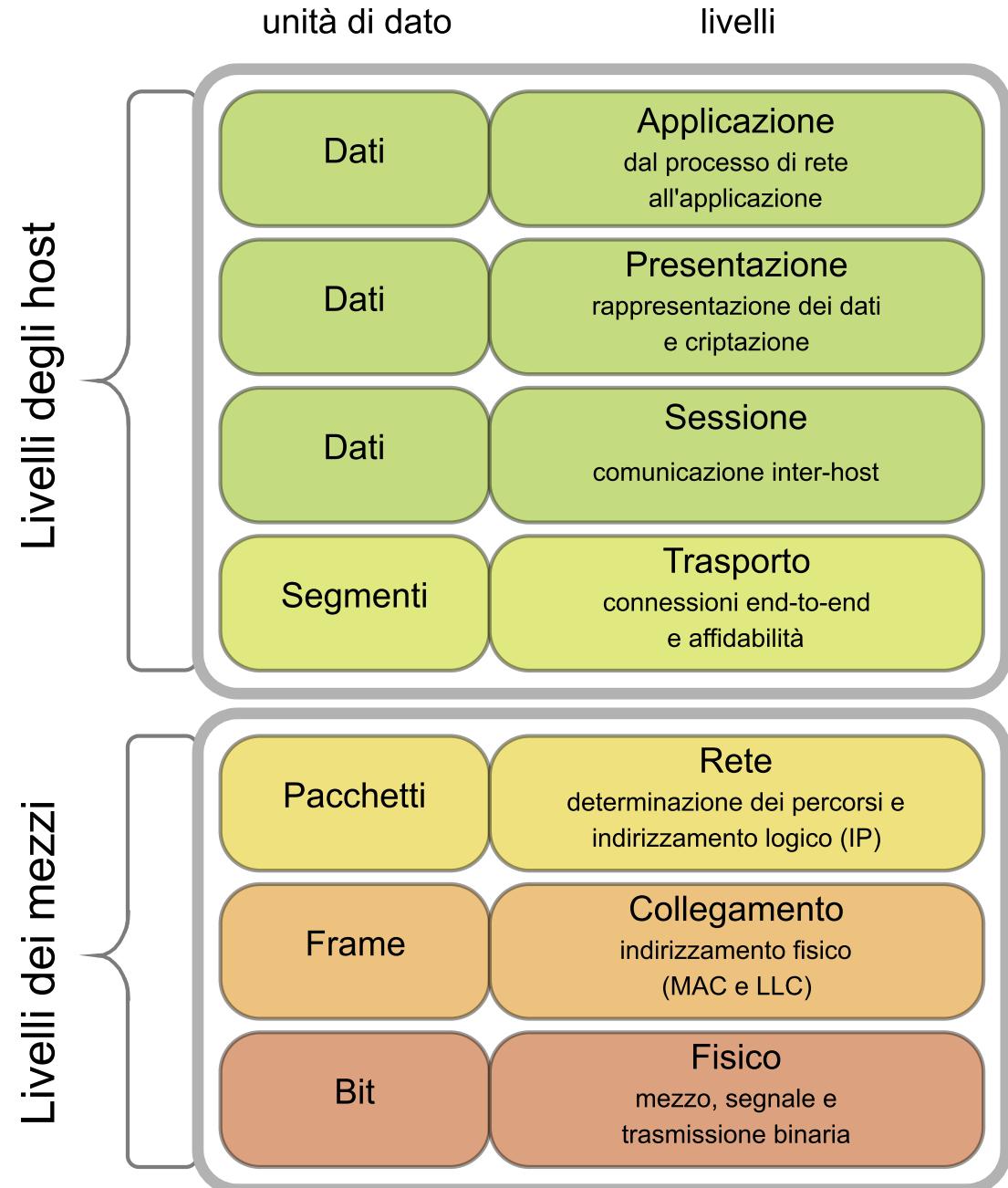
È come l'**indirizzo di residenza**

# Come comunicano i dispositivi in rete? modello ISO / OSI

È un modello utilizzato come standard architetturale per reti di calcolatori.

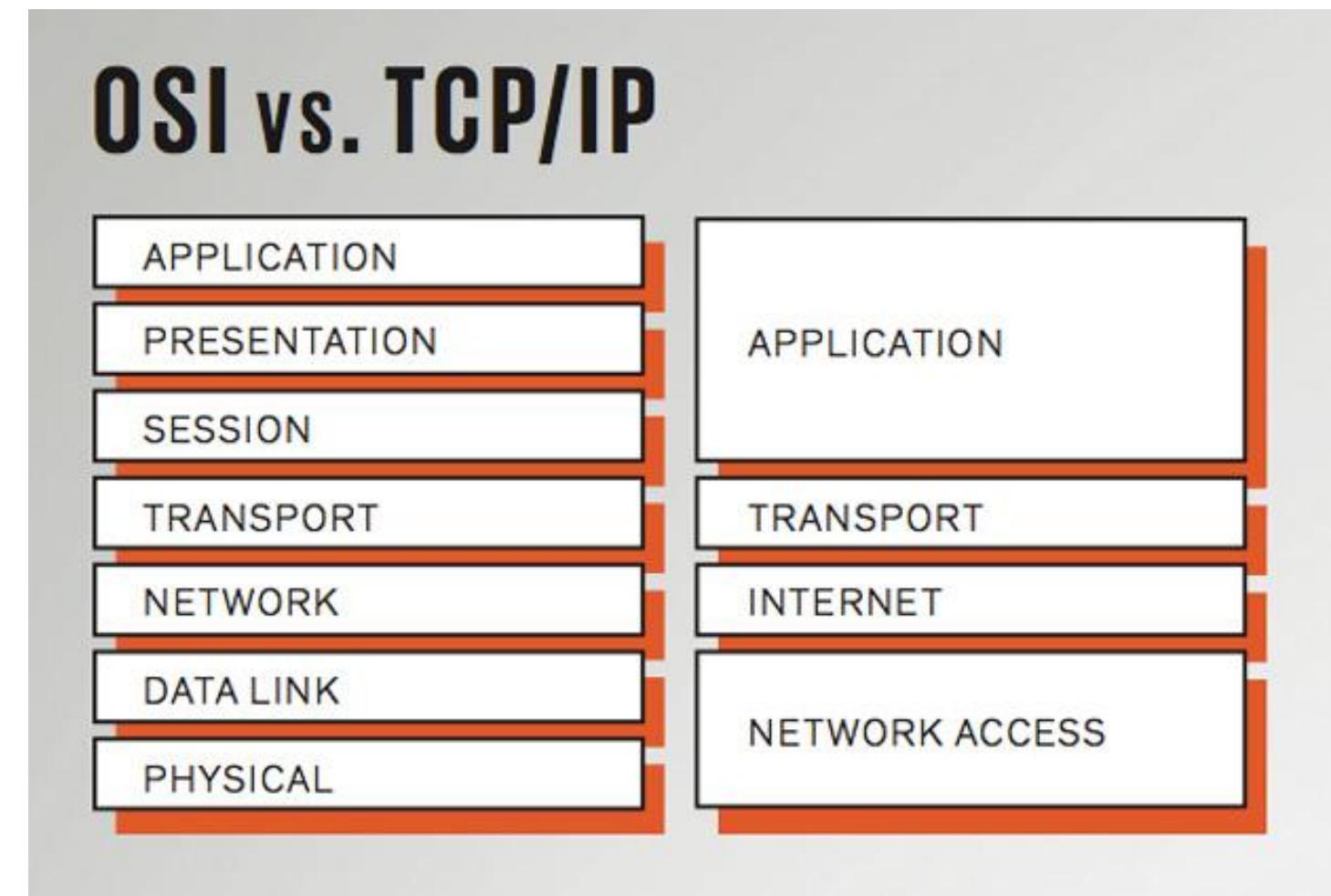
**Stabilisce per l'architettura logica di rete**, ovvero per le funzioni di comunicazione delle telecomunicazioni o di sistemi informatici, **una struttura a strati composta da una pila di protocolli di comunicazione di rete suddivisa in 7 livelli diversi di astrazione**, i quali insieme eseguono tutte le funzionalità della rete, seguendo un modello logico-gerarchico.

I layer vanno dal livello fisico (quello del mezzo fisico, ossia del cavo, delle onde radio, fibra ottica o qualsiasi altro sistema trasmissivo) fino al livello delle applicazioni, attraverso cui si realizza la comunicazione di alto livello.



# Come comunicano i dispositivi in rete?

## TCP / IP

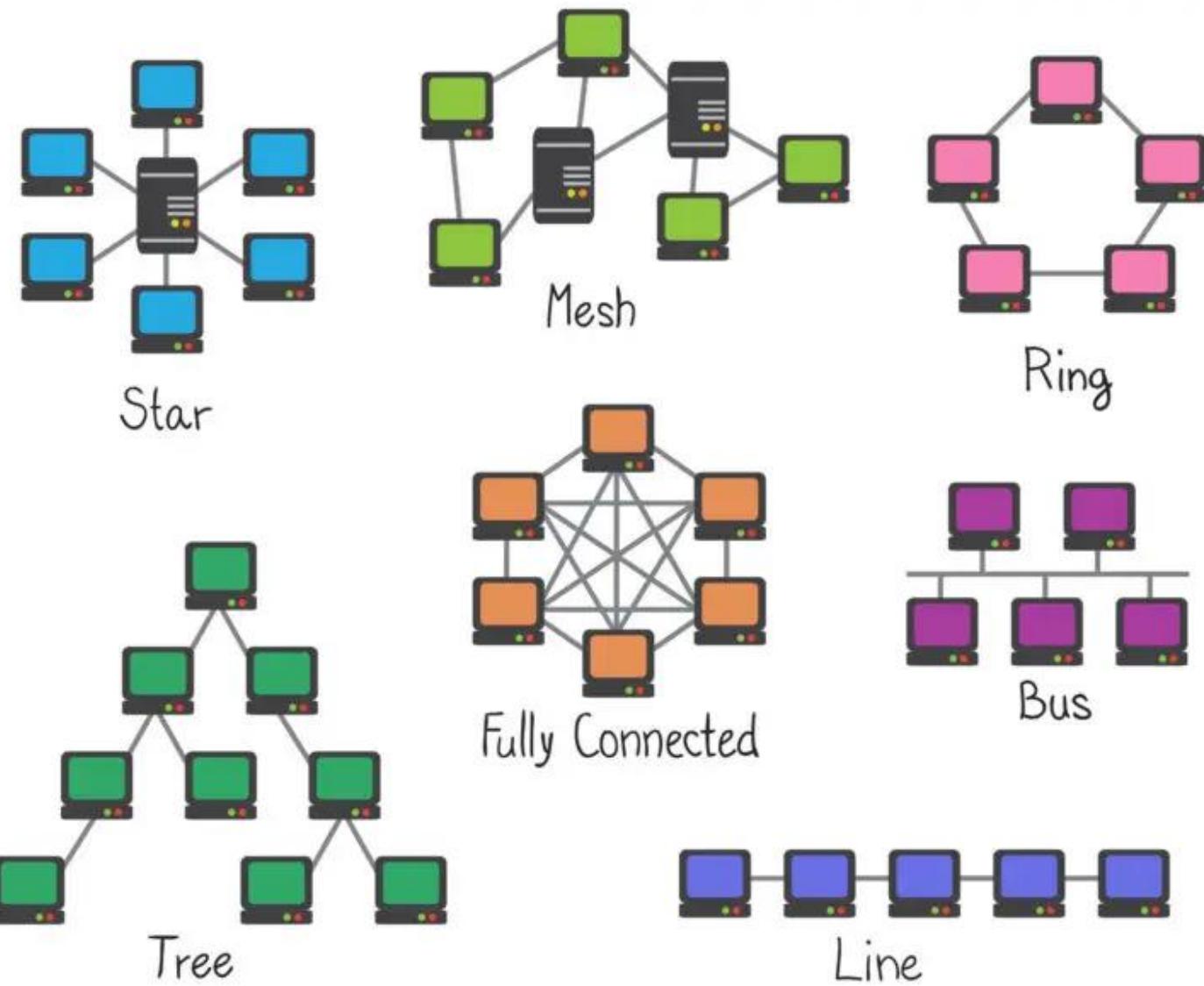


# Topologia di rete

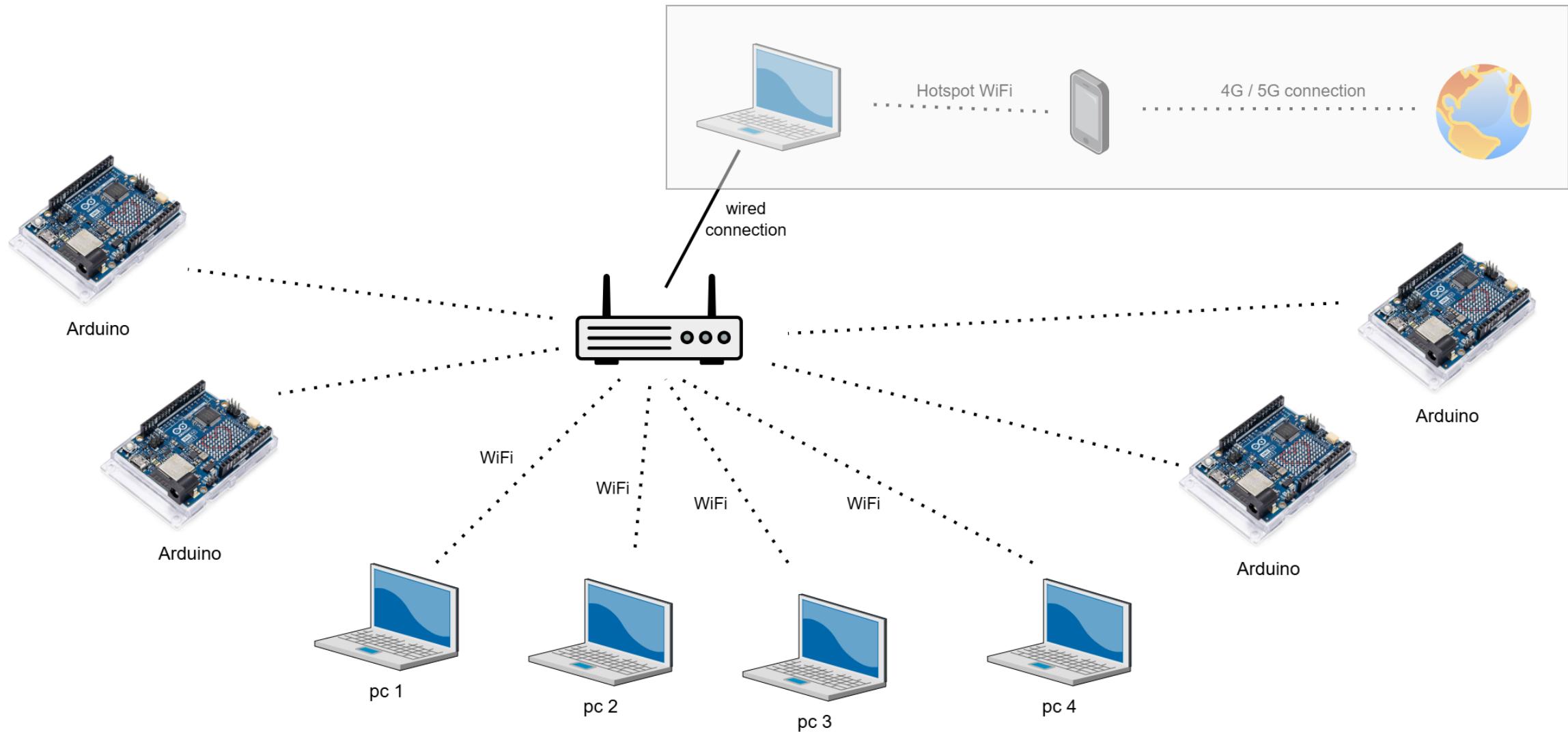
La topologia di rete è lo schema di disposizione fisica e/o logica dei nodi (dispositivi) e dei collegamenti in una rete, definendo come i dati fluiscono e influenzando prestazioni e affidabilità; si divide in fisica (layout dei cavi) e logica (flusso dati), con tipi comuni come Stella, Bus, Anello, Albero e Maglia, spesso combinati in topologie ibride per ottimizzare scalabilità ed efficienza.

La scelta della topologia è fondamentale per:

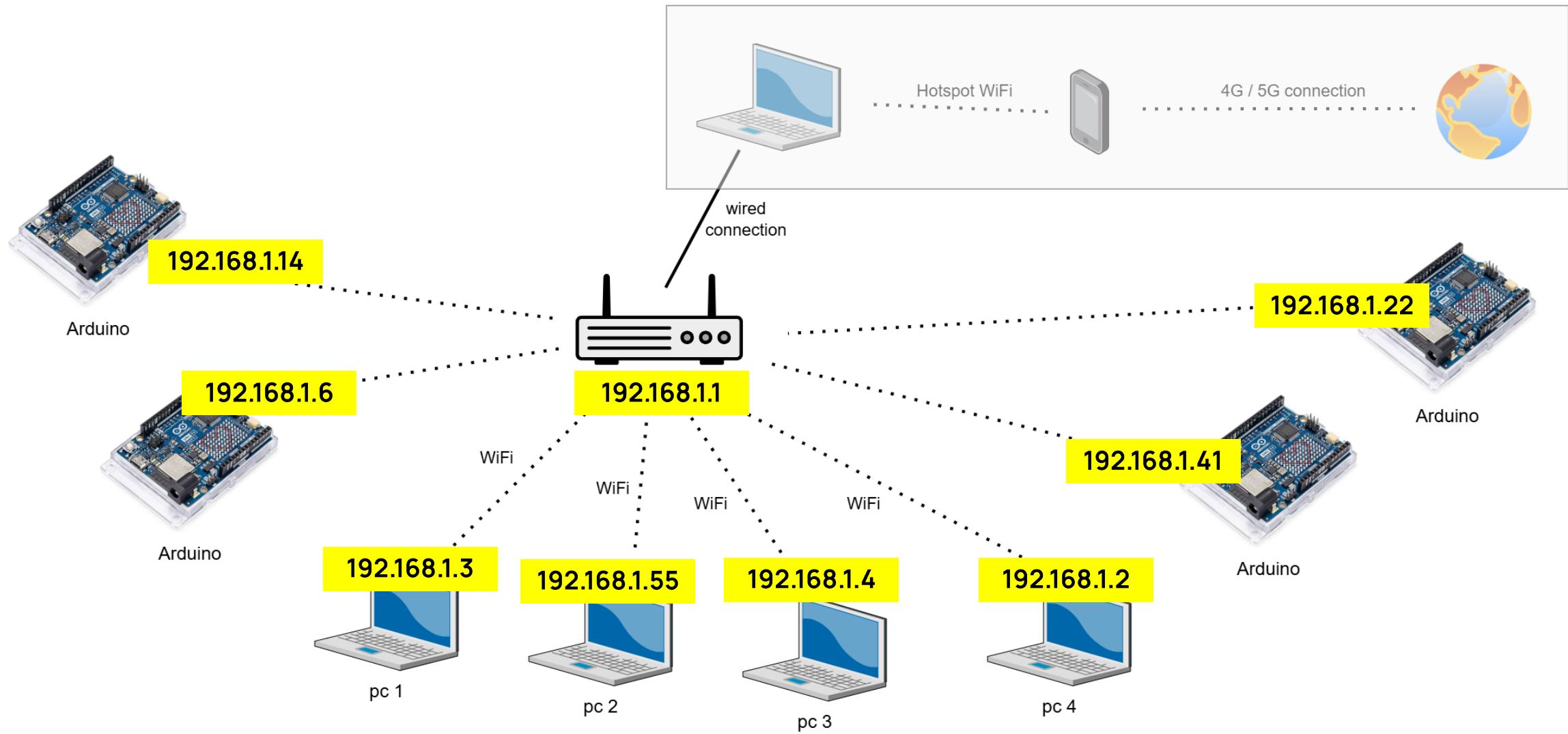
- **Prestazioni:** Velocità e congestione del traffico.
- **Affidabilità:** Tolleranza ai guasti.
- **Scalabilità:** Facilità di aggiungere nuovi dispositivi.
- **Costi:** Complessità e quantità di cablaggio



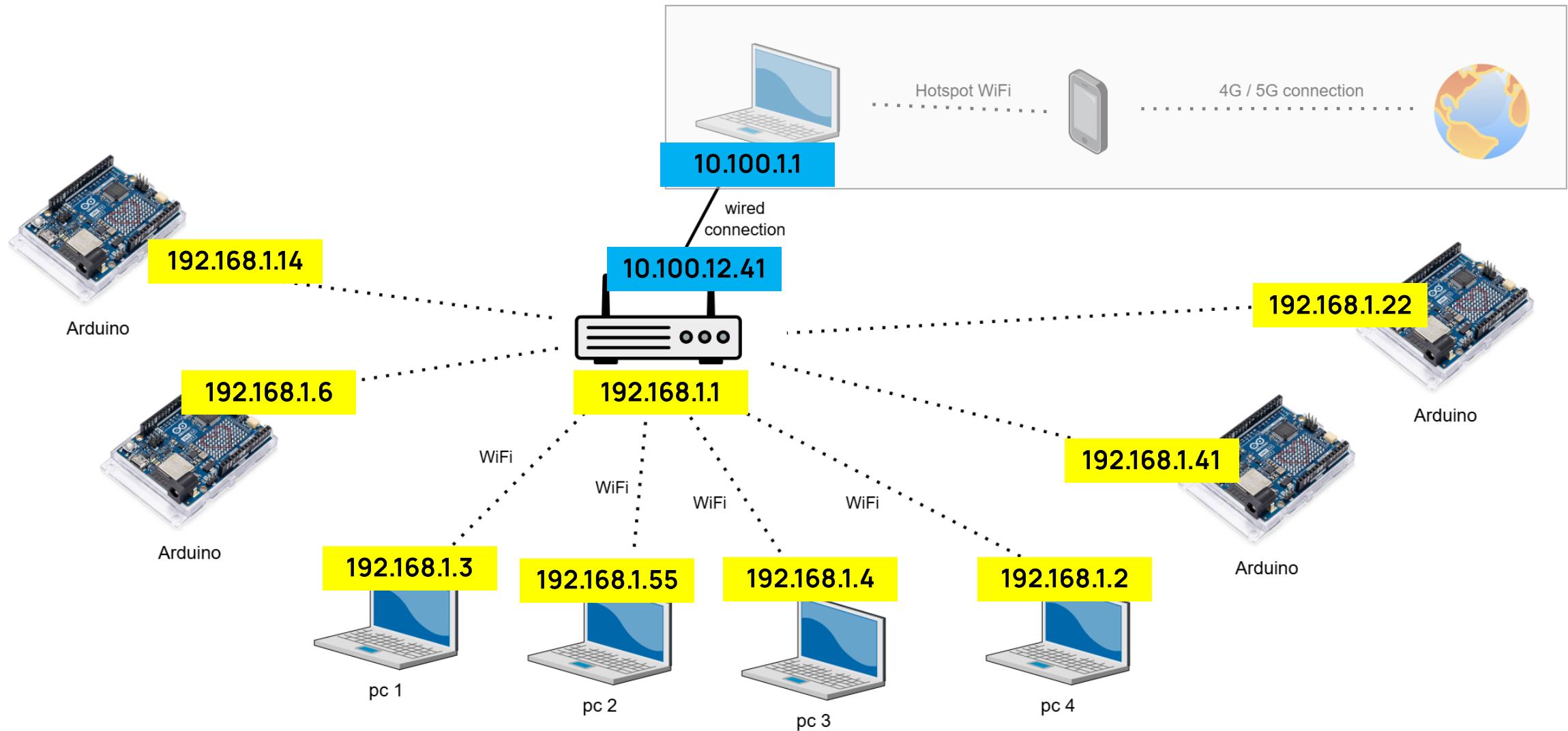
# Esempio: ARDUINO WIFI → collegamento alla rete locale



# Esempio: ARDUINO WIFI → collegamento alla rete locale



# Esempio: ARDUINO WIFI → collegamento alla rete locale



# Maschera di sottorete - accenni

**Maschera: 255.255.255.0**

**192.168.1.14**

La maschera di sottorete funziona come un filtro che divide un indirizzo IP in due parti:

- l'**indirizzo di rete** (identifica la rete)
- l'**indirizzo host** (identifica il dispositivo specifico).

Utilizzando un'operazione logica (AND binario) tra l'indirizzo IP e la maschera, il dispositivo determina se un altro indirizzo è sulla stessa rete locale (comunicazione diretta) o su una rete remota (richiede un router). Questo **permette di gestire il traffico in modo efficiente, suddividendo reti grandi in sottoreti più piccole, migliorando sicurezza e prestazioni**

**192.168.1.1**  
**11000000.10101000.00000001.00000001**

<https://jodies.de/ipcalc?host=192.168.1.1&mask1=16&mask2=>

**La rete è: 192.168.1  
L'host collegato è 14**

```
00001010.00000000.00000000.00000000
00001010.11111111.11111111.11111111
----- 24 bit -----
10101100.00010000.00000000.00000000
10101100.00011111.11111111.11111111
----- 20 bit -----
11000000.10101000.00000000.00000000
11000000.10101000.11111111.11111111
----- 16 bit -----
```

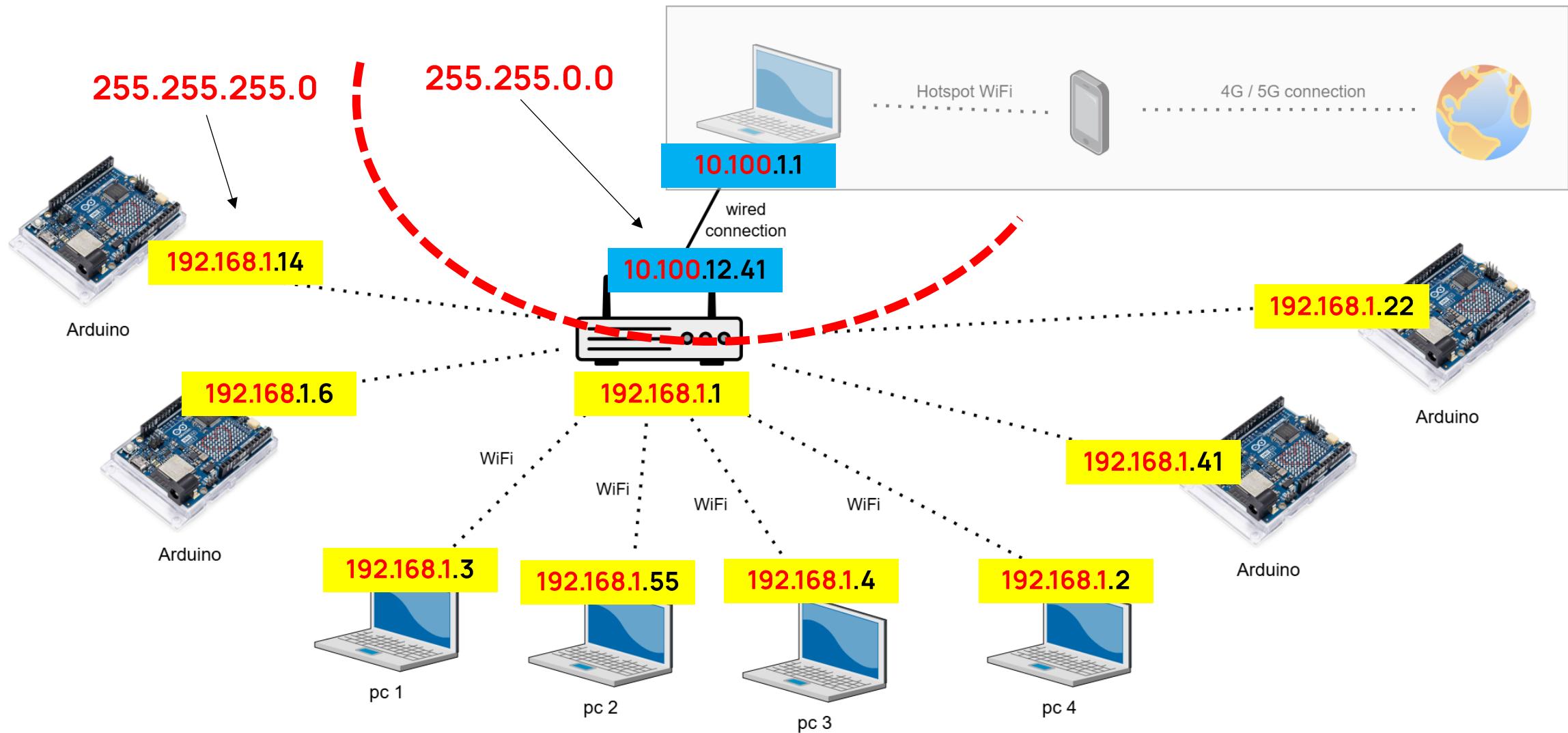
La classe C (192.168.1.0/24) offre 254 indirizzi utili, sufficienti per la maggior parte delle abitazioni, e l'IP .1 è tradizionalmente usato per il router, rendendolo facile da ricordare e configurare per gli utenti

## Maschera di sottorete - accenni

	Decimale	Binario
IP dispositivo connesso	192.168.1.14	11000000.10101000.00000001.00001110
Netmask (24)	255.255.255.0	11111111.11111111.11111111.00000000

	Decimale	Binario
IP dispositivo connesso	192.168.1.14	11000000.10101000.00000001.00001110
Netmask (20)	255.255.240.0	11111111.11111111.11110000.00000000

# Maschera di sottorete - accenni



# Extra – indirizzo IP locale, perché proprio quel numero?

Quando ci connettiamo al nostro router di casa o ad un device connesso alla rete locale solitamente digitiamo l'indirizzo **IP 192.168.1.X** seguito magari dal numero di una porta, ad esempio 80 per i servizi HTTP o 21 per i server FTP. Ma perché si è scelto di sfruttare proprio l'IP 192.168.1.1? Per rispondere a questa domanda dobbiamo ripercorrere brevemente la storia dell'informatica.

**In origine erano presenti 5 classi di Internet address, A, B, C erano destinati agli usi generali mentre D per il multicast addressing ed E per gli impieghi sperimentali.** Tale sistema di classi veniva sfruttato per allocare gli indirizzi IP.

- la classe A comprende gli IP: **10.0.0.0 - 10.255.255.255**;
- la classe B comprende gli IP: **172.16.0.0 - 172.31. 255.255**;
- la classe C comprende gli IP: **192.168.0.0 - 192.168.255.255**.

Anche se gli indirizzi IPv4 vengono espressi in decimali, le definizioni degli indirizzi di classe A, B e C sono considerate in binario, dunque **tali indirizzi sono rappresentati da 4 gruppi di otto bit**. Inoltre gli indirizzi IP sono in realtà divisi in due parti. Una parte rappresenta la rete, mentre l'altra l'host. Dunque il tipico indirizzo IP che usiamo nelle reti locali può essere suddiviso in questo modo:

192.168.1 < > .1

con l'ultima parte che rappresenta l'host mentre la prima la rete. Il suo corrispettivo in binario è invece:

11000000 10101000 00000001 < > 00000001

Col passare degli anni tantissime aziende non connesse ad Internet si sono dotate però di una rete locale che sfruttava le medesime classi di IP (A, B e C) utilizzate anche per Internet, dunque **l'IETF (Internet Engineering Task Force)**, l'organismo internazionale composto da tecnici e ricercatori interessati all'evoluzione tecnica e tecnologica di Internet, **ha scelto di destinare questi IP unicamente per uso locale per evitare problematiche di attribuzione (vedi standard RFC 1918)**.

Ecco perché oggi molti di noi conoscono e utilizzano quotidianamente questi indirizzi IP nella propria rete locale. I produttori di router sono liberi di utilizzare tali range di indirizzi IP anche se è difficile che le reti domestiche superino i 256 host individuali, quindi solitamente questi device sfruttano la classe C di default.

L'IETF ha inoltre riservato l'intero ventaglio di indirizzi 127 al meccanismo di **loopback**, quindi quando si elabora una richiesta ad un Web Server avviato sulla propria rete privata, o magari ad una Web App, si può sfruttare tale range di indirizzi IP per indicare al software di eseguire il comando in locale senza inoltrare la richiesta ad Internet.

Fonte: <https://www.html.it/magazine/perche-si-usa-ip-192-168-1-1-in-locale/>

# Extra – indirizzo IP locale, perché proprio quel numero?

Le classi di indirizzi IP (Classi A, B, C, D ed E) sono state **introdotte** per organizzare e gestire in modo efficiente gli indirizzi IP disponibili in un'epoca in cui Internet era molto meno diffuso.

- La suddivisione in classi, definita nelle specifiche originali di Internet, rispondeva a diverse esigenze di progettazione:
- **Gerarchia ed efficienza iniziale:** L'obiettivo era creare una struttura gerarchica per l'assegnazione degli indirizzi e facilitare l'instradamento (routing) dei pacchetti. I primi bit di un indirizzo IP ne determinavano la classe, e di conseguenza, quanti dei 32 bit totali fossero dedicati all'identificazione della rete (Net-ID) e quanti all'identificazione del singolo dispositivo (Host-ID).
- **Diverse esigenze di rete:** Sono state create diverse classi per soddisfare le esigenze di organizzazioni di dimensioni molto diverse:
  - **Classe A:** Progettata per reti molto grandi (come le grandi università o le prime grandi aziende) che necessitavano di milioni di host interni, ma erano relativamente poche come numero di reti globali.
  - **Classe C:** Ideale per migliaia di piccole reti locali, ognuna con un numero limitato di host (massimo 254).
  - **Classe B:** Un punto intermedio per reti di medie dimensioni.
- **Funzionalità speciali:** Le classi D ed E sono state riservate per scopi specifici:
  - **Classe D (Multicast):** Per comunicazioni di gruppo, come lo streaming video a più destinatari contemporaneamente.
  - **Classe E (Sperimentale):** Messa da parte per ricerca e sviluppo futuri.

Sebbene inizialmente funzionale, questo sistema si è rivelato **rigido** e inefficiente nell'uso dello spazio di indirizzamento, portando a un notevole spreco di indirizzi, specialmente per le classi A e B.

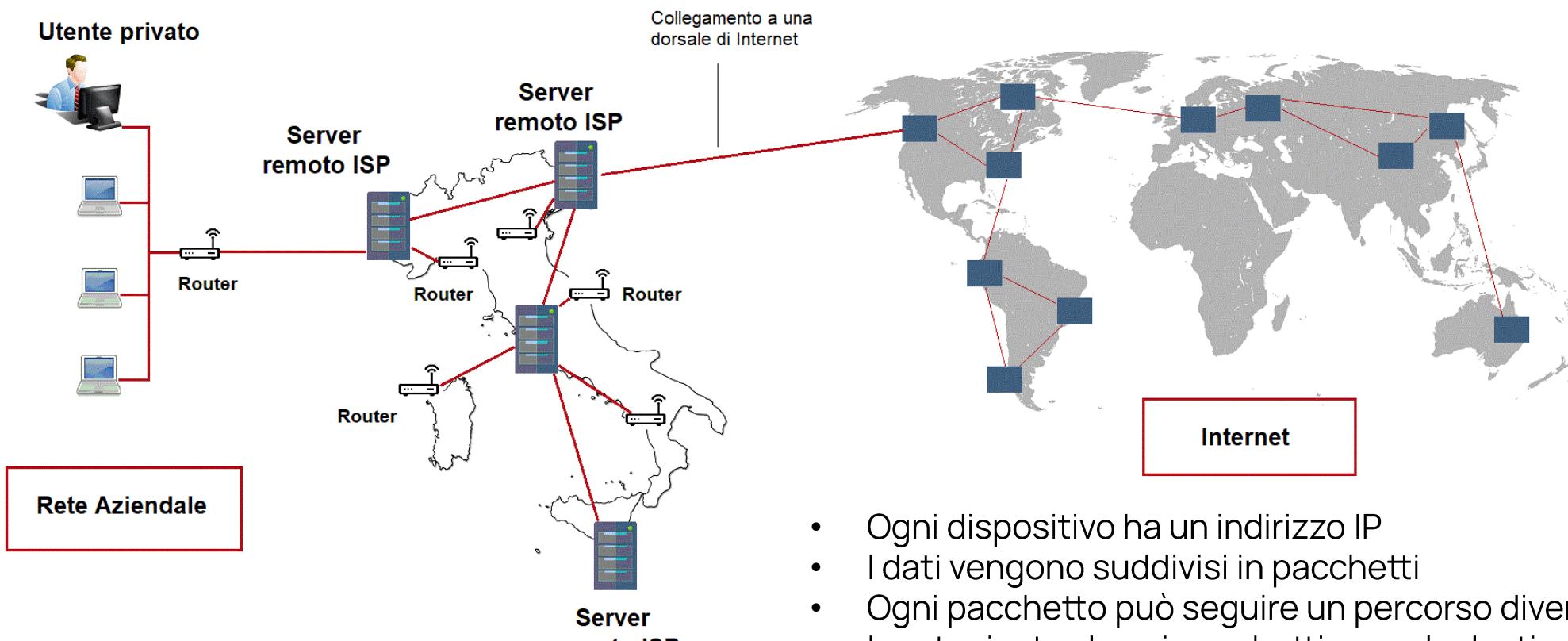
Per risolvere questi problemi e rallentare l'esaurimento degli indirizzi IPv4, il sistema "classful" è stato abbandonato in favore del **Classless Inter-Domain Routing (CIDR)**, che permette una gestione molto più flessibile e granulare degli indirizzi, utilizzando una notazione più moderna (es. /24 invece di "Classe C").

# Internet

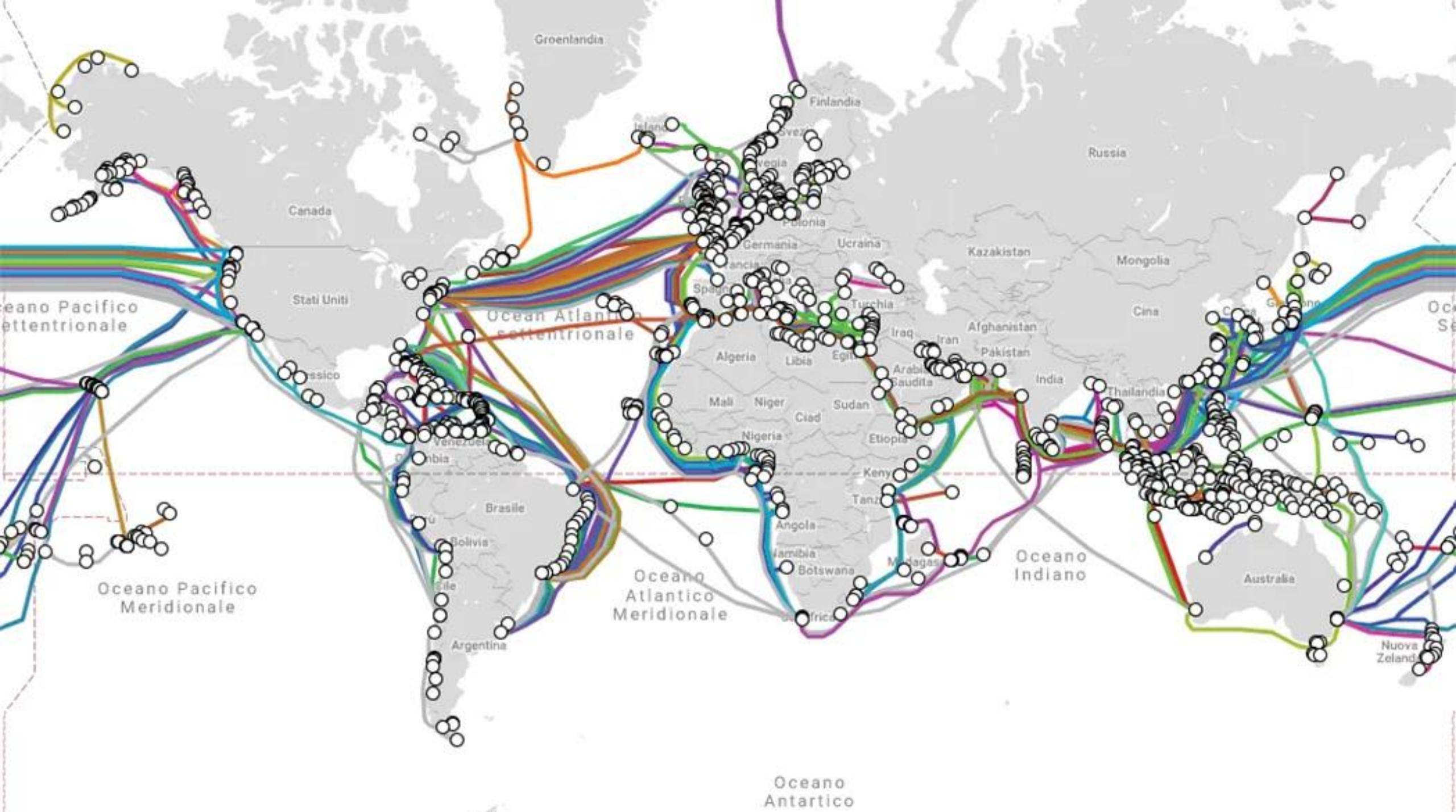
02

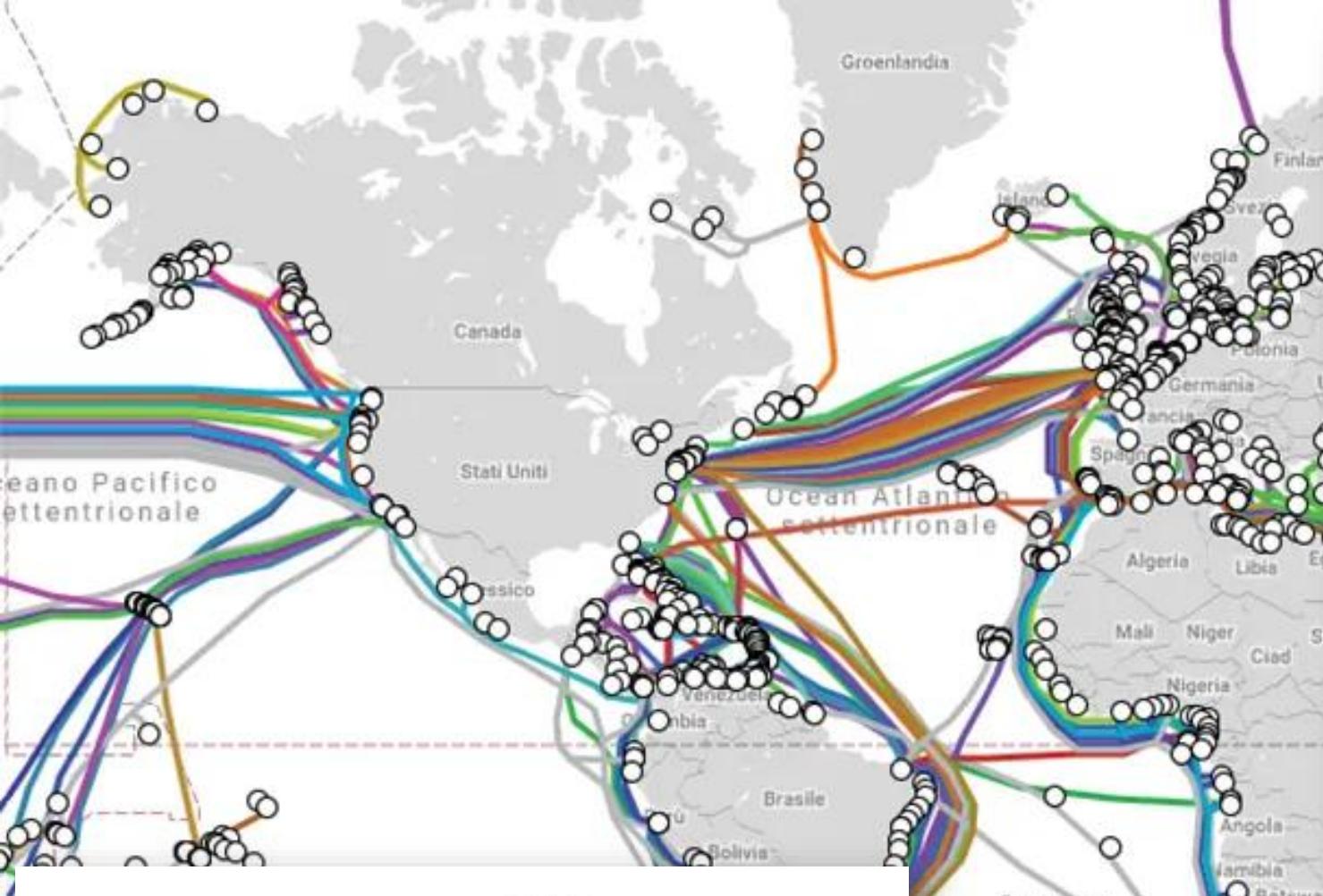
# Internet

Internet è una **rete globale di reti**, basata sul protocollo IP, che collega miliardi di dispositivi in tutto il mondo. È un sistema **decentralizzato e distribuito**.

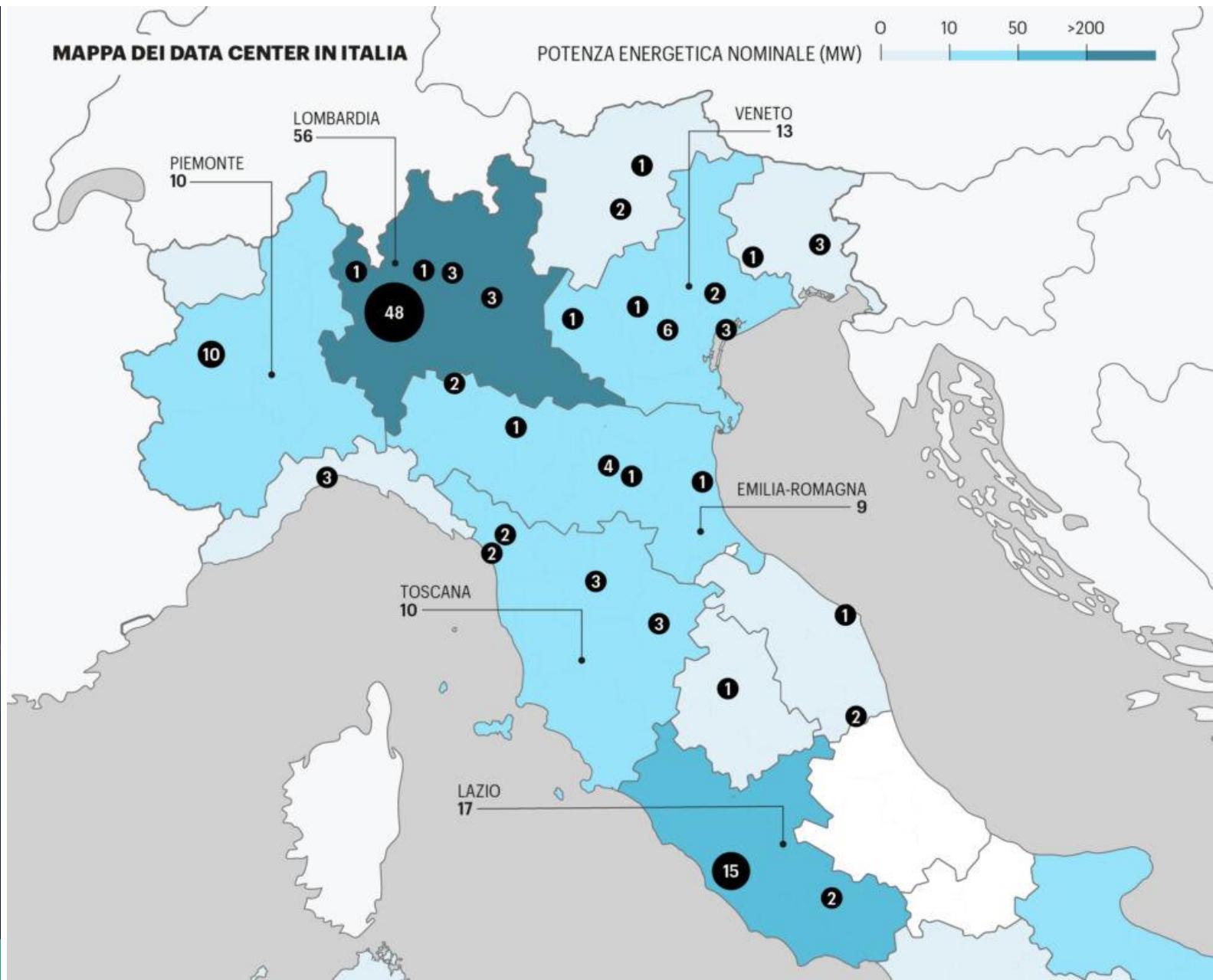
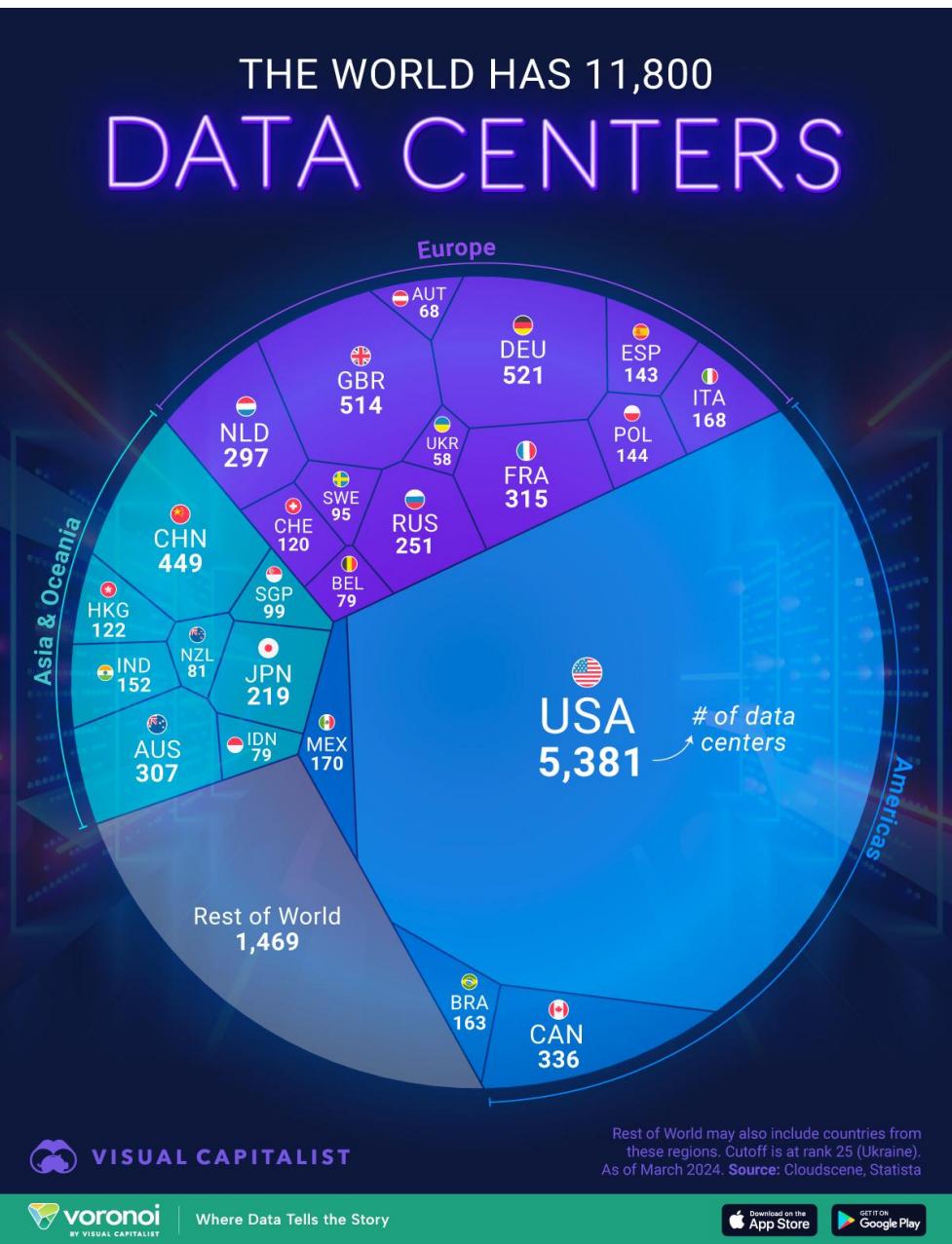


- Ogni dispositivo ha un indirizzo IP
- I dati vengono suddivisi in pacchetti
- Ogni pacchetto può seguire un percorso diverso
- I router instradano i pacchetti verso la destinazione
- A destinazione, i pacchetti vengono ricomposti









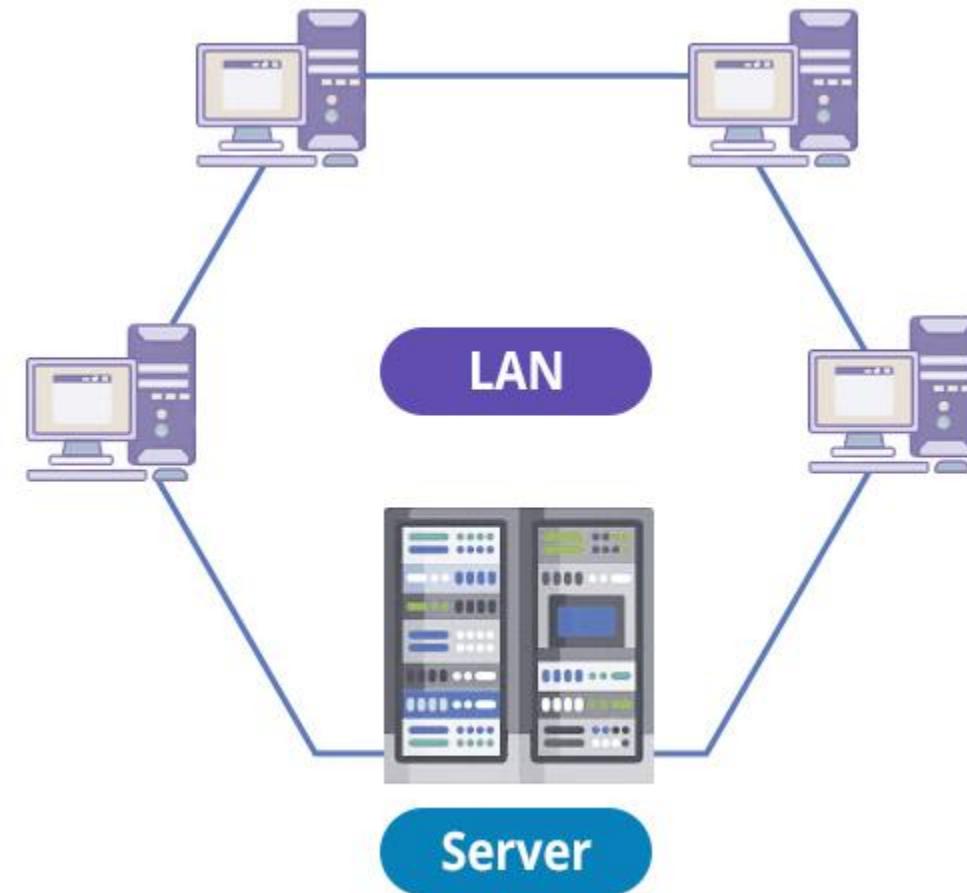
# TOP 50 BIGGEST DATA CENTER MARKETS

## BY ELECTRICITY CONSUMPTION in MEGAWATTS

1,600+ data centers surveyed from 63 markets



# Local Area Network (LAN)

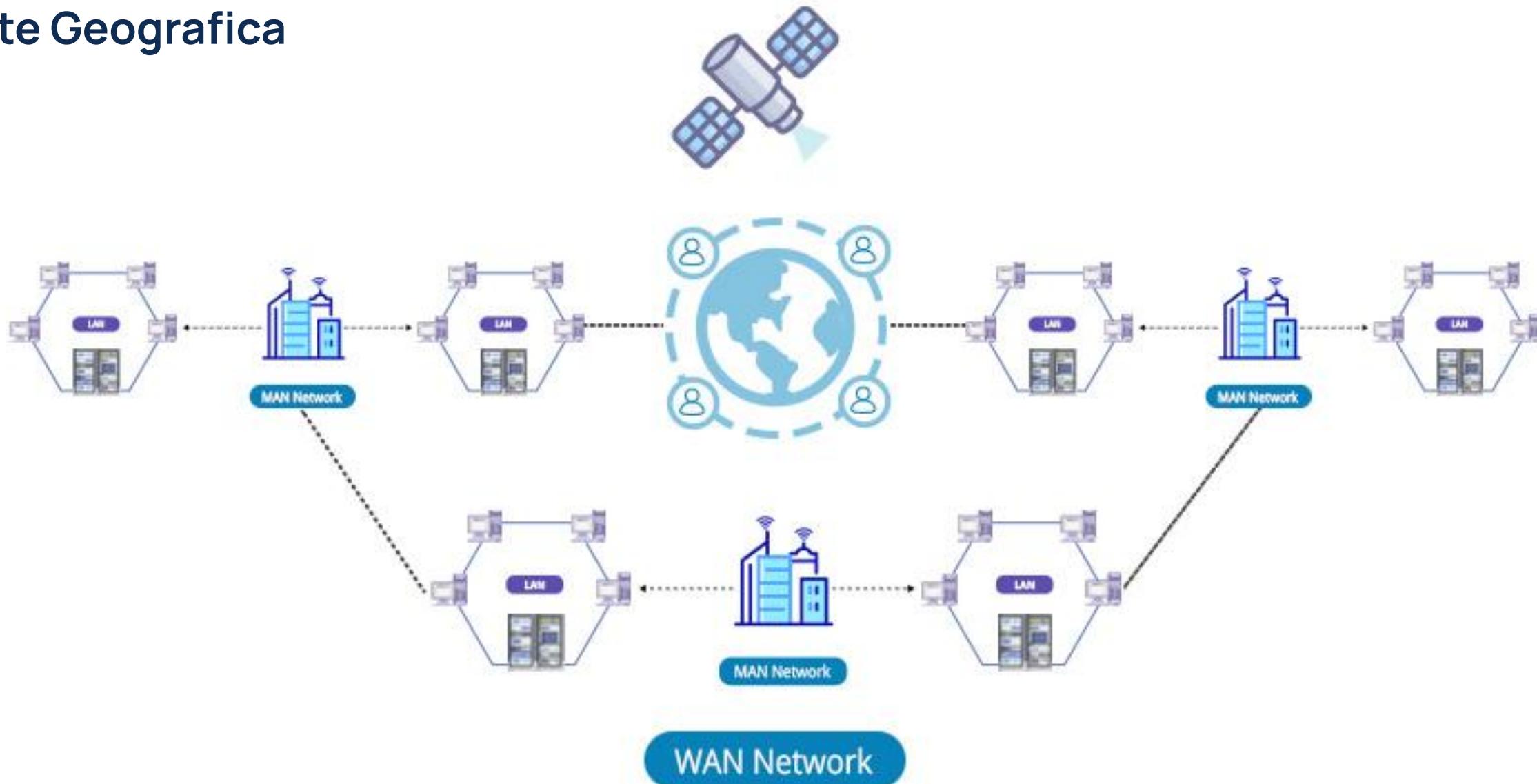


# Metropolitan Area Network (MAN)



# Wide Area Network (WAN)

## Rete Geografica



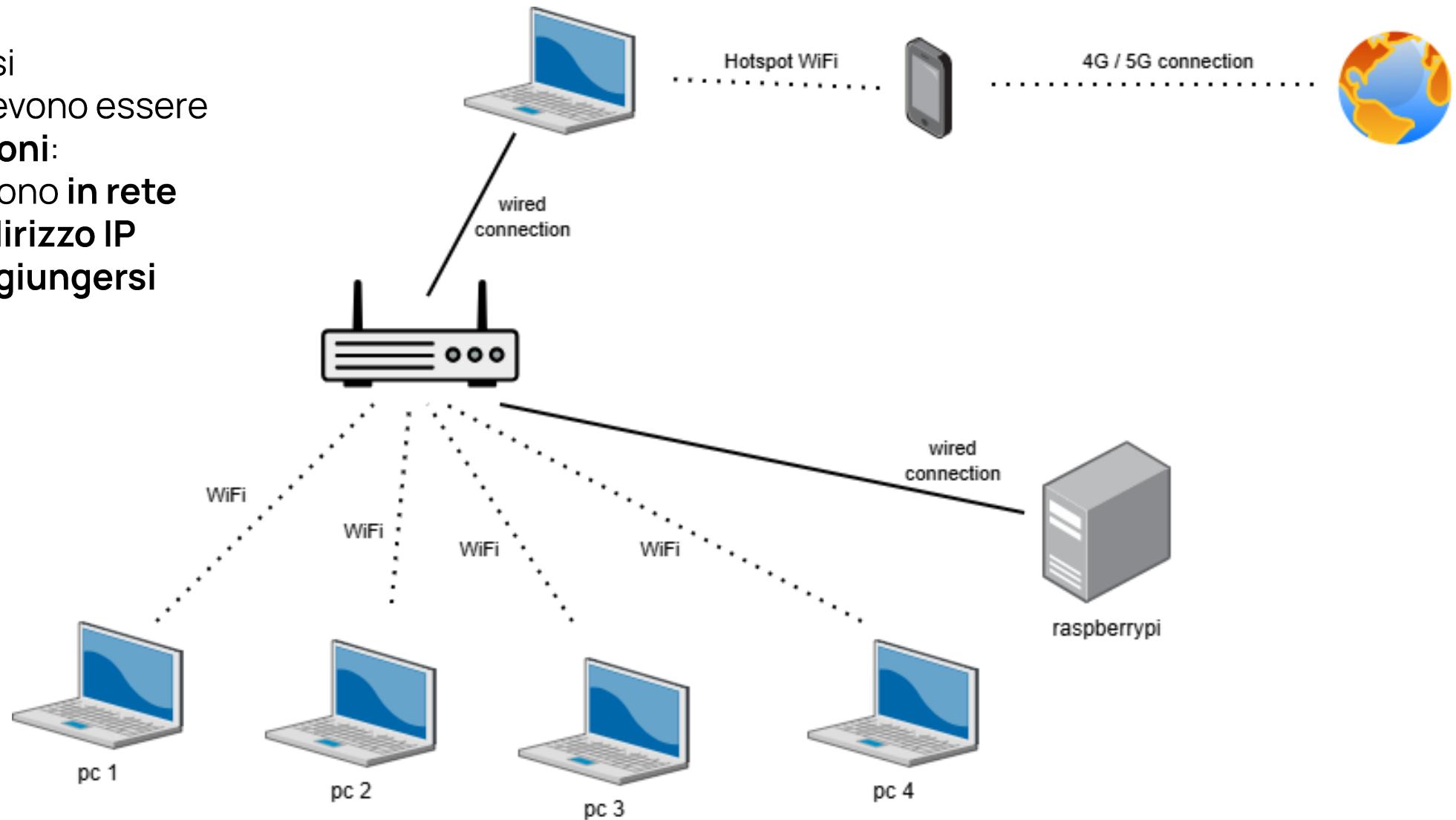
# LAN – Raspberry Pi e protocollo SSH

03

# Esempio di Rete - colleghiamoci al Raspberry Pi 5 !

Prima di qualsiasi collegamento devono essere vere **tre condizioni**:

1. i dispositivi sono **in rete**
2. hanno un **indirizzo IP**
3. possono **raggiungersi**



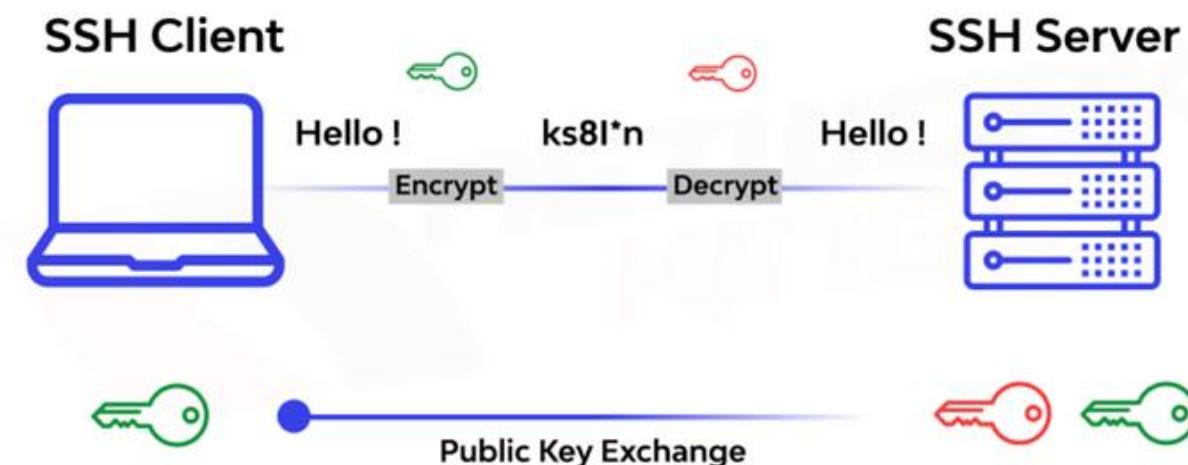
# SSH

**SSH (Secure Shell)** è un protocollo di rete crittografico che permette di accedere e gestire in modo sicuro computer e server remoti su reti non protette, come Internet, creando un tunnel sicuro che crittografa tutte le comunicazioni, autenticando gli utenti e proteggendo da intercettazioni non autorizzate, rendendolo essenziale per l'amministrazione di sistema e il trasferimento sicuro di file, in sostituzione di protocolli insicuri come Telnet.

- Quando diciamo “*mi collego a un altro computer*”, in realtà intendiamo una cosa molto precisa: **un computer invia comandi e riceve risposte da un altro computer attraverso la rete**, come se fosse fisicamente davanti a lui. Questo può avvenire in molti modi (desktop remoto, web, file sharing), ma **SSH è il metodo più usato in ambito tecnico**.
- Il PC può verificare la raggiungibilità con: **ping <indirizzoIP>**
- **Collegarsi significa aprire una comunicazione su una porta:** Un computer non offre un solo servizio, ma **molti servizi diversi**, ognuno su una **porta**.

Web → porta 80 / 443

SSH → porta 22



# SSH

**SSH (Secure Shell)** è un **protocollo di rete** che permette:

- accedere a un computer remoto
- eseguire comandi
- trasferire file

come se fossi davanti al terminale del computer remoto!

Prima di SSH esisteva **Telnet**, che però:

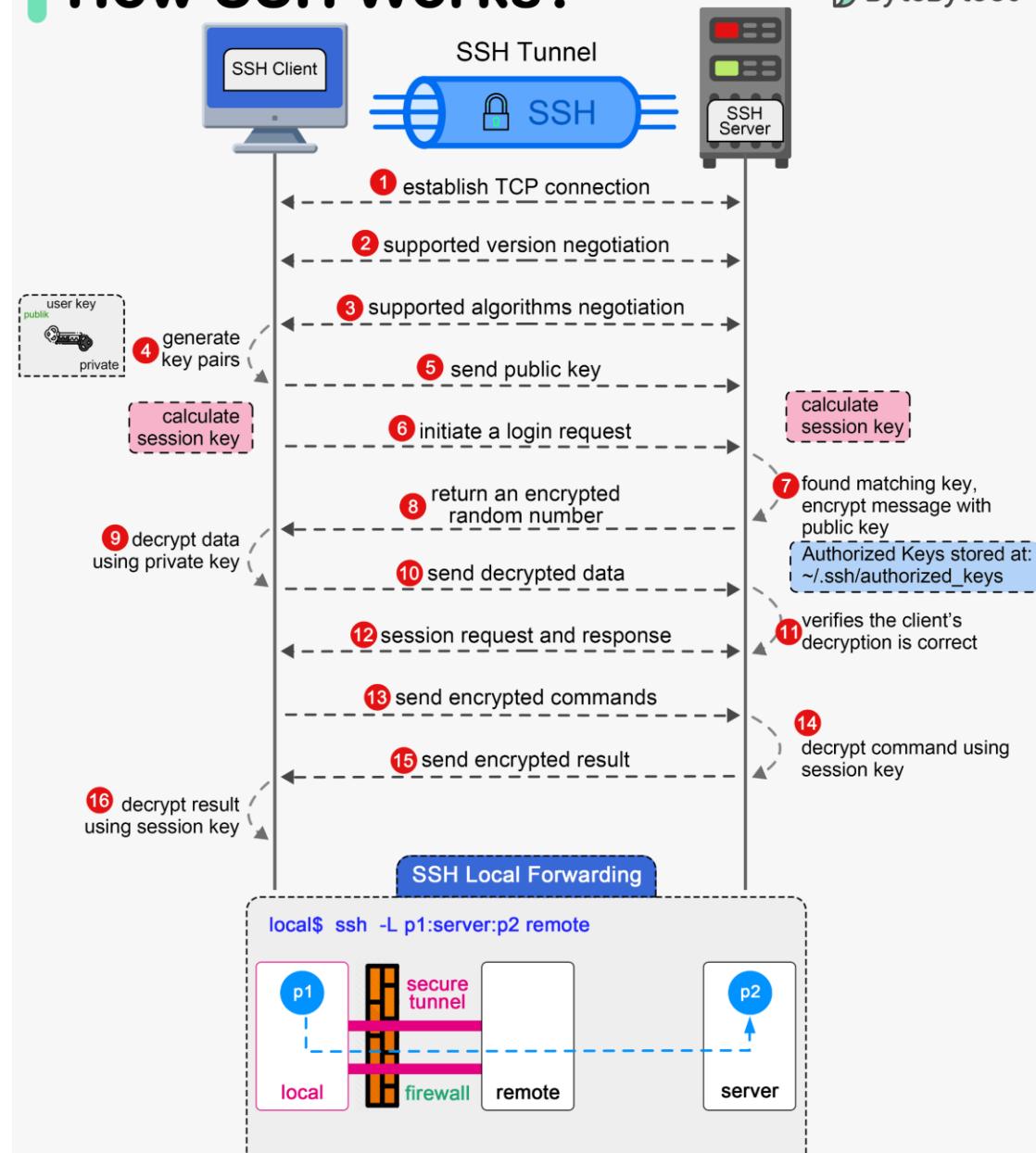
- trasmetteva tutto **in chiaro**
- password incluse

SSH risolve tutto questo:

- connessione **cifrata**
- autenticazione sicura
- integrità dei dati
- protezione da intercettazioni

## How SSH Works?

ByteByteGo



# SSH - come si usa il comando

## Sintassi base

```
ssh utente@host
```

## Esempi:

```
ssh carlo@192.168.1.50
```

```
ssh carlo@raspberrypi
```

```
ssh carlo@server.miodominio.it
```

**Porta di default: 22**, per specificare una porta diversa basta passare il parametro:

-p <numero\_porta>, esempio:

```
ssh -p 2222 utente@host
```

## Autenticazione con password

Alla prima connessione:

- Viene richiesta la verifica della chiave del server [yes]
- chiede la password dell'utente remoto

Opzioni utili (utilizzo simile a -p):

- v # debug
- X # forwarding grafico
- C # compressione
- i # chiave privata
- L # port forwarding
- J # jump host (server intermedio)

## SSH - colleghiamoci!

```
PS C:\Users\carlo> ssh admin@raspberrypi
admin@raspberrypi's password:
Linux raspberrypi 6.12.47+rpt-rpi-2712 #1 SMP PREEMPT Debian 1:6.12.47-1+rpt1 (2025-09-16) aarch64
```

The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/\*copyright.

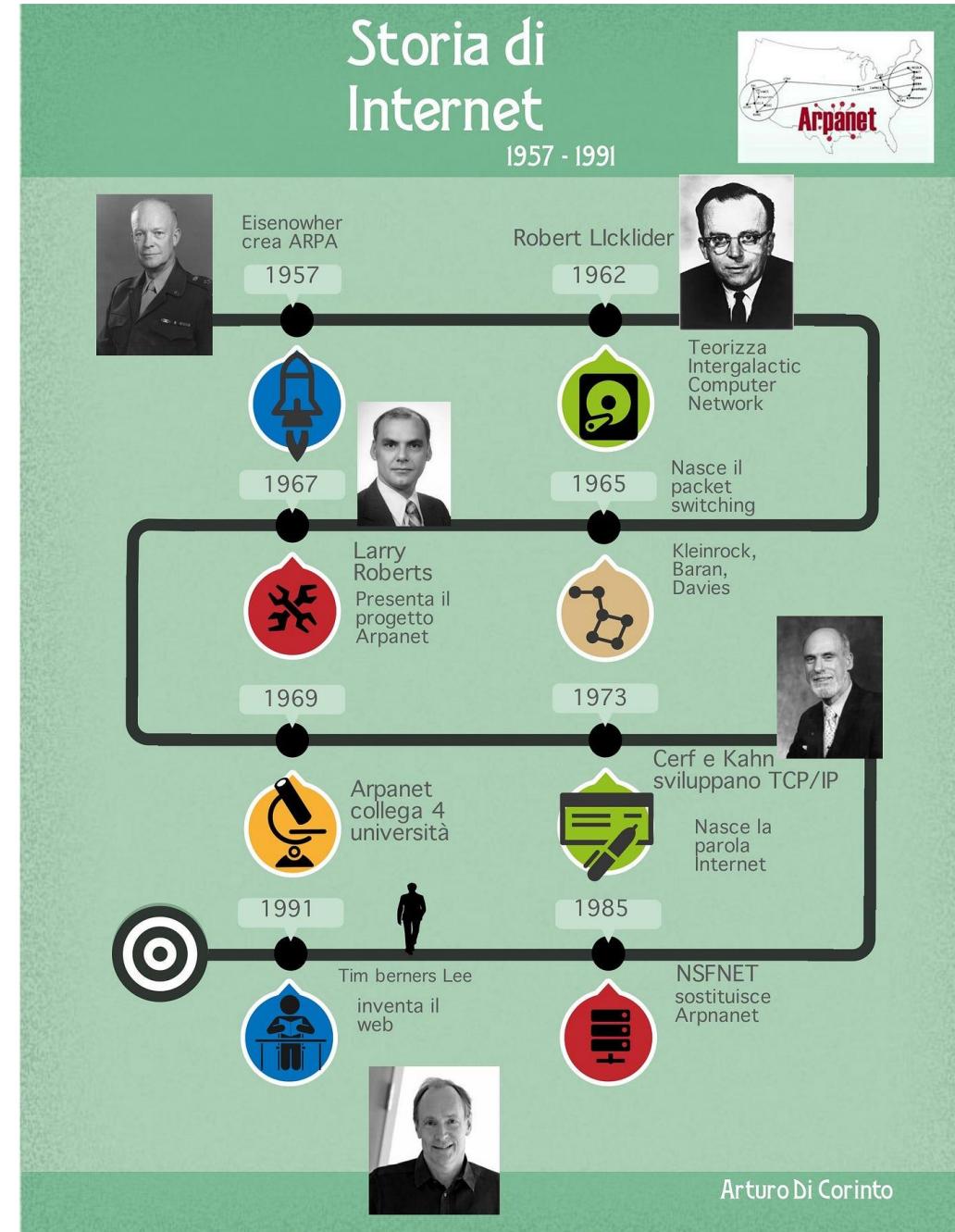
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.

Web console: <https://raspberrypi:9090/> or <https://192.168.218.91:9090/>

```
Last login: Sat Jan 17 18:53:13 2026 from fe80::8914:4024:b551:405a%wlan0
admin@raspberrypi:~$ |
```

# Storia di Internet

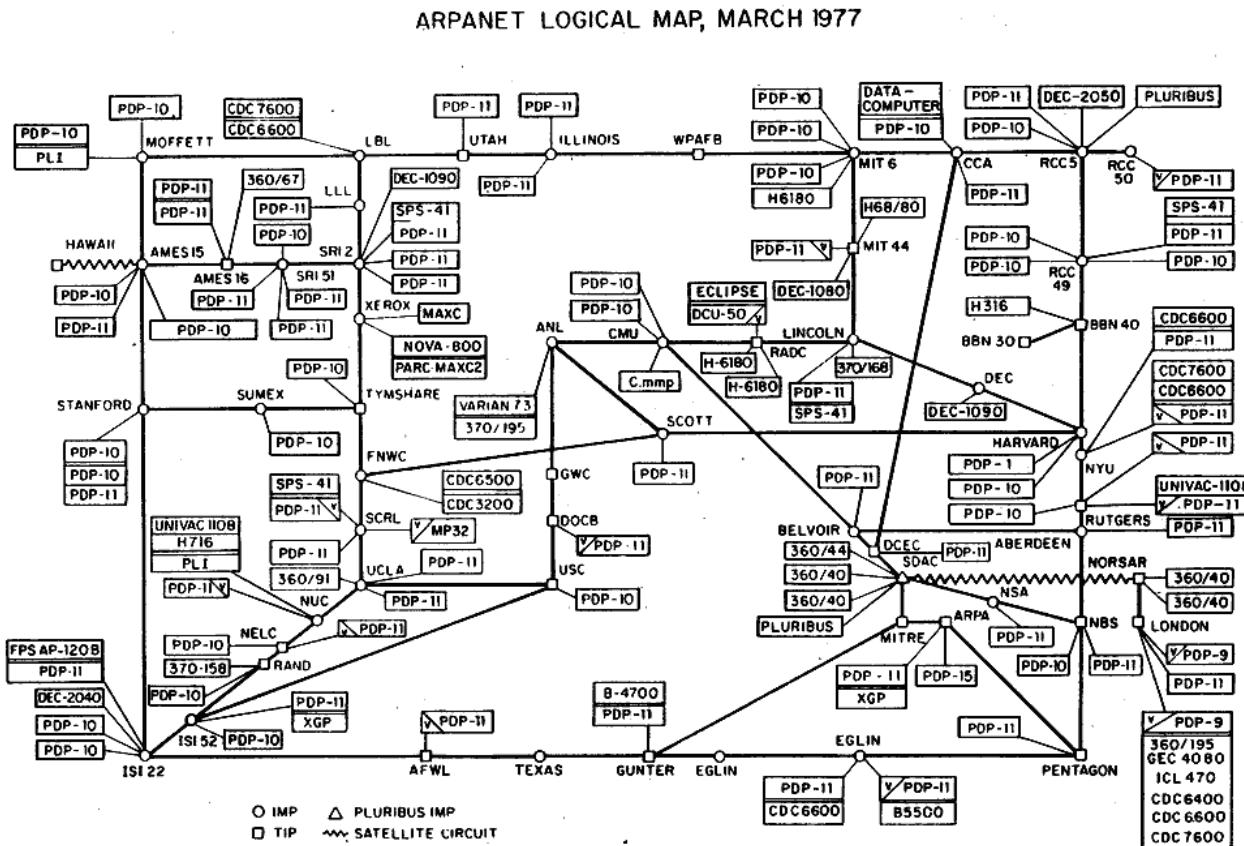
extra



# Anni '60-'70 - ARPANET

Negli Stati Uniti, in piena Guerra Fredda, il Dipartimento della Difesa finanzia un progetto chiamato **ARPANET**. L'obiettivo non era creare "Internet", ma una rete **resistente ai guasti**: se un nodo fosse stato distrutto, i dati avrebbero comunque trovato un percorso alternativo.

Nasce qui un'idea rivoluzionaria: i dati vengono suddivisi in pacchetti indipendenti, che possono viaggiare su percorsi diversi.



## Anni '70-'80 – TCP/IP

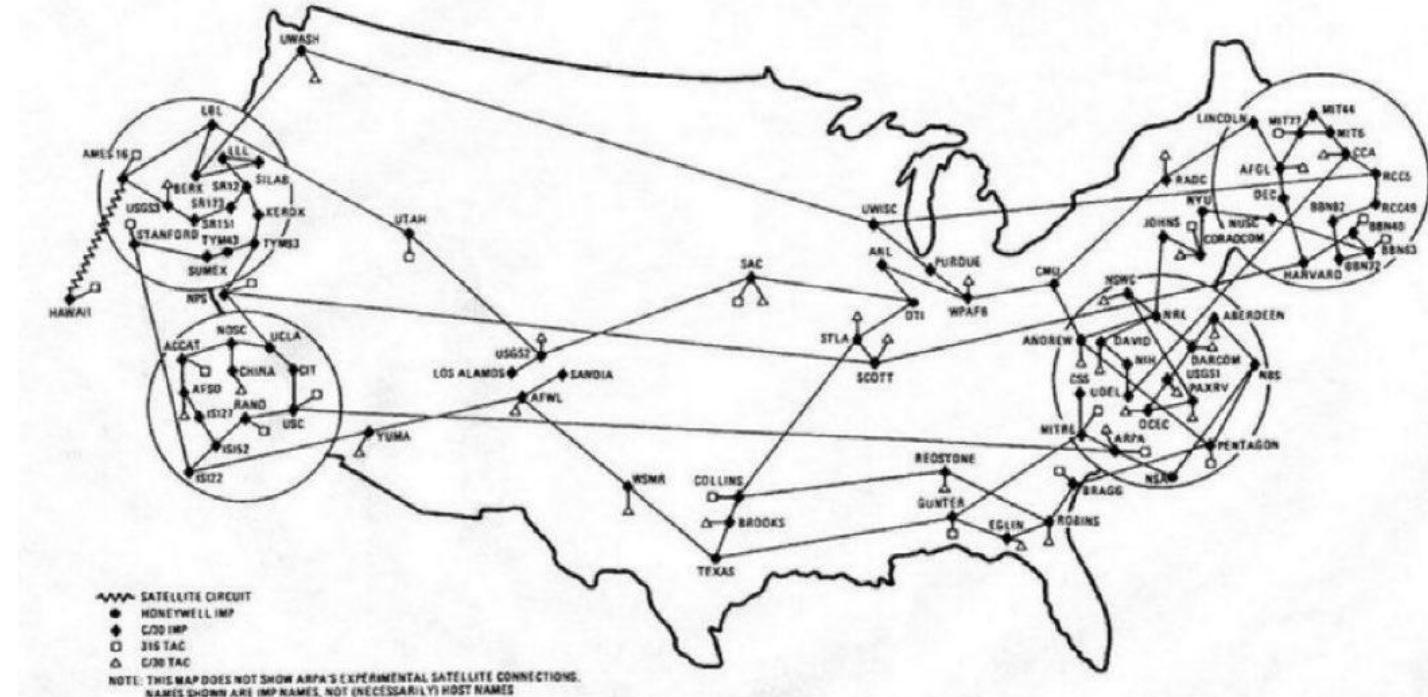
Con l'aumento delle reti, emerge il problema della compatibilità.

Vengono sviluppati i protocolli **TCP/IP**, che definiscono:

- come indirizzare i dispositivi
  - come spedire i dati
  - come correggere gli errori

**Il 1° gennaio 1983 ARPANET adotta ufficialmente TCP/IP: questa data è spesso considerata la nascita tecnica di Internet.**

## ARPANET GEOGRAPHIC MAP, FEBRUARY 1983



# Anni '90 - Il Web

Nel 1989, al CERN, Tim Berners-Lee introduce:

- HTTP
- HTML
- URL

Nasce il **World Wide Web**, che rende Internet accessibile anche ai non specialisti.

Da quel momento Internet smette di essere solo una rete accademica e diventa:

- commerciale
- sociale
- globale

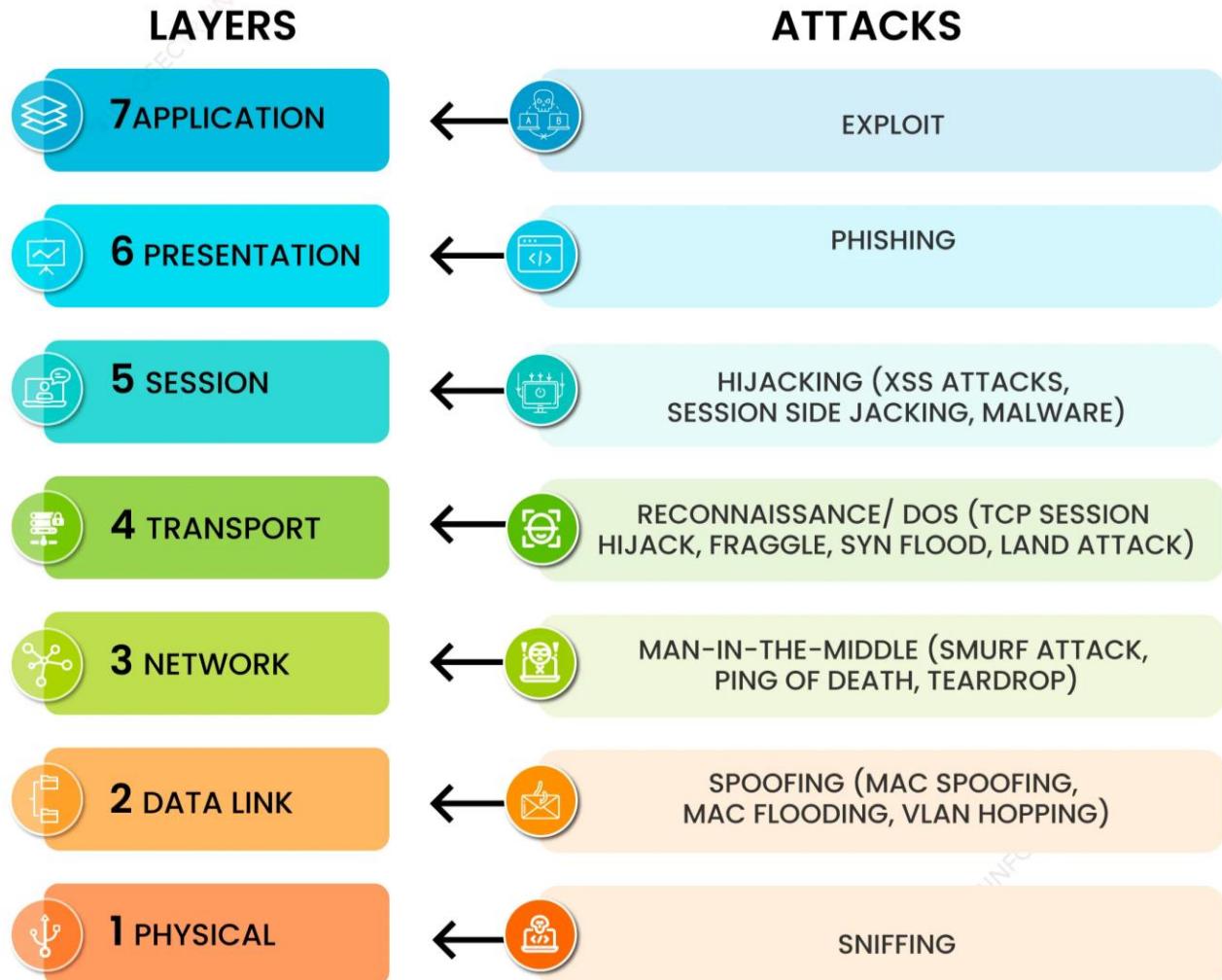


Home page del primo sito web della storia, pubblicato il 20 dicembre 1990 su <https://info.cern.ch/hypertext/WWW/TheProject.html>



Domande, Dubbi, Perplessità?

## COMMON SECURITY ATTACKS IN THE OSI LAYER MODEL



# Router

Partiamo dal presupposto che oggi una **rete informatica** è sempre collegata ad internet, raramente ci troviamo in presenza di rete totalmente off-line. Il router è lo strumento che permette di collegare la rete informatica aziendale a internet.

Tendenzialmente esiste un router principale che connette la LAN (Local Area Network) a internet e dispositivi aggiuntivi che la diffondono in azienda (es: i router wireless a cui ci si può connettere via Wi-Fi).

# Firewall

Letteralmente “muro di fuoco”, è uno strumento di protezione che ha il compito di controllare gli accessi alla rete, filtrando il traffico che arriva dall'esterno e che potrebbe essere dannoso o malevolo (pensiamo per esempio a tentativi di accesso non autorizzato per esfiltrare dati dell'azienda). Il firewall può essere un componente hardware o un componete software (o entrambi in abbinamento).

# Switch

Abbiamo detto che tendenzialmente la situazione tipo all'interno di un'azienda è quella di una rete composta da più dispositivi interconnessi che si incontrano e interagiscono tra loro, creando banalmente del traffico dati. Questo traffico deve essere gestito per non creare ingorghi e qui entra in gioco lo switch. Lo switch è il componente della rete che smista il traffico indirizzandolo solo verso i dispositivi destinatari. Per semplificare, potremmo paragonarlo ad un Vigile urbano.

# Server

Il server è uno dei componenti più complessi di una rete perché può svolgere più servizi. È a disposizione di tutti i componenti della LAN (i Client) che tipicamente fanno richiesta al server per determinate funzionalità.

Il server può essere una componente hardware, software o entrambi e può svolgere anche l'attività di autenticazione degli utenti per l'accesso ai repository documentali dell'azienda. Su una stessa rete possono essere presenti più server.

Le reti gestite tramite un server principale che gestisce le varie richieste vengono definite “*reti client server*”

# Client

Nel paragrafo sopra abbiamo citato i Client. Con Client vengono indicati tutti i componenti di una **rete informatica**, hardware o software. I computer, le stampanti, il software di posta elettronica, gli smartphone connessi tramite wi-fi, etc...

# Portata della rete

Per quanto riguarda la portata delle reti, vengono comunemente fatte le seguenti distinzioni:

- Personal Area Network (PAN) : con questo termine si indica il collegamento in rete di dispositivi situati entro un'area limitata, ad esempio in un raggio max. di 10 metri. Esempi sono la tecnologia Bluetooth o il servizio di connessione Wi-Fi ad hoc Airdrop di Apple.
- Local Area Network (LAN) : le reti locali sono tra le reti più diffuse e vengono utilizzate ad esempio in ambito domestico o nelle piccole e medie imprese.
- Metropolitan Area Network (MAN) : questo tipo di reti indica le reti presenti nelle città o in una regione.
- Wide Area Network (WAN) : un esempio di Wide Area Network è la rete DSL.
- GAN (Global Area Network) : l'esempio più conosciuto di rete globale è Internet.