FONDAMENTI DI RETI INFORMATICHE

Dalla teoria all'hardware: una guida completa

Argomento:	Reti informatiche — LAN, WAN, IP, Routing, Servizi
Destinatari:	Classe 5° Elettronica
Materiale:	Guida per l'esposizione orale

Anno Scolastico 2025/2026 — Esame di Stato

INDICE DEI CONTENUTI

1 COS'E' UNA RETE INFORMATICA

La definizione, il perche', l'analogia

Una **rete informatica** e' un insieme di due o piu' dispositivi elettronici interconnessi tra loro con lo scopo di **condividere risorse** e **scambiarsi informazioni**. Ogni dispositivo che fa parte di una rete viene chiamato **nodo** o, in ambito specifico, **host**.

Perche' esistono le reti?

- **Condivisione delle risorse**: stampanti, file, connessione internet — un solo dispositivo al servizio di tutti
- **Comunicazione**: email, messaggistica, videoconferenze — senza rete, niente di tutto questo
- **Centralizzazione dei dati**: un server unico invece di copie sparse su ogni macchina
- **Affidabilita' e ridondanza**: se un percorso cade, i dati trovano un'altra strada
- **Scalabilita'**: si aggiungono nodi senza ricostruire tutto da zero

✓ **CONCETTO CHIAVE**
ANALOGIA: Pensa alla rete stradale. Le strade sono i cavi (o le onde radio), le citta' sono i dispositivi (host), i semafori e gli svincoli sono router e switch. I pacchetti di dati sono come i camion che trasportano merci: seguono regole precise (i protocolli) per arrivare a destinazione.

I tre elementi fondamentali di ogni rete:

Elemento	Ruolo	Esempi pratici
Dispositivi (Nodi)	Generano, ricevono o instradano i dati	PC, server, smartphone, stampanti
Mezzi trasmissivi	Trasportano fisicamente i dati	Cavi UTP, fibra ottica, onde radio WiFi
Protocolli	Regole per comunicare correttamente	TCP/IP, Ethernet, HTTP, DNS

Cenno ai protocolli (trattati in dettaglio dai tuoi compagni):

Un **protocollo** e' semplicemente un insieme di regole condivise che permettono a dispositivi diversi di comunicare tra loro. Senza protocolli, ogni produttore parlerebbe la sua lingua e nessun dispositivo capirebbe l'altro. Il piu' importante e' la suite **TCP/IP**, su cui si basa tutto Internet — il funzionamento dettagliato verra' approfondito dai colleghi.

2 TIPI DI RETE: LAN, MAN, WAN, INTERNET

Classificazione per estensione geografica

Le reti si classificano in base alla loro **estensione geografica**. Capire questa distinzione e' fondamentale perche' influenza direttamente la tecnologia usata, le velocita' raggiungibili e i dispositivi necessari.

LAN — Local Area Network

Rete locale confinata in uno spazio fisico limitato: una stanza, un edificio, un campus. E' la rete che probabilmente hai in casa e che usi ogni giorno a scuola.

- Estensione: da pochi metri a qualche chilometro
- Velocita': da 100 Mbps (Fast Ethernet) a 10 Gbps (10GbE)
- Tecnologie: Ethernet (cavi UTP Cat5e/Cat6), WiFi 802.11
- Gestita direttamente da chi la possiede (privato o azienda)
- Latenza bassissima — tipicamente < 1 ms

WAN — Wide Area Network

Rete geografica che copre aree vaste: citta', regioni, nazioni o addirittura continenti. Collega tra loro piu' LAN distanti.

- Estensione: da decine di km a scala mondiale
- Velocita': variabile, da pochi Mbps a centinaia di Gbps su fibra
- Tecnologie: fibra ottica intercontinentale, MPLS, SD-WAN
- Gestita dagli ISP (Internet Service Provider)
- Latenza maggiore rispetto alla LAN (ms-decine di ms)

MAN — Metropolitan Area Network

Via di mezzo tra LAN e WAN: copre una citta' o un'area metropolitana. Tipicamente usata da operatori telefonici o grandi organizzazioni.

- Estensione: 5–50 km circa
- Tecnologie: fibra ottica, WiMAX
- Esempio: rete di una universita' su piu' campus cittadini

INTERNET — La rete delle reti

Internet non e' una singola rete ma l'interconnessione di migliaia di reti autonome (AS, Autonomous Systems) in tutto il mondo. E' la WAN piu' grande che esiste.

- Basata interamente sul protocollo TCP/IP
- Nessun proprietario centrale: e' una federazione di reti
- Circa 5 miliardi di utenti connessi (2024)
- I dati viaggiano attraverso router che instradano i pacchetti globalmente

✓ **CONCETTO CHIAVE**
DISTINZIONE PRATICA: Quando navighi su YouTube da casa, il traffico parte dal tuo PC nella LAN domestica, passa per il router (gateway), attraversa la WAN del tuo ISP e raggiunge i server Google via Internet. Tre tipi di rete in una sola operazione.

3 HOST, CLIENT E SERVER

I ruoli fondamentali nella comunicazione di rete

Host

In ambito networking, un **host** e' qualsiasi dispositivo connesso a una rete che possiede un **indirizzo IP**. Il termine e' generico: include computer, smartphone, stampanti, telecamere IP, smart TV, e qualsiasi altro dispositivo 'intelligente' con una scheda di rete. **Ogni host e' identificato univocamente** all'interno della sua rete dall'indirizzo IP assegnatogli.

Il modello Client/Server

Il paradigma dominante nelle reti moderne e' il modello **client/server**. Definisce ruoli precisi nella comunicazione:

Ruolo	Chi inizia?	Cosa fa?	Esempi
CLIENT	Inizia la comunicazione	Fa una richiesta al server e attende la risposta	Browser, app email, client FTP, app mobile
SERVER	Aspetta passivamente	Riceve la richiesta, elabora e risponde	Web server, mail server, file server, DNS server

Il server: cosa e' fisicamente?

Un server **non e' necessariamente un hardware speciale**: e' il software che gira su un host che lo rende un server. Detto questo, in ambienti professionali i server sono macchine progettate per:

- Funzionare **24/7 senza interruzioni** (alta disponibilita')
- Gestire **molte richieste simultanee** (alta concorrenza)
- Garantire **affidabilita' e ridondanza** (RAID, alimentatori doppi, ECC RAM)
- Essere installati in **rack** all'interno di datacenter climatizzati

ATTENZIONE

ATTENZIONE: Un host puo' essere client e server allo stesso tempo! Il tuo PC e' client quando scarica email, ma diventa server se hai abilitato la condivisione file. Questa e' la base del modello PEER-TO-PEER.

Peer-to-Peer (P2P)

Alternativa al modello client/server: ogni nodo e' contemporaneamente client e server. Non esiste una gerarchia. Usato in: BitTorrent, blockchain, reti VoIP (Skype originale). Vantaggio: nessun single point of failure. Svantaggio: difficile da gestire e proteggere.

B

MODELLO OSI E SUITE TCP/IP

Come i protocolli sono organizzati a livelli

I protocolli di rete sono organizzati in **livelli (layer)**: ogni livello si occupa di una funzione specifica e usa i servizi del livello sottostante, offrendo i propri al livello superiore. Questo approccio modulare permette di sostituire o aggiornare un layer senza modificare gli altri.

Il Modello OSI — 7 Layer

L'OSI (Open Systems Interconnection) è il modello di riferimento teorico, sviluppato dall'ISO negli anni '80. Non è usato direttamente in produzione, ma è lo standard universale per descrivere e diagnosticare le reti.

N.	Layer	Protocolli/Standard	Funzione
7	APPLICATION	`HTTP, HTTPS, FTP, SMTP, DNS, SSH`	Interfaccia con le applicazioni utente. Fornisce servizi di rete alle app (browser, client email…).
6	PRESENTATION	`TLS/SSL, JPEG, MP4, ASCII, UTF-8`	Traduzione, cifratura e compressione dei dati. Garantisce che i dati siano leggibili dal destinatario.
5	SESSION	`NetBIOS, RPC, SIP`	Gestisce l'apertura, il mantenimento e la chiusura delle sessioni di comunicazione.
4	TRANSPORT	`TCP, UDP`	Trasporto end-to-end affidabile (TCP) o veloce senza garanzie (UDP). Porte, segmentazione, controllo flusso.
3	NETWORK	`IP (v4/v6), ICMP, ARP, Routing`	Indirizzamento logico (IP) e routing dei pacchetti tra reti diverse. Il layer del router.
2	DATA LINK	`Ethernet, WiFi 802.11, PPP`	Trasferimento frame tra nodi adiacenti. Indirizzamento MAC, rilevamento errori. Il layer dello switch.
1	PHYSICAL	`Cavi UTP, Fibra, WiFi (onde radio)`	Trasmissione grezza di bit sul mezzo fisico: tensioni elettriche, impulsi ottici, onde radio.

✓ **CONCETTO CHIAVE**

REGOLA MNEMONICA: 'All People Seem To Need Data Processing' (Application, Presentation, Session, Transport, Network, Data Link, Physical) — oppure dal basso: 'Please Do Not Throw Sausage Pizza Away'.

Il Modello TCP/IP — 5 Layer (modello pratico)

Il modello TCP/IP è il modello **realmente usato in Internet**. Semplifica l'OSI condensando alcuni layer. Esistono versioni a 4 e a 5 layer: qui usiamo la versione a 5 layer (la più usata in ambito didattico e professionale).

L.	Layer TCP/IP	Protocolli chiave	Funzione — unità dati
5	APPLICATION	`HTTP/S · FTP · SMTP · DNS · SSH`	Racchiude i layer 5-6-7 dell'OSI. Le applicazioni comunicano direttamente qui. I dati si chiamano messaggi o dati.
4	TRANSPORT	`TCP · UDP`	Gestione connessioni end-to-end. TCP = affidabile (ACK, ritrasmissione). UDP = veloce senza garanzie. Unità: segmento (TCP) / datagramma (UDP).
3	INTERNET	`IPv4 · IPv6 · ICMP · ARP`	Instradamento (routing) tra reti diverse via indirizzo IP. Corrisponde al Layer 3 OSI. Unità: pacchetto.
2	NETWORK ACCESS (Data Link)	`Ethernet · WiFi 802.11 · PPP`	Trasmissione frame tra nodi adiacenti sulla stessa rete. Indirizzamento MAC. Corrisponde ai Layer 1+2 OSI. Unità: frame.
1	PHYSICAL	`Cavi UTP/Fibra · Onde radio · Segnali elettrici`	Trasmissione grezza di bit sul mezzo fisico. Tensioni, impulsi di luce, onde radio. Unità: bit.

■ NOTA
COME I DUE MODELLI SI CONFRONTANO: OSI layer 7+6+5 = TCP/IP Application. OSI layer 4 = TCP/IP Transport. OSI layer 3 = TCP/IP Internet. OSI layer 2+1 = TCP/IP Network Access. In pratica si usa TCP/IP, si usa OSI per parlare e diagnosticare.

OSI vs TCP/IP — Corrispondenza tra i modelli

Layer OSI	N. OSI	Layer TCP/IP (5L)	Dispositivo tipico
Application	7	Application	—
Presentation	6		—
Session	5		—
Transport	4	Transport	Firewall L4
Network	3	Internet	Router
Data Link	2		Switch
Physical	1	Network Access	Hub, Cavi, NIC

** I layer Application (7,6,5 OSI) sono unificati in un unico layer Application nel modello TCP/IP. I layer Physical e Data Link (1,2 OSI) sono unificati nel layer Network Access TCP/IP.*

4 HARDWARE DI RETE — NIC, CAVI, CONNETTORI

L'infrastruttura fisica: dove tutto inizia

Prima di capire come i dati viaggiano in rete, dobbiamo capire **su cosa fisicamente viaggiano**. L'hardware di rete e' il fondamento di tutto: senza di esso, nessun protocollo puo' funzionare.

NIC — Network Interface Card

La **NIC** (o scheda di rete) e' il componente hardware che permette a un host di connettersi fisicamente alla rete. Ogni NIC possiede un indirizzo **MAC (Media Access Control)** univoco, 'bruciato' in fabbrica dal produttore. Pensa al MAC come alla **targa di un'auto**: e' fissa, assegnata alla macchina, non cambia mai. L'IP invece e' come la **posizione GPS**: cambia a seconda di dove ti trovi.

Caratteristica	Dettaglio
Indirizzo MAC	48 bit (6 byte) in notazione esadecimale — es. AA:BB:CC:DD:EE:FF
Struttura MAC	Primi 3 byte = OUI (produttore) | Ultimi 3 byte = numero seriale
Layer OSI	Opera a Layer 2 (Data Link) per Ethernet
Tipologie	Ethernet RJ-45, WiFi 802.11, Fibra ottica SFP
Velocita' comuni	100 Mbps (Fast), 1 Gbps (GbE), 10 Gbps (10GbE), 40/100 Gbps (datacenter)

Cavi Ethernet — Categorie e standard

I cavi UTP (Unshielded Twisted Pair) sono il mezzo trasmissivo piu' diffuso nelle reti locali. Il 'twisted' (intrecciato) riduce le interferenze elettromagnetiche tra le coppie di fili.

Categoria	Max velocita'	Max distanza	Frequenza	Uso tipico
Cat 5e	1 Gbps	100 m	100 MHz	Reti domestiche legacy
Cat 6	10 Gbps	55 m (10G) 100 m (1G)	250 MHz	Uffici, reti aziendali
Cat 6A	10 Gbps	100 m	500 MHz	Standard attuale consigliato
Cat 7	10 Gbps	100 m	600 MHz	Ambienti con alte interferenze
Cat 8	25-40 Gbps	30 m	2000 MHz	Datacenter, top-of-rack

** Cat 6A e' lo standard consigliato per nuove installazioni*

Fibra ottica

La fibra ottica trasmette dati come **impulsi di luce** attraverso un nucleo di vetro o plastica. Vantaggi rispetto al rame: velocita' elevatissime, distanze enormi (decine di km), immunita' alle interferenze elettromagnetiche.

- **Single-mode (SMF)**: nucleo 9 micron, luce laser, distanze fino a 100 km, per WAN e backbone
- **Multi-mode (MMF)**: nucleo 50/62.5 micron, LED, distanze fino a 500 m, per reti intra-edificio
- Connettori: LC (piu' comune), SC, ST — il connettore non determina le prestazioni, solo il cavo

5 SWITCH — LA RETE LOCALE

Layer 2, MAC address, forwarding intelligente

Lo **switch** e' il dispositivo centrale della LAN. Il suo compito e' **connettere piu' dispositivi nella stessa rete locale** e fare in modo che i dati arrivino solo al destinatario corretto, senza inondare tutta la rete.

Come funziona: MAC address table

Lo switch impara **dove si trova ogni dispositivo** osservando il traffico. Ad ogni frame Ethernet che riceve, legge il **MAC address sorgente** e registra su quale porta e' arrivato. Costruisce cosi' una tabella interna. E' come un **portinaio intelligente** di un condominio: la prima volta che vede qualcuno uscire dall'appartamento 3 segna 'Rossi abita al piano 3'; la volta successiva, invece di suonare a tutti i campanelli (broadcast), porta la posta direttamente al piano giusto.

MAC Address	Porta	VLAN	Appreso da
`AA:BB:CC:DD:EE:01`	Gi0/1	VLAN 10	Traffico in ingresso
`AA:BB:CC:DD:EE:02`	Gi0/2	VLAN 10	Traffico in ingresso
`AA:BB:CC:DD:EE:03`	Gi0/5	VLAN 20	Traffico in ingresso

I tre comportamenti fondamentali dello switch

UNICAST (known destination)

Il MAC destinazione e' nella tabella: il frame viene inviato SOLO sulla porta corrispondente. Questo e' il comportamento normale e ottimale.

BROADCAST / FLOOD (unknown destination)

Il MAC destinazione NON e' in tabella (o il frame e' broadcast FF:FF:FF:FF:FF:FF): il frame viene inviato su TUTTE le porte tranne quella sorgente. Lo switch 'impara' la risposta.

FILTERING

Sorgente e destinazione sono sulla stessa porta (stesso segmento): il frame viene scartato perche' si 'parlano da soli'. Risparmio di banda.

Switch vs Hub — Perche' lo switch ha vinto

Caratteristica	Hub (obsoleto)	Switch (moderno)
Logica	Nessuna — ripete su tutte le porte	Intelligente — usa MAC table
Dominio di collisione	Unico per tutte le porte	Uno per ogni porta
Dominio di broadcast	Condiviso	Condiviso (ma controllabile con VLAN)
Banda	Condivisa tra tutti	Dedicata per ogni connessione
Layer OSI	Layer 1 (fisico)	Layer 2 (data link)
Utilizzo oggi	Praticamente zero	Standard in ogni rete

■ **DETTAGLIO TECNICO**
I moderni switch managed (gestiti) offrono funzionalita' avanzate come VLAN, QoS, Port Security, Spanning Tree Protocol (STP), Link Aggregation (LACP) e mirroring delle porte per il monitoraggio del traffico.

6 ROUTER — IL COLLEGAMENTO TRA RETI

Layer 3, routing table, gateway di default

Il **router** e' il dispositivo responsabile di **instradare i pacchetti tra reti diverse**. Se lo switch connette dispositivi nella stessa LAN, il router connette reti diverse tra loro: la tua LAN domestica con Internet, o la rete di sede con quella della filiale.

Differenza fondamentale Switch vs Router

	Switch	Router
Lavora a	Layer 2 — Data Link	Layer 3 — Network
Usa come indirizzo	MAC address (fisico)	IP address (logico)
Connette	Dispositivi nella stessa rete	Reti diverse tra loro
Conosce	MAC table	Routing table
Separa i broadcast?	No (stessa LAN li vede tutti)	Si — ogni interfaccia è un dominio broadcast separato

La routing table — Il cuore del router

Il router decide dove mandare ogni pacchetto consultando la sua **routing table** (tabella di routing). Ogni entry dice: *'Per raggiungere la rete X, manda il pacchetto verso il router Y tramite l'interfaccia Z'*. E' esattamente come il **navigatore GPS della tua auto**: non conosce ogni singola strada del mondo, ma sa qual e' la prossima svolta da prendere per avvicinarsi alla destinazione.

```
Destination Mask Gateway Interface Metric 0.0.0.0 0.0.0.0 203.0.113.1 eth0 1 (default)
192.168.1.0 255.255.255.0 0.0.0.0 eth1 0 (LAN locale) 10.0.0.0 255.0.0.0 192.168.1.254
eth1 10 (rete remota) 192.168.2.0 255.255.255.0 192.168.1.254 eth1 5 (filiale)
```

Gateway di default

Il **gateway di default** (o default gateway) e' l'indirizzo IP del router a cui un host invia tutti i pacchetti destinati a reti che non conosce. E' letteralmente la 'porta di uscita' dalla LAN. In una rete domestica tipica e' l'indirizzo del router/modem: solitamente **192.168.1.1** o **192.168.0.1**.

Routing statico vs dinamico

ROUTING STATICO	Le rotte sono configurate manualmente dall'amministratore. Semplice, prevedibile, nessun overhead. Usato in reti piccole o su percorsi fissi (es. default route verso Internet).
ROUTING DINAMICO	I router si 'parlano' tra loro usando protocolli di routing (OSPF, BGP, EIGRP) e aggiornano automaticamente le tabelle. Adattivo ai guasti. Essenziale su Internet e nelle grandi reti aziendali. BGP e' il 'protocollo di Internet'.

7 INDIRIZZI IP — IPv4 E CENNI IPv6

La logica dell'indirizzamento in rete

L'**indirizzo IP** (Internet Protocol) e' l'indirizzo logico assegnato a ogni interfaccia di rete. A differenza del MAC address (fisso in hardware), l'IP e' **configurabile e gerarchico**: questa gerarchia e' fondamentale per il routing su scala globale.

Struttura indirizzo IPv4 — 192.168.1.100 / 24

Parte di RETE (subnet /24 → 3 ottetti fissi)
Parte di HOST (ottetto variabile → da .1 a .254)

Struttura di un indirizzo IPv4 — parte di rete e parte di host

Classi di indirizzi IPv4

Classe	Range primo ottetto	Subnet mask default	N. reti	Host/rete	Uso
A	1–126	255.0.0.0 /8	128	16.777.214	Grandi organizzazioni
B	128–191	255.255.0.0 /16	16.384	65.534	Medie imprese, ISP
C	192–223	255.255.255.0 /24	2.097.152	254	Reti piccole (case, uffici)
D	224–239	—	—	—	Multicast
E	240–255	—	—	—	Riservato / sperimentale

Indirizzi privati (RFC 1918) — Non instradabili su Internet

Range	Classe	Subnet CIDR	N. indirizzi	Uso tipico
`10.0.0.0 – 10.255.255.255`	A	/8	16.777.216	Grandi reti aziendali, datacenter
`172.16.0.0 – 172.31.255.255`	B	/12	1.048.576	Reti medie, VPN
`192.168.0.0 – 192.168.255.255`	C	/16	65.536	Reti domestiche e PMI

ATTENZIONE
Gli indirizzi privati NON sono instradabili su Internet. Il router di casa usa il NAT (Network Address Translation) per tradurre l'IP privato (es. 192.168.1.5) nel tuo IP pubblico assegnato dall'ISP prima di inviare il traffico verso Internet.

Indirizzi speciali da conoscere

- `127.0.0.1`: Loopback — 'me stesso'. Usato per testare lo stack TCP/IP locale senza hardware
- `0.0.0.0`: Indirizzo non specificato — usato nella routing table come 'default route'
- `255.255.255.255`: Broadcast limitato — inviato a tutti nella rete locale
- `169.254.x.x`: APIPA — assegnato automaticamente se il DHCP non risponde (Automatic Private IP Addressing)

IPv6 — Perche' esiste e in cosa differisce

IPv4 offre circa 4,3 miliardi di indirizzi. Con la crescita esplosiva di dispositivi connessi (IoT, smartphone, auto), questi stanno esaurendo. **IPv6** risolve il problema con uno spazio di indirizzi astronomico:

- Lunghezza: **128 bit** contro i 32 di IPv4 — 3,4 x 10^{38} indirizzi (praticamente infiniti)
- Notazione: `2001:0db8:85a3:0000:0000:8a2e:0370:7334` — 8 gruppi da 4 cifre esadecimali
- Nessun NAT necessario: ogni dispositivo ha il suo IP pubblico
- SLAAC: auto-configurazione senza DHCP (Stateless Address Autoconfiguration)
- Coesistenza con IPv4: **dual stack** — la maggior parte delle reti moderne usa entrambi

8 SUBNET MASK — DIVIDERE LA RETE

CIDR notation, network/host, broadcast address

La **subnet mask** (maschera di sottorete) e' un numero di 32 bit che indica quali bit dell'indirizzo IP appartengono alla **parte di rete** e quali alla **parte di host**. E' inseparabile dall'indirizzo IP: un IP senza subnet mask e' incompleto.

Notazione CIDR (Classless Inter-Domain Routing)

La notazione CIDR affianca all'IP il numero di bit 'uno' nella subnet mask. E' piu' compatta e oggi universalmente usata:

Notazione CIDR	Subnet Mask	Indirizzi totali	Host utilizzabili	Uso pratico
`/8`	255.0.0.0	16.777.216	16.777.214	Reti backbone ISP
`/16`	255.255.0.0	65.536	65.534	Grandi aziende
`/24`	255.255.255.0	256	254	LAN ufficio/casa — lo standard
`/25`	255.255.255.128	128	126	Subnetting /24 in due meta'
`/26`	255.255.255.192	64	62	Subnetting — 4 subnet da /24
`/30`	255.255.255.252	4	2	Link punto-punto tra router
`/32`	255.255.255.255	1	0	Host route singolo

Host utilizzabili = Indirizzi totali – 2 (network address e broadcast address)

Esempio pratico — Rete 192.168.1.0/24

Dato: `192.168.1.50/24` — calcola tutti gli indirizzi significativi:

Tipo	Indirizzo	Spiegazione
Network address	`192.168.1.0`	Identifica la rete — non assegnabile a host
Primo host	`192.168.1.1`	Primo indirizzo usabile (tipicamente il router)
Host generico	`192.168.1.50`	Il nostro indirizzo — assegnato a un dispositivo
Ultimo host	`192.168.1.254`	Ultimo indirizzo usabile
Broadcast	`192.168.1.255`	Inviato a TUTTI gli host della rete

■ DETTAGLIO TECNICO
FORMULA: Host utilizzabili = 2^n - 2, dove n = numero di bit della parte host. Per /24: n = 32 - 24 = 8 bit host → 2^8 - 2 = 256 - 2 = 254 host.

Come leggere una subnet mask — passo per passo

La subnet mask in binario e' sempre una sequenza di '1' seguita da '0'. Gli '1' indicano i bit della RETE, gli '0' indicano i bit dell'HOST. Vediamo come funziona concretamente:

Notazione	In binario (32 bit)	Significato
`/8 = 255.0.0.0`	`11111111.00000000.00000000.00000000`	8 bit rete, 24 bit host → 16 milioni di host
`/16 = 255.255.0.0`	`11111111.11111111.00000000.00000000`	16 bit rete, 16 bit host → 65.534 host
`/24 = 255.255.255.0`	`11111111.11111111.11111111.00000000`	24 bit rete, 8 bit host → 254 host
`/30 = 255.255.255.252`	`11111111.11111111.11111111.11111100`	30 bit rete, 2 bit host → solo 2 host (link P2P)

✓ **CONCETTO CHIAVE**
TRUCCO MENTALE: Il numero dopo la slash (/) ti dice quanti bit sono 1 nella maschera. /24 = 24 bit a 1 = tre ottetti fissi = la parte che identifica la rete. Piu' grande e' il numero, piu' piccola e' la rete (meno host ci stanno).

9 DHCP — ASSEGNAZIONE AUTOMATICA DEGLI IP

Dynamic Host Configuration Protocol — RFC 2131

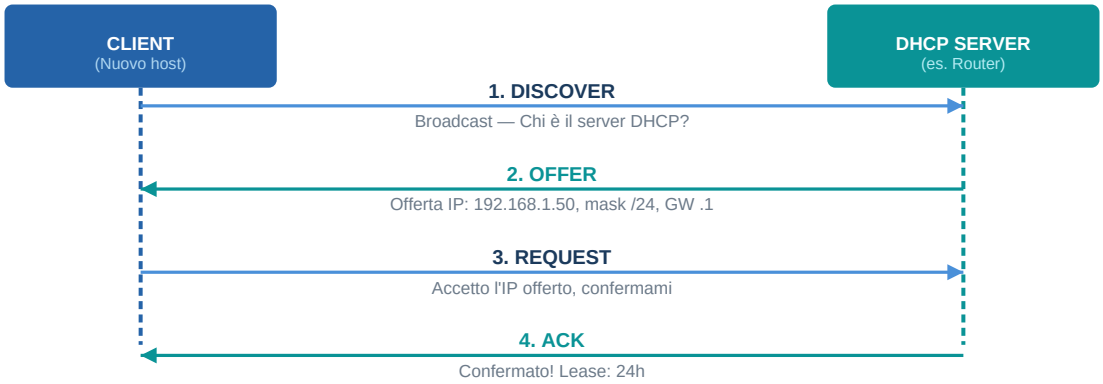
Il **DHCP** (Dynamic Host Configuration Protocol) e' il protocollo che permette a un dispositivo di ottenere **automaticamente** tutti i parametri necessari per funzionare in rete, senza alcuna configurazione manuale. Senza DHCP, ogni dispositivo andrebbe configurato a mano — impensabile con migliaia di host.

Analogia: immagina di entrare per la prima volta in un grande ufficio. Non sai dove sederti, qual e' il numero del telefono, chi e' il tuo referente. Il DHCP e' come l'**addetto all'accoglienza**: ti assegna una scrivania (IP), ti dice qual e' la porta d'uscita (gateway), ti da' la rubrica (DNS) e ti dice per quanto tempo quella scrivania e' tua (lease time).

Parametri forniti dal DHCP

- **Indirizzo IP**: l'indirizzo assegnato al client per la durata del lease
- **Subnet mask**: la maschera della rete (es. /24)
- **Default gateway**: l'IP del router — la porta di uscita dalla LAN
- **DNS server**: gli indirizzi dei resolver DNS da usare
- **Lease time**: la durata dell'assegnazione (es. 24 ore, 7 giorni)
- (Opzionale) **NTP server**, domain name, WINS, e altri parametri avanzati

Il processo DORA — Come il client ottiene un IP



Handshake DHCP — sequenza DORA (Discover, Offer, Request, Acknowledge)

DISCOVER	Il client, appena connesso, non ha ancora un IP. Invia un pacchetto broadcast (MAC FF:FF:FF:FF:FF:FF, IP dst 255.255.255.255) chiedendo: 'C'e' un server DHCP in questa rete?'
OFFER	Il server DHCP risponde offrendo un indirizzo IP disponibile dal suo pool, insieme a tutti i parametri di rete. Se ci sono piu' server, il client accetta la prima offerta.
REQUEST	Il client risponde confermando di voler accettare l'IP offerto (ancora in broadcast, per notificare tutti i server che ha scelto).
ACKNOWLEDGE	Il server conferma l'assegnazione. Il client puo' ora usare l'indirizzo IP. Il server segna l'IP come 'in uso' per la durata del lease.

IP statico vs IP dinamico

	IP dinamico (DHCP)	IP statico (manuale)
Configurazione	Automatica — zero intervento	Manuale — da admin o utente
Permanenza	Cambia al rinnovo del lease	Fisso — non cambia mai
Uso tipico	Client, laptop, smartphone	Server, stampanti, router, telecamere IP
Gestione	Centralizzata nel server DHCP	Distribuita — rischio di conflitti IP

10

DNS — LA RUBRICA DI INTERNET

Domain Name System — RFC 1034/1035

Il **DNS** (Domain Name System) e' il sistema che traduce i **nomi di dominio** leggibili dagli umani (come *www.google.com*) negli **indirizzi IP** che i computer usano per comunicare. Senza DNS, dovremmo ricordare l'IP numerico di ogni sito che vogliamo visitare — esattamente come prima dei telefoni cellulari dovevamo memorizzare tutti i numeri a mano. Il DNS e' la **rubrica telefonica di Internet**: tu cerchi il nome, lui ti da' il numero.

Gerarchia DNS — Come e' strutturato il sistema

Root servers	.

13 cluster di server root nel mondo (identificati da a.root-servers.net a m.root-servers.net). Conoscono chi gestisce ogni TLD. Punto di partenza di ogni risoluzione.

TLD servers	.com .it .org .net .edu

Top Level Domain servers: gestiscono i domini di primo livello. Verisign gestisce .com e .net, il Registro.it gestisce .it.

Authoritative NS	ns1.google.com

Il server DNS 'autorevole' per uno specifico dominio. Ha la risposta definitiva. Se chiedi l'IP di google.com, risponde il name server di Google.

Resolver (Recursive)	8.8.8.8 1.1.1.1 ISP DNS

Il resolver ricorsivo e' quello che interroghi tu (configurato dal DHCP). Si occupa di fare tutto il lavoro: interroga root, TLD e authoritative per conto tuo.

Processo di risoluzione — Cosa succede quando scrivi 'www.google.com'

1. Il browser controlla la sua **cache locale**. Se l'ha gia' risolto di recente, usa quello.
2. Controlla il file **hosts** di sistema (/etc/hosts o C:\Windows\System32\drivers\etc\hosts).
3. Interroga il **resolver ricorsivo** configurato (es. 8.8.8.8 di Google o DNS dell'ISP).
4. Il resolver chiede al **root server**: 'Chi gestisce .com?'
5. Root server risponde con i **TLD server** per .com.
6. Il resolver chiede al **TLD server**: 'Chi gestisce google.com?'
7. TLD server risponde con i **name server autoritativi** di Google.
8. Il resolver chiede al **name server di Google**: 'Qual e' l'IP di www.google.com?'
9. Risposta: {b('142.250.x.x')} — l'IP viene restituito al browser e **messo in cache** (TTL).
10. Il browser si connette all'IP e carica la pagina.

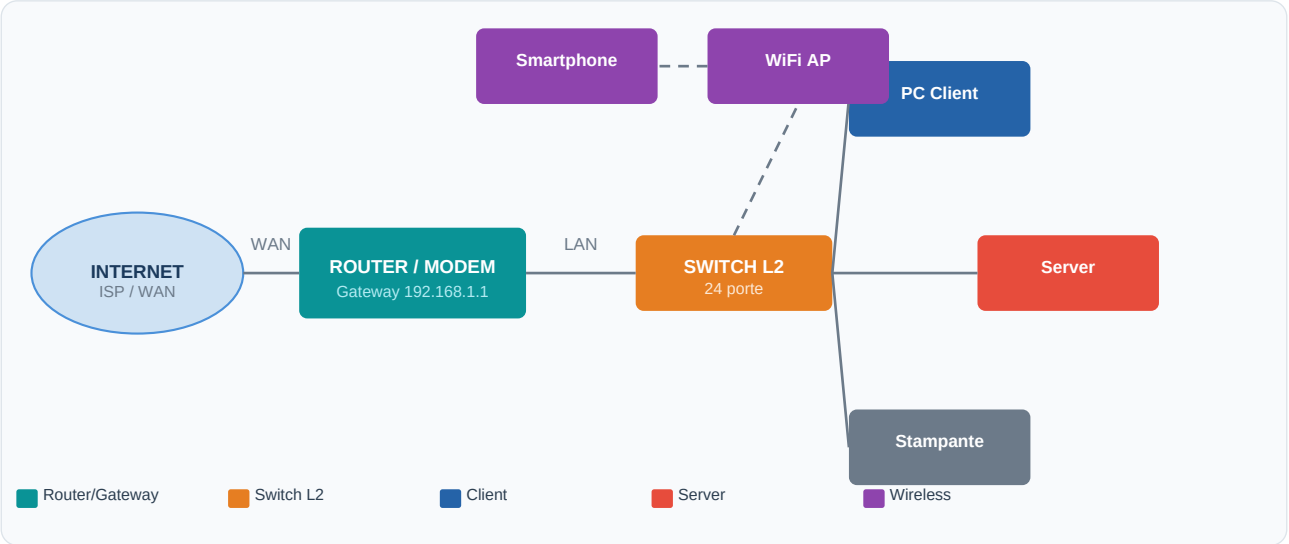
Record DNS fondamentali

Tipo	Nome	Funzione	Esempio
A	Address	Nome → IPv4	google.com → 142.250.74.46
AAAA	Quad-A	Nome → IPv6	google.com → 2a00:1450:4002:806::200e
CNAME	Alias	Nome → altro nome	www → google.com
MX	Mail Exchange	Dominio → mail server	google.com → smtp.google.com
NS	Name Server	Dominio → name server	google.com → ns1.google.com
PTR	Pointer	IPv4 → nome (reverse DNS)	142.250.74.46 → google.com
TXT	Text	Testo libero (SPF, DKIM…)	Verifica dominio, anti-spam

11 ESEMPIO PRATICO — RETE REALE

Tutto insieme: dalla presa a muro al server web

Ora che abbiamo tutti i pezzi, vediamo come si compongono in una **rete aziendale reale**. Seguiamo il percorso di una richiesta HTTP dall'utente al server web, identificando ogni componente.



Schema rete tipica — dalla LAN all'Internet

Cosa succede quando un utente apre 'www.example.com'

1	**PC si connette alla rete**	Il PC ottiene IP, subnet mask, gateway e DNS via DHCP dal router. Es: IP 192.168.1.42/24, gateway 192.168.1.1, DNS 192.168.1.1
2	**Risoluzione DNS**	Il browser interroga il DNS (192.168.1.1). Il router forwarda la query al DNS dell'ISP o a 8.8.8.8. Risposta: example.com → 93.184.216.34
3	**Routing verso Internet**	Il pacchetto ha dst 93.184.216.34 (non nella LAN). Il PC lo manda al gateway 192.168.1.1. Il router applica NAT: traduce 192.168.1.42 → IP pubblico assegnato dall'ISP.
4	**Lo switch nella LAN**	Il frame Ethernet dal PC raggiunge lo switch. Lo switch consulta la MAC table: porta 3 → router. Forwarda il frame solo su quella porta. Zero sprechi.
5	**Il server risponde**	Il server web (IP 93.184.216.34) riceve la richiesta HTTP, elabora e risponde. La risposta torna attraverso lo stesso percorso in senso inverso.

Riepilogo dispositivi e loro layer OSI

Dispositivo	Layer OSI	Indirizzo usato	Funzione principale
NIC / Cavo	Layer 1 — Fisico	Segnale elettrico/ottico	Trasmissione bit
Switch	Layer 2 — Data Link	MAC address	Forwarding nella LAN
Router	Layer 3 — Network	IP address	Routing tra reti
Firewall	Layer 3-7	IP + porta + payload	Filtraggio traffico
Load balancer	Layer 4-7	IP + TCP/UDP	Distribuzione del carico

NOTA
PUNTO DI PASSAGGIO per i tuoi compagni: tutto questo traffico usa protocolli precisi a ogni layer. TCP garantisce la consegna affidabile (layer 4), IP gestisce il routing (layer 3), Ethernet gestisce il link locale (layer 2). I tuoi compagni approfondiranno TCP/IP, HTTP, e il modello OSI completo nelle esposizioni successive.

A INFRASTRUTTURA FISICA DI INTERNET

Dai cavi sottomarini al router di casa

Prima di capire come funziona Internet in astratto, vale la pena vedere **come è fatto fisicamente**: dalla fibra posata sul fondo degli oceani fino al cavo che entra nel tuo router di casa.

1	**CAVI SOTTOMARINI (Submarine Cables)**	La dorsale di Internet è letteralmente posata sul fondo degli oceani. Cavi in fibra ottica lunghi migliaia di km collegano i continenti. Ogni cavo trasporta decine di Tbps di traffico. Sono gestiti da consorzi di operatori (Google, Meta, Telecom Italia, ecc.). Oggi esistono oltre 400 cavi sottomarini attivi nel mondo.
2	**LANDING STATION & IXP**	I cavi sottomarini approdano a terra nelle Landing Station (stazioni di atterraggio). Da lì il traffico entra negli IXP — Internet Exchange Point: punti neutri dove gli operatori (ISP, CDN, cloud provider) si interconnettono fisicamente per scambiarsi traffico a costi ridotti. In Italia il principale è il MIX di Milano.
3	**POP NAZIONALE (Point of Presence)**	I grandi ISP nazionali (TIM, Fastweb, Vodafone…) hanno datacenter distribuiti sul territorio — i POP Nazionali. Qui si trovano i router core che gestiscono il traffico a livello di backbone nazionale, collegati tra loro e agli IXP con fibra a 100 Gbps o più.
4	**POP DI ZONA / QUARTIERE**	Dal POP Nazionale il segnale scende ai POP di zona, armadi o locali tecnici distribuiti nei quartieri delle città. Da qui partono i collegamenti verso le singole abitazioni e uffici — tipicamente via fibra FTTH (Fiber To The Home) o rame VDSL/ADSL nelle zone non ancora cablate.
5	**MUFFOLA / ROE (Ripartitore Ottico di Edificio)**	Nel caso della fibra FTTH, la fibra arriva fino alla muffola o ROE — un piccolo armadio o scatola posizionata in strada o al piano terra dell'edificio. Qui il cavo in fibra viene splittato (diviso) per i diversi appartamenti/unità dell'edificio tramite uno splitter ottico passivo.
6	**PTE (Punto di Terminazione della rete)**	Il PTE è il punto dove la rete dell'operatore termina e inizia la rete del cliente: tipicamente una presa ottica a muro (per FTTH) o la borchia telefonica (per ADSL/VDSL). Da qui parte il breve cavo che collega al tuo ONT/modem.
7	**ONT + ROUTER DI CASA**	L'ONT (Optical Network Terminal) converte il segnale ottico in segnale elettrico Ethernet. Il router domestico (spesso combinato con l'ONT) gestisce la LAN di casa: assegna IP via DHCP, fa NAT verso Internet, fornisce il WiFi. Il tuo PC ottiene infine l'IP privato (es. 192.168.1.x) e può navigare.

✓ **CONCETTO CHIAVE**
PERCORSO COMPLETO: Il tuo browser → router di casa (NAT) → ONT → PTE → muffola/ROE → POP di zona → POP Nazionale → IXP → cavo sottomarino → datacenter dall'altra parte del mondo. Tutto in meno di 50 ms.

RIEPILOGO — I CONCETTI CHIAVE

Tutto quello che devi ricordare

Mappa dei concetti

RETE	Due o piu' dispositivi che comunicano per condividere risorse
LAN / WAN	Classificazione per estensione geografica — da casa a Internet
HOST	Qualsiasi dispositivo con indirizzo IP in rete
CLIENT/SERVER	Chi fa la richiesta vs chi risponde — il paradigma dominante
NIC	Scheda di rete — il punto di accesso fisico, con MAC address univoco
SWITCH	Connette dispositivi nella LAN usando MAC table — Layer 2
ROUTER	Connette reti diverse usando routing table — Layer 3, default gateway
IPv4	32 bit, 4 ottetti — privati (192.168.x.x) non instradabili su Internet
SUBNET MASK	Distingue parte rete e parte host — /24 = 254 host, /30 = 2 host
DHCP	Assegna IP automaticamente con il processo DORA — Discover Offer Request Ack
DNS	Traduce nomi in IP — record A, CNAME, MX — risoluzione gerarchica

✓ **CONCETTO CHIAVE**

Il percorso di un pacchetto: PC → NIC → cavo → Switch (MAC table) → Router (IP table) → Internet → Server. A ogni salto, un layer OSI diverso. A ogni layer, un indirizzo diverso. Questo e' il cuore del networking moderno.