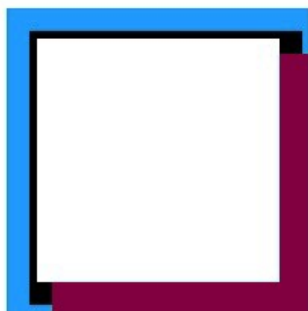


MINI MANUALE RETI v.1.5



ingvitel

sito web di riferimento: <https://ingvitel.altervista.org>

Divulgazione a solo scopo didattico

Indice generale

Avvertenze e Note Legali.....	3
1.1 Tabella protocollare ISO/OSI e TCP/IP.....	4
1.2 Indipendenza modulare dei singoli livelli ISO/OSI, spiegazione concettuale.....	5
1.3 Standard RFC e documentazione di riferimento.....	6
1.4 Elenco e descrizione dei principali protocolli, algoritmi e tecniche di riferimento.....	6
1.5 Standard IEEE 802.....	16
1.6 Altre definizioni.....	17
2.1 Progettazione di una rete.....	18
2.2 Analisi essenziali dei requisiti di rete (rif. fase 1).....	19
2.3 Scelta e analisi topologia della rete (rif. fase 2).....	20
2.4 Classificazione dispositivi attivi (rif. fase 3).....	26
2.5 Scelta e analisi modalità di connessione (rif. fase 4).....	28
3.1 Indirizzamento IPv4.....	31
3.2 Formule IPv4.....	33
3.3 Rete, sottorete e subnetting.....	34
3.4 Progetto SUBNETTING N.1.....	35
4.1 Router e le tecniche di Routing.....	39
4.2 Il Router.....	39
4.3 Fondamenti di Routing.....	39
4.4 Il Default Gateway.....	39
4.5 Routing Statico.....	39
4.6 Routing Dinamico.....	40
4.7 Algoritmo di Dijkstra.....	40
4.8 Algoritmo di Bellman-Ford.....	40
4.9 Il RIP, OSPF e EIGRP.....	40
4.10 Cenni di Routing Gerarchico, Concetto di Area ID.....	40
5.1 Bibliografia:.....	42

Avvertenze e Note Legali

Nel rispetto della legge sul diritto d'autore 22/04/1941 n° 633, G.U. 16/07/1941, e successiva integrazione L. 9/01/2008, n°2, si fa presente al lettore che il presente testo **"MINI MANUALE RETI v1.4"**, oltre la parte esclusiva di ingegno e redazione propria, contiene materiale opportunamente selezionato dalla rete e/o da altre opere esclusivamente per fini di insegnamento e discussione. Inoltre sono stati inseriti i riferimenti bibliografici per ogni riproduzione parziale di opere dell'ingegno e creatività. Per completezza di informazione riportiamo qui l'art. di pubblico interesse della legge sopracitata.

Art. 70.

1. Il riassunto, la citazione o la riproduzione di brani o di parti di opera e la loro comunicazione al pubblico sono liberi se effettuati per uso di critica o di discussione, nei limiti giustificati da tali fini e purché non costituiscano concorrenza all'utilizzazione economica dell'opera; se effettuati a fini di insegnamento o di ricerca scientifica l'utilizzo deve inoltre avvenire per finalità illustrative e per fini non commerciali.

1-bis. E' consentita la libera pubblicazione attraverso la rete internet, a titolo gratuito, di immagini e musiche a bassa risoluzione o degradate, per uso didattico o scientifico e solo nel caso in cui tale utilizzo non sia a scopo di lucro. Con decreto del Ministro per i beni e le attività culturali, sentiti il Ministro della pubblica istruzione e il Ministro dell'università e della ricerca, previo parere delle Commissioni parlamentari competenti, sono definiti i limiti all'uso didattico o scientifico di cui al presente comma.(1)

2. Nelle antologie ad uso scolastico la riproduzione non può superare la misura determinata dal regolamento, il quale fissa la modalità per la determinazione dell'equo compenso.

3. Il riassunto, la citazione o la riproduzione debbono essere sempre accompagnati dalla menzione del titolo dell'opera, dei nomi dell'autore, dell'editore e, se si tratti di traduzione, del traduttore, qualora tali indicazioni figurino sull'opera riprodotta.

(1) Comma aggiunto dalla L. 9 gennaio 2008, n. 2.

*Inoltre l'art. 10 della Convenzione di Berna, mentre rinvia, nel comma 2, alle legislazioni nazionali per la disciplina dell'utilizzazione a titolo illustrativo (**peraltro a fini di insegnamento**), dichiara lecita la citazione dell'opera se contenuta "nella misura giustificata dallo scopo", e richiede quindi che la riproduzione parziale di un'opera per poter esser considerata quale lecita citazione della stessa, si inserisca funzionalmente in un discorso, quale premessa o quale mezzo di convalida o di critica delle tesi ivi sostenute. (cfr. Cassazione civile, sez. I, 07 marzo 1997, n. 208).*

Durante le attività raccolta del materiale, preparazione e divulgazione di quest'opera l'autore ha posto il massimo impegno per garantire che le informazioni contenute siano corrette, compatibilmente con le conoscenze disponibili al momento della pubblicazione; esso, tuttavia, non può essere ritenuto responsabile dei risultati dell'utilizzo di tali informazioni e resta a disposizione per integrare la citazione delle fonti, qualora incompleta o imprecisa.

Realizzare un libro è un'attività lunga e complessa; nonostante la cura e l'attenzione posta dall'autore l'esperienza ci insegna che è praticamente impossibile pubblicare un'opera priva di errori.

Chiunque dovesse riscontrare irregolarità in qualsiasi parte del presente volume e/o ritiene che vi siano parti coperte da copyright la cui trascrizione non è assolutamente gradita al titolare è invitato a segnalarlo tempestivamente all'indirizzo ingvitel@gmail.com.

prof. Lorenzo Vitello

1.1 Tabella protocollare ISO/OSI e TCP/IP

livelli ISO/OSI	modello ISO/OSI	livelli TCP/IP	modello TCP/IP	protocolli principali	tecniche e algoritmi più diffusi	come vengono chiamati i flussi gestiti dal livello	principali funzioni svolte dal livello	dispositivi di rete coinvolti
7	Applicazion e	4	Applicazion e	TELNET, FTP,SFTP, HTTP, HTTPS, SSH SMTP, POP3, DNS, DHCP		dati	- funge da interfaccia tra il sistema informativo e il mondo reale - contiene tutti i programmi applicativi utili all'end-user per svolgere attività in rete - trasferimento, accesso e gestione dei file; - posta elettronica; - terminale virtuale; - scambio risultati tra programmi (applicazioni client-server)	
6	Presentazione			JPG, ASCII, TIFF, PCT, crittografia, MIDI, MP3, MP4, WAV, MPE	algoritmi di compressioni multimediali, crittografia dati (WEP, WPA, WPA2, WPA3,RSA,PGP,AES ,ecc...)	dati	- rappresentazione dei dati; - compressione dei dati; - cifratura dei dati (sicurezza);	
5	Sessione			RPC, Appletalk ASP, DECnet SC		dati	- operazioni di login (utente e password) - suddivide il dialogo tra le applicazioni in unità logiche (dette sessioni); - gestisce la chiusura ordinata del dialogo tra unità logiche; - introduce i punti di sincronizzazione;	
4	Trasporto	3	Trasporto	TCP, UDP		segmenti	- segmentazione e assemblaggio dei dati; - controllo end-to-end dei dati per prevenire errori e malfunzionamenti - definisce i parametri per la qualità del servizio; - riordino pacchetti su RX in ordine corretto rispetto a TX; - rimodulazione flusso dati per diverse velocità tra TX e RX;	
3	Rete	2	Rete	IP, IPv4, IPv6, RIP, BGP, IGMP, OSPF, ICMP, IPSEC, ARP, RARP	tecniche di SUBNETTING, dijkstra, bellman-ford,	pacchetti	- moltipolazione dei pacchetti - instradamento (routing) - controllo congestione - internetworking (comunicazione tra reti diverse)	- Router
2	Collegament O (suddiviso in livello MAC e LCC)	1	Fisico	PPP, SLIP, FDDI, ATM, Frame Relay, ARP, CDMA, CSMA/CD, 1-persistent CSMA, non-persisteng CSMA, p-persistent CSMA, TDMA, FDMA, token passing, aloha puro, aloha slotted	tecniche di moltipolazione, tecniche di accesso, scheduling	Frame (o trama)	- suddivide i bit forniti dal livello fisico in frame; - individua la presenza di errori nei frame e gestire i meccanismi per correggerli; - definire l'accesso multiplo da parte di diversi utenti allo stesso canale di comunicazione; - regolare la trasmissione tra dispositivi che lavorano a velocità diverse	- Switch, - Bridge
1	Fisico			Ethernet (IEEE 802.3), Wireless (IEEE 802.11)	gestione cavi ethernet: - RJ45 gestione Cavi coassiali: - RG213 (coax thick) - RG48 (coax thin) gestione Doppini - UTP - S-UTP - STP gestione Fibre ottiche: - Multimodali - Monomodali	BIT (tensioni e correnti)	- modulazione del segnale (scelta forme d'onda e altre caratteristiche fisiche del segnale) - analisi cavi e connettori (cablaggio)	- Repeater - HUB, - Modem

FIG. 1 (tabella ISO/OSI e TCP/IP)

(Rif. Bibliografici [8] – pag 251, 252, 253, 254, 255, 256)

1.2 Indipendenza modulare dei singoli livelli ISO/OSI, spiegazione concettuale

Nella pila protocollare ISO/OSI, ciascun livello può operare in modo indipendente dai dettagli implementativi dei livelli sottostanti grazie al principio dell'astrazione. Questo significa che:

- Un livello superiore interagisce solo con l'interfaccia fornita dal livello immediatamente inferiore. Questo concetto è noto come "incapsulamento" o "astrazione dei servizi".
- L'astrazione permette che ogni livello fornisca un insieme di funzioni o servizi attraverso un'interfaccia ben definita, senza che il livello superiore abbia bisogno di sapere come questi servizi siano effettivamente realizzati.
- In pratica, ogni livello utilizza i servizi forniti dal livello inferiore come se fossero primitive o funzioni di base, senza preoccuparsi della complessità interna di tali servizi.

Per esempio:

- Il livello di applicazione (Livello 7) usa i servizi del livello di presentazione (Livello 6) senza conoscere i dettagli di come il livello di presentazione gestisce la codifica o la compressione dei dati.
- Il livello di trasporto (Livello 4) fornisce comunicazioni end-to-end affidabili al livello di sessione (Livello 5), ma il livello di sessione non ha bisogno di sapere se il livello di trasporto utilizza TCP o UDP per fare questo.

Questo principio di astrazione facilita la modularità, l'interoperabilità e la manutenzione dei sistemi di rete, poiché permette di aggiornare o modificare un livello senza influenzare necessariamente gli altri.

FONTI E APPROFONDIMENTI: per un approfondimento sui principi della pila protocollare ISO/OSI, consulta lo standard ISO/IEC 7498-1. Per ulteriori dettagli, si consigliano testi come 'Computer Networks' di Tanenbaum e Wetherall, o corsi online disponibili su piattaforme come Coursera o edX."

1.3 Standard RFC e documentazione di riferimento

La suite di protocolli TCP/IP è definita da vari standard RFC (Request for Comments) gestiti dall'Internet Engineering Task Force (IETF).

Tale IETF è un'organizzazione aperta, internazionale e volontaria, con tecnici e ingegneri partecipanti da tutto il mondo, che sviluppa e promuove standard tecnici per Internet. Fondata nel 1986, l'IETF si concentra sulla produzione di documenti tecnici che influenzano la progettazione, l'uso e la gestione di Internet e delle sue infrastrutture interconnesse.

I documenti RFC sono custoditi e resi disponibili principalmente attraverso il sito web dell'RFC Editor e tramite vari archivi online. Il sito web dell'RFC Editor è il repository ufficiale per tutti i documenti RFC. Il sito dell'RFC Editor offre accesso a tutti gli RFC pubblicati, con la possibilità di cercare, leggere, e scaricare i documenti in formato HTML, testo semplice, o PDF.

L'indirizzo del sito è www.rfc-editor.org

1.4 Elenco e descrizione dei principali protocolli, algoritmi e tecniche di riferimento

- **1-persistent CSMA:**
 - Acronimo: 1-persistent CSMA
 - Tipo: Tecnica
 - Strato: Fisico
 - RFC: Nessuno
 - Descrizione: Un algoritmo di CSMA dove un dispositivo trasmette immediatamente se il canale è libero, altrimenti aspetta e ritenta.

- **AES 128 (Advanced Encryption Standard con chiave a 128 bit)**
 - Acronimo: Advanced Encryption Standard
 - Tipo: Protocollo di crittografia
 - Strato: Può essere applicato a vari livelli, ma comunemente al livello di trasporto (TLS) o applicativo
 - RFC: RFC 3602 (AES Ciphersuites for TLS)
 - Descrizione: AES-128 è una versione dell'algoritmo AES con una chiave di 128 bit. È implementato per la cifratura simmetrica dei dati. Usato in molte applicazioni di sicurezza, inclusi protocolli di sicurezza web (SSL/TLS), cifratura di file, e per la protezione dei dati in transito o a riposo.

- **AES 256 (Advanced Encryption Standard con chiave a 256 bit)**
 - Acronimo: Advanced Encryption Standard
 - Tipo: Protocollo di crittografia
 - Strato: Applicabile a vari livelli, ma spesso a trasporto o applicativo
 - RFC: RFC 3602 (AES Ciphersuites for TLS)
 - Descrizione: AES-256 utilizza una chiave di 256 bit, offrendo un livello di sicurezza ancora maggiore rispetto ad AES-128. È implementato per crittografare dati in modo molto sicuro. Utilizzato in applicazioni che richiedono una sicurezza elevata, come la protezione di dati governativi, militari, finanziari, e in molti sistemi di cifratura moderni.

- **Aloha Puro:**
 - Acronimo: Aloha Puro
 - Tipo: Tecnica
 - Strato: Fisico
 - RFC: Nessuno
 - Descrizione: Metodo di accesso al mezzo di trasmissione dove i nodi inviano pacchetti in qualsiasi momento senza coordinamento, e se c'è una collisione, ritrasmettono dopo un tempo casuale. Serve per reti a bassa velocità o con comunicazioni sporadiche.

- **Aloha Slotted:**
 - Acronimo: Aloha Slotted
 - Tipo: Tecnica
 - Strato: Fisico
 - RFC: Nessuno
 - Descrizione: Miglioramento del Puro Aloha dove il tempo è diviso in slot e i nodi possono trasmettere solo all'inizio di uno slot, riducendo la probabilità di collisione. Serve per migliorare l'efficienza della trasmissione nei sistemi di comunicazione condivisi.
-
- **AppleTalk ASP (AppleTalk Session Protocol):**
 - Acronimo: AppleTalk Session Protocol
 - Tipo: Protocollo
 - Strato: Applicativo (parte della suite AppleTalk)
 - RFC: Nessuno (AppleTalk non è basato su RFC)
 - Descrizione: Gestisce le sessioni tra applicazioni nella rete AppleTalk, ora obsoleto ma importante per la compatibilità storica.
-
- **ARP (Address Resolution Protocol):**
 - Acronimo: Address Resolution Protocol
 - Tipo: Protocollo
 - Strato: Rete/Link
 - RFC: RFC 826
 - Descrizione: Mappa un indirizzo IP a un indirizzo MAC, permettendo la comunicazione a livello di rete.
-
- **ASCII (American Standard Code for Information Interchange):**
 - Acronimo: American Standard Code for Information Interchange
 - Tipo: Codifica dei caratteri (tecnica)
 - Strato: Applicativo (applicazioni per la gestione dati)
 - RFC: Nessuno
 - Descrizione: Standard per la rappresentazione dei caratteri testuali, permette la comunicazione tra dispositivi che utilizzano diverse codifiche di caratteri.
-
- **ATM (Asynchronous Transfer Mode):**
 - Acronimo: Asynchronous Transfer Mode
 - Tipo: Tecnologia (rete)
 - Strato: Collegamento dati (ma anche fisico)
 - RFC: Nessuno specifico, ma diversi RFC trattano l'uso di ATM in contesti IP
 - Descrizione: Tecnologia di commutazione a pacchetto per telecomunicazioni, adatta per reti ad alta velocità con qualità di servizio garantita.
-
- **BGP (Border Gateway Protocol):**
 - Acronimo: Border Gateway Protocol
 - Tipo: Protocollo
 - Strato: Rete
 - RFC: RFC 4271
 - Descrizione: Protocollo di routing esterno utilizzato per scambiare informazioni di routing tra Autonomous System, cruciale per il routing su Internet.
-
- **DECnet SC (Session Control):**
 - Acronimo: Session Control
 - Tipo: Protocollo
 - Strato: Applicativo (parte della suite DECnet)

- RFC: Nessuno (DECnet non è basato su RFC)
 - Descrizione: Controlla le sessioni tra le applicazioni in reti DECnet, usato principalmente nei sistemi Digital Equipment Corporation.
-
- **CDMA (Code Division Multiple Access):**
 - Acronimo: Code Division Multiple Access
 - Tipo: Tecnica
 - Strato: Fisico
 - RFC: Nessuno
 - Descrizione: Metodo di accesso multiplo che permette a più trasmissioni di condividere lo stesso canale utilizzando codici unici per separare le comunicazioni.
-
- **Crittografia:**
 - Acronimo: N/A
 - Tipo: Tecnica
 - Strato: Può essere applicato a vari livelli, specialmente trasporto per sicurezza
 - RFC: Vari, dipende dal metodo (es. TLS - RFC 5246)
 - Descrizione: Metodo per codificare informazioni in modo che solo chi ha la chiave corretta possa decifrarle, fondamentale per la sicurezza dei dati.
-
- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):**
 - Acronimo: Carrier Sense Multiple Access with Collision Detection
 - Tipo: Tecnica
 - Strato: Fisico (LAN)
 - RFC: Nessuno, standardizzato da IEEE 802.3
 - Descrizione: Metodo per gestire l'accesso al mezzo di trasmissione nelle reti Ethernet, rilevando e gestendo le collisioni.
-
- **DHCP (Dynamic Host Configuration Protocol):**
 - Acronimo: Dynamic Host Configuration Protocol
 - Tipo: Protocollo
 - Strato: Applicativo
 - RFC: RFC 2131
 - Descrizione: Assegna automaticamente indirizzi IP e altre configurazioni di rete ai dispositivi, semplificando la gestione delle reti.
-
- **DNS (Domain Name System):**
 - Acronimo: Domain Name System
 - Tipo: Protocollo
 - Strato: Applicativo
 - RFC: RFC 1034, RFC 1035
 - Descrizione: Traduce i nomi di dominio leggibili dall'uomo in indirizzi IP, facilitando la navigazione su Internet.
-
- **Ethernet (IEEE 802.3):**
 - Acronimo: Ethernet
 - Tipo: Protocollo
 - Strato: Collegamento dati (ma anche fisico)
 - RFC: Nessuno, standardizzato da IEEE 802.3
 - Descrizione: Protocollo di rete per reti locali (LAN) che utilizza CSMA/CD per gestire l'accesso condiviso al mezzo di comunicazione. Serve per la connessione di dispositivi in una rete locale, offrendo velocità elevate e affidabilità.
-
- **FDDI (Fiber Distributed Data Interface):**

- Acronimo: Fiber Distributed Data Interface
 - Tipo: Tecnologia (rete)
 - Strato: Collegamento dati
 - RFC: Nessuno
 - Descrizione: Standard per reti locali ad alta velocità che utilizza la fibra ottica, noto per la sua alta affidabilità e velocità.
-
- **FDMA (Frequency Division Multiple Access):**
 - Acronimo: Frequency Division Multiple Access
 - Tipo: Tecnica
 - Strato: Fisico
 - RFC: Nessuno
 - Descrizione: Tecnica che permette a più utenti di condividere una banda di frequenze, assegnando a ciascuno una porzione distinta dello spettro.
-
- **Frame Relay:**
 - Acronimo: Frame Relay
 - Tipo: Tecnologia (rete)
 - Strato: Collegamento dati
 - RFC: Nessuno
 - Descrizione: Servizio WAN che trasmette dati in pacchetti chiamati frame, ottimizzato per trasmissioni bursty con bassa latenza.
-
- **FTP (File Transfer Protocol):**
 - Acronimo: File Transfer Protocol
 - Tipo: Protocollo
 - Strato: Applicativo
 - RFC: RFC 959
 - Descrizione: Protocollo per il trasferimento di file tra client e server su una rete, usato per caricare e scaricare file.
-
- **HTTP (HyperText Transfer Protocol):**
 - Acronimo: HyperText Transfer Protocol
 - Tipo: Protocollo
 - Strato: Applicativo
 - RFC: RFC 2616 (ora obsoleto, sostituito da RFC 7230-7235)
 - Descrizione: Protocollo per la distribuzione di informazioni ipertestuali come pagine web, fondamentale per il funzionamento di Internet.
-
- **HTTPS (HTTP Secure):**
 - Acronimo: HTTP Secure
 - Tipo: Protocollo
 - Strato: Applicativo (utilizza TLS/SSL a livello di trasporto)
 - RFC: Utilizza HTTP (RFC 7230-7235) e TLS (RFC 5246)
 - Descrizione: Versione sicura di HTTP che utilizza crittografia per garantire la sicurezza delle comunicazioni, proteggendo i dati durante il trasferimento.
-
- **JPG (Joint Photographic Experts Group):**
 - Acronimo: Joint Photographic Experts Group
 - Tipo: Formato di file (tecnica)
 - Strato: Applicativo (applicazioni gestiscono immagini)
 - RFC: Nessuno
 - Descrizione: Metodo di compressione con perdita per immagini digitali, utilizzato per ridurre la dimensione dei file immagine pur mantenendo una qualità accettabile.

- **ICMP (Internet Control Message Protocol):**
 - Acronimo: Internet Control Message Protocol
 - Tipo: Protocollo
 - Strato: Rete
 - RFC: RFC 792 (ICMPv4), RFC 4443 (ICMPv6)
 - Descrizione: Usato per segnalare errori, problemi di consegna e altri messaggi di controllo tra dispositivi IP.
-
- **IGMP (Internet Group Management Protocol):**
 - Acronimo: Internet Group Management Protocol
 - Tipo: Protocollo
 - Strato: Rete
 - RFC: RFC 1112, RFC 2236 (IGMPv2), RFC 3376 (IGMPv3)
 - Descrizione: Gestisce l'iscrizione de
-
- **IP (Internet Protocol):**
 - Acronimo: Internet Protocol
 - Tipo: Protocollo
 - Strato: Rete
 - RFC: RFC 791 (per IPv4), RFC 2460 (per IPv6)
 - Descrizione: Protocollo fondamentale per l'instradamento dei pacchetti tra reti, fornisce l'indirizzamento logico per i dispositivi.
-
- **IPSec (Internet Protocol Security):**
 - Acronimo: Internet Protocol Security
 - Tipo: Protocollo
 - Strato: Rete
 - RFC: Vari, tra cui RFC 4301 (Security Architecture for the Internet Protocol)
 - Descrizione: Suite di protocolli per la sicurezza a livello di rete, utilizzata per crittografare e autenticare le comunicazioni IP.
-
- **IPv4 (Internet Protocol version 4):**
 - Acronimo: Internet Protocol version 4
 - Tipo: Protocollo
 - Strato: Rete
 - RFC: RFC 791
 - Descrizione: Versione originale del protocollo IP, utilizza indirizzi a 32 bit, ora in fase di esaurimento.
-
- **IPv6 (Internet Protocol version 6):**
 - Acronimo: Internet Protocol version 6
 - Tipo: Protocollo
 - Strato: Rete
 - RFC: RFC 2460
 - Descrizione: Evoluzione di IPv4 con indirizzi a 128 bit, progettato per risolvere la carenza di indirizzi IP e migliorare la gestione delle reti.
-
- **MIDI (Musical Instrument Digital Interface):**
 - Acronimo: Musical Instrument Digital Interface
 - Tipo: Protocollo (ma anche formato di file)
 - Strato: Applicativo (applicazioni audio)
 - RFC: Nessuno
 - Descrizione: Protocollo per comunicare dati musicali tra strumenti elettronici, software e hardware.

- **MP3 (MPEG-1 Audio Layer III):**
- Acronimo: MPEG-1 Audio Layer III
- Tipo: Formato di file (tecnica)
- Strato: Applicativo (applicazioni audio)
- RFC: Nessuno
- Descrizione: Metodo di compressione con perdita per file audio, ampiamente usato per la distribuzione di musica digitale.

- **MP4 (MPEG-4 Part 14):**
- Acronimo: MPEG-4 Part 14
- Tipo: Formato di file (tecnica)
- Strato: Applicativo (applicazioni audio/video)
- RFC: Nessuno
- Descrizione: Formato contenitore che supporta audio, video e sottotitoli, utilizzato per streaming e archiviazione multimediale.

- **MPE (Multimedia Presentation Environment):**
- Acronimo: Multimedia Presentation Environment
- Tipo: Formato di file (tecnica)
- Strato: Applicativo (applicazioni audio/video)
- RFC: Nessuno
- Descrizione: Formato per presentazioni multimediali, meno comune oggi.

- **Non-persistent CSMA:**
- Acronimo: Non-persistent CSMA
- Tipo: Tecnica
- Strato: Fisico
- RFC: Nessuno
- Descrizione: Un metodo dove, se il canale è occupato, il dispositivo aspetta un tempo casuale prima di controllare nuovamente lo stato del canale.

- **OSPF (Open Shortest Path First):**
- Acronimo: Open Shortest Path First
- Tipo: Protocollo
- Strato: Rete
- RFC: RFC 2328 (OSPFv2), RFC 5340 (OSPFv3)
- Descrizione: Protocollo di routing a stato di collegamento che utilizza un algoritmo di shortest path per determinare il percorso migliore all'interno di una rete autonoma.

- **p-persistent CSMA:**
- Acronimo: p-persistent CSMA
- Tipo: Tecnica
- Strato: Fisico
- RFC: Nessuno
- Descrizione: Variante di CSMA dove un dispositivo trasmette con una probabilità p se il canale è libero, altrimenti aspetta per un tempo prima di riprovare.

- **PGP (Pretty Good Privacy)**
- Acronimo: Pretty Good Privacy
- Tipo: Protocollo di crittografia
- Strato: Applicativo
- RFC: RFC 4880 (OpenPGP Message Format)

- Descrizione: PGP è un sistema per la cifratura e la firma dei dati che utilizza combinazioni di crittografia simmetrica e asimmetrica (come RSA per le chiavi pubbliche). È implementato per garantire la riservatezza e l'autenticità delle comunicazioni, specialmente nelle email. Utilizzato per la crittografia di messaggi, file e comunicazioni digitali.
- **POP3 (Post Office Protocol version 3):**
 - Acronimo: Post Office Protocol version 3
 - Tipo: Protocollo
 - Strato: Applicativo
 - RFC: RFC 1939
 - Descrizione: Permette di scaricare la posta elettronica da un server remoto su un client locale, utile per la gestione offline delle email.
- **PPP (Point-to-Point Protocol):**
 - Acronimo: Point-to-Point Protocol
 - Tipo: Protocollo
 - Strato: Collegamento dati
 - RFC: RFC 1661
 - Descrizione: Protocollo per stabilire una connessione diretta tra due nodi, usato frequentemente per il collegamento dial-up e alcune WAN.
- **RARP (Reverse Address Resolution Protocol):**
 - Acronimo: Reverse Address Resolution Protocol
 - Tipo: Protocollo
 - Strato: Rete/Link
 - RFC: RFC 903
 - Descrizione: Permette a un dispositivo di scoprire il proprio indirizzo IP basandosi sul proprio indirizzo MAC, oggi sostituito da BOOTP e DHCP
- **RIP (Routing Information Protocol):**
 - Acronimo: Routing Information Protocol
 - Tipo: Protocollo
 - Strato: Rete
 - RFC: RFC 1058 (RIP v1), RFC 2453 (RIP v2)
 - Descrizione: Protocollo di routing a distanza vettoriale per la distribuzione delle informazioni di routing tra i router.
 - i membri del multicast group, permettendo ai dispositivi di segnalare interesse per ricevere trasmissioni multicast.
- **RPC (Remote Procedure Call):**
 - Acronimo: Remote Procedure Call
 - Tipo: Tecnica
 - Strato: Applicativo
 - RFC: RFC 1831, RFC 1832 (per ONC RPC)
 - Descrizione: Consente a un programma di eseguire una procedura su un altro sistema remoto come se fosse locale, facilitando la comunicazione tra applicazioni distribuite.
- **RSA (Rivest-Shamir-Adleman)**
 - Acronimo: Rivest-Shamir-Adleman
 - Tipo: Protocollo di crittografia
 - Strato: Applicativo (può essere utilizzato in vari strati, ma tipicamente implementato nelle applicazioni per crittografia a chiave pubblica)
 - RFC: RFC 3447 (PKCS #1: RSA Cryptography Specifications Version 2.1)

- Descrizione: RSA è un algoritmo di crittografia asimmetrica che usa una coppia di chiavi: una pubblica per cifrare i messaggi e una privata per decifrarli. È ampiamente usato per la firma digitale, lo scambio di chiavi e la crittografia dei dati sensibili in applicazioni come email sicure (PGP), HTTPS, e VPN.
- **SFTP (Secure File Transfer Protocol):**
 - Acronimo: Secure File Transfer Protocol
 - Tipo: Protocollo
 - Strato: Applicativo (utilizza SSH a livello di trasporto)
 - RFC: Non direttamente definito da un RFC, ma utilizza SSH (RFC 4251-4254)
 - Descrizione: Fornisce un trasferimento sicuro dei file attraverso una connessione criptata, alternativa sicura a FTP.
- **SLIP (Serial Line Internet Protocol):**
 - Acronimo: Serial Line Internet Protocol
 - Tipo: Protocollo
 - Strato: Collegamento dati
 - RFC: RFC 1055
 - Descrizione: Protocollo per la trasmissione di pacchetti IP su linee seriali, predecessore di PPP, ora meno utilizzato.
- **SMTP (Simple Mail Transfer Protocol):**
 - Acronimo: Simple Mail Transfer Protocol
 - Tipo: Protocollo
 - Strato: Applicativo
 - RFC: RFC 5321
 - Descrizione: Protocollo per l'invio di email tra server, consentendo la trasmissione di messaggi di posta elettronica.
- **SSH (Secure SHell):**
 - Acronimo: Secure Shell
 - Tipo: Protocollo
 - Strato: Applicativo (ma opera anche sul trasporto)
 - RFC: RFC 4251-4254
 - Descrizione: Fornisce un canale sicuro per accedere a sistemi remoti, include autenticazione e crittografia dei dati per garantire la sicurezza delle connessioni.
- **TELNET:**
 - Acronimo: TELecomunications NETwork
 - Tipo: Protocollo
 - Strato: Applicativo
 - RFC: RFC 854
 - Descrizione: Permette di accedere a un computer remoto come se si fosse collegati localmente, utile per la gestione remota di sessioni di terminale.
- **TCP (Transmission Control Protocol):**
 - Acronimo: Transmission Control Protocol
 - Tipo: Protocollo
 - Strato: Trasporto
 - RFC: RFC 793
 - Descrizione: Fornisce un servizio di comunicazione affidabile, orientato alla connessione tra applicazioni, garantendo l'ordine e l'integrità dei dati.
- **TDMA (Time Division Multiple Access):**
 - Acronimo: Time Division Multiple Access

- Tipo: Tecnica
 - Strato: Fisico
 - RFC: Nessuno
 - Descrizione: Metodo di accesso multiplo dove il tempo è diviso in slot, e ogni dispositivo trasmette solo durante il suo slot temporale assegnato.
-
- **TIFF (Tagged Image File Format):**
 - Acronimo: Tagged Image File Format
 - Tipo: Formato di file (tecnica)
 - Strato: Applicativo (applicazioni gestiscono immagini)
 - RFC: Nessuno
 - Descrizione: Formato di file per immagini raster che supporta vari tipi di compressione e può memorizzare immagini ad alta qualità, spesso usato in ambiti professionali.
-
- **Token Passing:**
 - Acronimo: Token Passing
 - Tipo: Tecnica
 - Strato: Fisico (e collegamento dati)
 - RFC: Nessuno
 - Descrizione: Metodo di controllo di accesso al mezzo dove un token circola tra i dispositivi, solo chi possiede il token può trasmettere.
-
- **UDP (User Datagram Protocol):**
 - Acronimo: User Datagram Protocol
 - Tipo: Protocollo
 - Strato: Trasporto
 - RFC: RFC 768
 - Descrizione: Offre una comunicazione senza connessione, veloce ma senza garanzia di consegna o ordine dei dati, utile per applicazioni che privilegiano la velocità
-
- **WAV (Waveform Audio File Format):**
 - Acronimo: Waveform Audio File Format
 - Tipo: Formato di file (tecnica)
 - Strato: Applicativo (applicazioni audio)
 - RFC: Nessuno
 - Descrizione: Formato audio non compresso o con compressione senza perdita, usato per alta qualità audio.
-
- **WEP (Wired Equivalent Privacy)**
 - Acronimo: Wired Equivalent Privacy
 - Tipo: Protocollo di crittografia
 - Strato: Fisico/Collegamento dati (livello 2 del modello OSI, ma non direttamente mappato al modello TCP/IP)
 - RFC: Nessuno (poiché è specifico per IEEE 802.11)
 - Descrizione: WEP è un vecchio protocollo di sicurezza per reti Wi-Fi che utilizza la cifratura RC4 con chiavi a 64 o 128 bit. È implementato tramite un sistema di chiave statica, che si è dimostrato insicuro. Utilizzato principalmente nelle reti wireless, ma ormai obsoleto a causa di numerose vulnerabilità.

- **Wireless (IEEE 802.11):**
- Acronimo: Wireless (comunemente noto come Wi-Fi)
- Tipo: Protocollo
- Strato: Collegamento dati (ma anche fisico)
- RFC: Nessuno, standardizzato da IEEE 802.11
- Descrizione: Standard per le reti wireless locali (WLAN) che permette la connessione senza fili tra dispositivi. Utilizza metodi di accesso multiplo come CSMA/CA.
Serve per fornire connettività Internet e di rete senza la necessità di cavi fisici, facilitando la mobilità e l'installazione flessibile.

- **WPA (Wi-Fi Protected Access)**
- Acronimo: Wi-Fi Protected Access
- Tipo: Protocollo di crittografia
- Strato: Fisico/Collegamento dati (livello 2 del modello OSI)
- RFC: Nessuno (standard IEEE 802.11i)
- Descrizione: Introdotto per migliorare le carenze di WEP, WPA usa TKIP (Temporal Key Integrity Protocol) per aggiornare dinamicamente le chiavi di cifratura. Implementa anche un sistema di verifica dell'integrità dei messaggi. Utilizzato per la sicurezza delle reti Wi-Fi, ma è stato superato da WPA2.

- **WPA2 (Wi-Fi Protected Access 2)**
- Acronimo: Wi-Fi Protected Access 2
- Tipo: Protocollo di crittografia
- Strato: Fisico/Collegamento dati (livello 2 del modello OSI)
- RFC: Nessuno specifico, ma si basa su IEEE 802.11i
- Descrizione: WPA2 utilizza AES-CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) come metodo di cifratura, offrendo maggiore sicurezza rispetto a WPA. È implementato in due modalità principali: Personal (PSK) per reti domestiche e Enterprise per ambienti aziendali con autenticazione centralizzata. È ampiamente utilizzato nelle reti Wi-Fi moderne.

- **WPA3 (Wi-Fi Protected Access 3)**
- Acronimo: Wi-Fi Protected Access 3
- Tipo: Protocollo di crittografia
- Strato: Fisico/Collegamento dati (livello 2 del modello OSI)
- RFC: Nessuno (standard IEEE 802.11i-2018)
- Descrizione: WPA3 migliora ulteriormente la sicurezza rispetto a WPA2 con SAE (Simultaneous Authentication of Equals) per una migliore protezione delle password e crittografia individualizzata per reti pubbliche. È implementato per fornire protezione contro attacchi di forza bruta e di tipo dictionary. Utilizzato nelle nuove reti Wi-Fi per una sicurezza avanzata.

1.5 Standard IEEE 802

Lo Standard IEEE 802 è una serie di standard sviluppati dall'Institute of Electrical and Electronics Engineers (IEEE) per le reti di computer. Questi standard coprono una vasta gamma di tecnologie di rete, principalmente focalizzati su:

- reti locali (LAN)
- le reti metropolitane (MAN).

il numero 802 deriva dal fatto che il progetto ha avuto inizio nel 1980 quando fu fondato il Local and Metropolitan Area Network Standard Committee.

L'Institute of Electrical and Electronics Engineers (IEEE) è una delle più grandi organizzazioni professionali al mondo dedicata all'avanzamento della tecnologia per il beneficio dell'umanità. Fondata nel 1963 dalla fusione dell'American Institute of Electrical Engineers e dell'Institute of Radio Engineers, l'IEEE ha come obiettivo:

- Promuovere l'innovazione tecnologica e l'eccellenza nel campo dell'ingegneria elettrica, dell'elettronica e delle scienze informatiche.

- Sviluppare standard tecnici per assicurare l'interoperabilità e la sicurezza delle tecnologie.

- Fornire un forum per la condivisione della conoscenza attraverso conferenze, pubblicazioni e corsi educativi.

- Supportare l'educazione e la carriera degli ingegneri attraverso certificazioni, workshop e networking.

Struttura e Attività:

- Membri: IEEE conta oltre 400.000 membri in più di 160 paesi, tra cui ingegneri, scienziati, tecnici, accademici e studenti.

- Pubblicazioni: Pubblica numerose riviste, conferenze e standard tecnici.

- Standard: È noto per sviluppare standard tecnici come quelli della serie IEEE 802 per le reti, IEEE 754 per l'aritmetica a virgola mobile, e molti altri.

- Conferenze: Organizza conferenze internazionali che coprono ampiamente i campi di interesse.

Sede Centrale:

L'IEEE ha la sua sede centrale a Piscataway, New Jersey, Stati Uniti. Tuttavia, mantiene uffici regionali e sezioni locali in tutto il mondo per servire i suoi membri globali.

Presenza Globale:

Sebbene la sede principale sia negli Stati Uniti, l'IEEE opera a livello internazionale con regioni che coprono:

- Regione 1-6: Stati Uniti e Canada
- Regione 7: Canada
- Regione 8: Europa, Medio Oriente e Africa
- Regione 9: America Latina
- Regione 10: Asia-Pacifico

Ogni regione ha le proprie sezioni, capitoli tecnici e sezioni studentesche che organizzano eventi locali e offrono opportunità di networking e sviluppo professionale.

L'IEEE è quindi una rete globale che non solo facilita lo scambio di conoscenze ma anche l'evoluzione delle tecnologie attraverso la collaborazione internazionale.

La serie 802 si divide in diversi sottostandard, ognuno dei quali affronta aspetti specifici della tecnologia di rete, ovvero:

802 LAN/MAN (Ethernet)

802.1 Bridging and Management per reti 802 LAN, MAN e le reti geografiche WAN

802.2 LLC (logical link control)

802.5 Token RING

802.3 Ethernet con metodo accesso CSMA/CD

802.11 - WLAN o wireless-lan

802.11a - WLAN a frequenza 5 GHz, 54 Mbps, 50 m

802.11b - WLAN a frequenza 2.4 GHz, 11 Mbps 50 m

802.11d - Adattamento a contesti regolatori in base alla nazione in cui è installato il sistema

802.11e - Miglioramento: Gestione della qualità del servizio.

802.11f - Inter-Access Point Protocol (IAPP)

802.11g - WLAN a frequenza 2.4 GHz, 54 Mbps 125 m

802.11h - 5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) e Transmit Power Control (TPC) per compatibilità con l'Europa

802.11n - WLAN a frequenza 2.4 GHz e/o 5 GHz, 600 Mbps, 500 m

802.11ac - (Wi-Fi 5) wlan a frequenza 2.4 GHz e/o 5 GHz, 6.77 Gbps (8 antenne, 160MHz), 200 m

802.11ah - WLAN HaLow, IoT/domotica, frequenza 900Mhz

802.11ax - (Wi-Fi 6) WLAN a frequenza 5 GHz. WLAN multi-stazione è di 11 Gbit/s

802.11be - (Wi-Fi 7) WLAN a frequenza 5 GHz. WLAN multi-stazione è di 30 Gbit/s (in arrivo nel 2024)

802.11i - (ratificato il 24 giugno 2004) - Miglioramento della sicurezza

802.11j - Estensione per il Giappone

802.11k - Misurazione delle sorgenti radio

802.11n - (Wi-Fi 4) Aumento della banda disponibile, fino a 450 Mb/s, 2,4 GHz e 5 GHz

802.11p - WAVE - Wireless Ability in Vehicular Environments (gestione per autoveicoli, ambulanze ecc.)

802.11r - Roaming rapido

802.11s - Gestione delle reti mesh
802.11T - Gestione e Test
802.11u - Connessione con reti non 802, come le reti cellulari.
802.11v - Gestione delle reti wireless
802.15 - WPAN
802.15.3a - Standard per reti WPAN in via di sviluppo
802.15.4a - Standard per reti WPAN in via di sviluppo
802.15.1 - Bluetooth
802.16 - WiMAX - Broadband wireless access
802.19 - Coexistence TAG
802.20 - Mobile Broadband Wireless Access
802.21 - Media Independent Handoff
802.22 - Wireless Regional Area Network

(Rif. Bibliografici [6],[7],[29])

1.6 Altre definizioni

SCHEDA DI RETE

Nell'ambito dei dispositivi di rete e dei terminali host di rete la scheda di rete (in inglese: network interface controller, in acronimo NIC, oppure network interface card, network adapter, LAN adapter o physical network interface) è un'interfaccia digitale, costituita da una scheda elettronica, che svolge tutte le funzionalità logiche di elaborazione necessarie a consentire la connessione del dispositivo ad una rete informatica e la conseguente trasmissione e ricezione di dati. (Rif. Bibliografico [9])

INTERFACCIA DI RETE

Nell'ambito dei dispositivi di rete e dei terminali host di rete **un'interfaccia** rappresenta logicamente una porta fisica di connessione in ingresso o in uscita al dispositivo nella quale si inserisce un connettore di un cavo (a volte anche wireless) per permettere dunque un collegamento dell'apparato con un altro tramite un link di rete (es. interfaccia ethernet, Wi-Fi, USB). Tipicamente nel caso degli apparati di rete l'interfaccia fisicamente comprende la scheda di rete munita dell'alloggio per il connettore che, nel caso dei terminali (computer), può essere tipicamente o una porta seriale o una porta parallela per il collegamento con le varie periferiche o del terminale con la rete locale.
(Rif. Bibliografico [12])

INDIRIZZO MAC (o MAC-ADDRESS)

Un esempio di indirizzo MAC-48 è "00-08-74-4C-7F-1D".

In informatica e telecomunicazioni l'indirizzo **MAC** (in inglese MAC-address, dove MAC sta per Media Access Control), detto anche indirizzo fisico, indirizzo ethernet o indirizzo LAN, è un codice di 48 bit (6 byte) assegnato in modo univoco dal produttore ad ogni scheda di rete ethernet o wireless prodotta al mondo, tuttavia modificabile a livello software. Rappresenta in sostanza un identificativo per un particolare dispositivo di rete a livello di rete locale: ad es. due schede di rete in due diversi calcolatori avranno due diversi nomi (e quindi diversi indirizzi **MAC**), così come avranno nomi diversi una scheda Ethernet ed una scheda wireless posizionate nel medesimo computer.

L'originale Indirizzo **MAC** IEEE 802, ora chiamato ufficialmente "**MAC-48**", deriva dalla specifica dell'Ethernet.

Gli indirizzi **MAC-48** vengono solitamente rappresentati in formato esadecimale, separando ciascun ottetto con un trattino o con i due punti.

(Rif. Bibliografico [11])

SUBNET MASK (o maschera di sottorete)

La maschera di sottorete (in inglese subnet mask), nell'ambito di una rete TCP/IP, è un parametro di configurazione che definisce la dimensione (intesa come intervallo di indirizzi) della sottoreteIP, o subnet, a cui appartiene un host, al fine di ridurre il traffico di rete e facilitare la ricerca e il raggiungimento di un determinato host con relativo indirizzo IP.

(Rif. Bibliografico [14])

2.1 Progettazione di una rete

Per progettazione di una rete di calcolatori (o networking) si intende un'organizzazione complessiva di aspetti tecnici, fisici e logici per connettere tra loro 2 o più calcolatori elettronici, analizzando punto-punto come gli elementi che formano la rete sono strutturati e interconnessi tra loro.

Nello specifico la progettazione complessiva di una rete è definita principalmente nelle seguenti FASI:

FASE	Descrizione	Hardware, tecniche e protocolli coinvolti
1	analisi essenziali dei requisiti di rete	identificare il numero di nodi; i requisiti di traffico; le necessità di scalabilità; la disponibilità di risorse (budget, spazio fisico)
2	scelta e analisi topologia della rete	topologia ad Anello (Ring); topologia a Stella (Star); topologia a Maglia (Mesh); topologia a Maglia completa (fully connected) topologia a Linea dorsale; topologia Lineare aperta (Line) topologia ad Albero (Tree) (la topologia di rete descrive la struttura fisica o logica in cui i nodi di una rete (computer, server, dispositivi di rete) sono collegati tra loro. La scelta della topologia influisce su performance, scalabilità, gestione della rete e costi.)
3	scelta dei dispositivi di rete per garantire connettività hardware e software nella rete	switch; router; access-point; repeater; Hub; Bridge; Modem;
4	scelta e analisi modalità di connessione dei nodi per la trasmissione dati	cavi Ethernet, Fibra ottica multi-modale o mono-modale, WiFi, Bluetooth, sistemi laser, IR, link satellitari, canalette, ecc... per connettere dispositivi mobili, computer, stampanti, terminali touch, videosorveglianza, sistemi di sicurezza, domotica, sistemi di sicurezza, telefonia VOIP ed tutti i collegamenti tra dispositivi che necessitano di una connessione permanente
5	progettazione del cablaggio strutturato standard internazionali di qualità e sicurezza	EIA/TIA-568, EIA/TIA-570 ISO/IEC DIS 11801, cablaggio strutturato, centro stella di campus e di edificio, armadio di piano (rack), cablaggio di campus, cablaggio verticale (singolo edificio), cablaggio orizzontale (locali di un singolo piano)
6	partizionamento IPv4 della rete	assegnazioni indirizzi IP per host, broadcast, gateway per i router ed uso eventuale della tecnica del subnetting
7	analisi della manutenibilità e scalabilità di una rete	
8	analisi e cura delle prestazioni	
9	sicurezza della rete e riservatezza dei dati	firewall, DMZ, WEP, WPA2, RSA, AES128, AES256, PGP, ecc...

2.2 Analisi essenziali dei requisiti di rete (rif. fase 1)

In una rete di calcolatori, un nodo è qualsiasi dispositivo attivo o punto di connessione che può inviare, ricevere o inoltrare dati all'interno della rete. Si distinguono essenzialmente in 2 sottocategorie:

1) un **nodo generico di rete** è un elemento fondamentale della rete che permette l'interconnessione, lo scambio e la gestione dei dati. La capacità di un nodo di comunicare con altri nodi definisce la struttura e l'efficienza della rete stessa.

I nodi generici di rete (o dispositivi di Rete) sono:

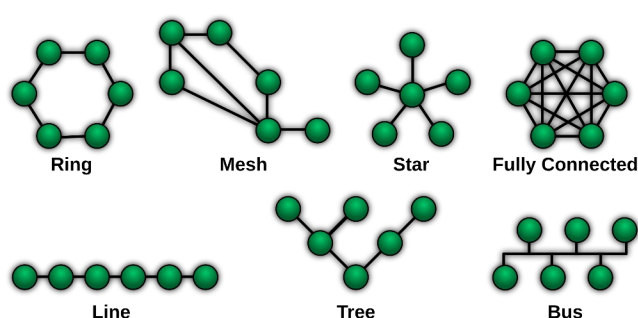
- Router: Dirige il traffico tra diverse reti, spesso tra una rete locale e Internet.
- Switch: Connette dispositivi all'interno di una stessa rete LAN, migliorando le prestazioni mediante il filtraggio e l'inoltro dei pacchetti.
- Hub: Connette più dispositivi ma senza intelligente gestione del traffico (ormai meno comune).

2) un **nodo finale (detto anche host)** è un dispositivo che produce o utilizza direttamente i dati, ad esempio PC, smartphone, server o stampanti in rete.

I nodi finali (detti anche host) sono:

- Computer: PC, server, laptop, workstation. Questi sono spesso i nodi finali (chiamati anche host) che generano o consumano i dati.
- Dispositivi periferici: Stampanti di rete, dispositivi di storage connessi in rete (NAS), telefoni IP, ecc.
- Dispositivi Mobili: Smartphone e tablet che possono connettersi a reti WiFi o cellulari;
Sensori e attuatori: in reti di sensori e sistemi IoT (internet delle cose), questi nodi possono rilevare cambiamenti ambientali o eseguire azioni fisiche basate sui dati ricevuti;

2.3 Scelta e analisi topologia della rete (rif. fase 2)



topologia ad Anello (Ring);
topologia a Stella (Star);
topologia a Maglia (Mesh);
topologia a Maglia completa (fully connected)
topologia a Linea dorsale;
topologia Lineare aperta (Line)
topologia ad Albero (Tree)

In NETWORKING la topologia di rete è il modello geometrico (grafo) finalizzato a rappresentare le relazioni di connettività, fisica o logica, tra gli elementi costituenti la rete stessa (detti anche nodi). Il concetto di topologia si applica a qualsiasi tipo di rete di telecomunicazioni: telefonica, rete di computer, Internet

Definizioni basilari

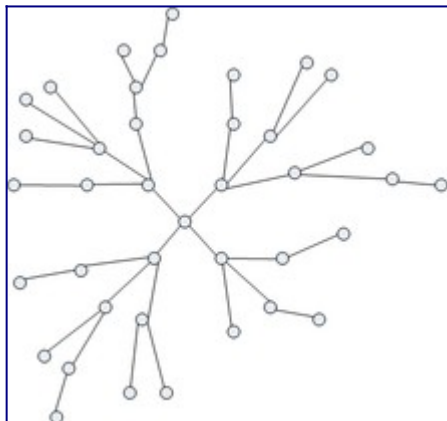
Gli elementi fondamentali della topologia sono i *nodi* e i *rami*. Il nodo individua un elemento della rete connotato da specifiche funzionalità mentre il ramo evidenzia la relazione di connettività tra i nodi. La topologia viene rappresentata quindi sotto forma di grafo in cui i nodi, in grado di scambiarsi direttamente l'informazione, sono collegati tra loro tramite uno o più rami.

Il significato di queste entità geometriche è diverso a seconda del tipo di rete e del tipo di operatività che si considera. Per esempio, in una rete informatica a seconda del livello applicativo considerato, un nodo può rappresentare un computer o un elemento di commutazione a livelli differenti (come un *router* oppure uno *switch*), mentre un ramo può rappresentare la connettività fisica effettiva oppure la connettività logica come appare a un determinato livello protocollare di pacchetto (per esempio a livello IP piuttosto che Ethernet).

Due nodi possono essere messi in comunicazione in due modi differenti:

- con una connessione fisica, quando fra i due nodi è presente un canale fisico che li collega in modo diretto; in questo caso, il ramo rappresenta anche un'entità fisica vera e propria;
- con una connessione logica, quando la rete assume le dimensioni WAN e quindi è impossibile pensare ad un collegamento fisico per ciascuna coppia di nodi oppure quando si vuole considerare lo schema di distribuzione dell'informazione secondo un particolare punto di vista. In questo caso, il ramo rappresenta la relazione logica tra i nodi, astruendo dal livello fisico propriamente detto.

La topologia di rete è determinata soltanto dalla configurazione dei collegamenti tra i nodi. Per la precisione, non riguardano la topologia di rete: le distanze tra i nodi, le tecnologie usate per le interconnessioni fisiche, le velocità di trasmissione, il tipo di segnale (elettrico, ottico, elettromagnetico eccetera).



Esempio di una rete di telecomunicazioni formata da interconnessioni tra dispositivi.

In informatica e telecomunicazioni un nodo è un qualsiasi dispositivo hardware del sistema in grado di comunicare con gli altri dispositivi che fanno parte della rete; può quindi essere un computer, una stampante, un fax, un modem ecc. In ogni caso il nodo deve essere dotato di una scheda di rete.

I nodi sono collegati tra loro da un pannello di connessione (in inglese Hub), chiamato anche concentratore, che ha la funzione di semplificare la connessione fisica tra i vari nodi e di instradare i segnali che vengono inviati da un nodo all'altro.

Nelle reti di telecomunicazioni indica genericamente un dispositivo ricetrasmittente di elaborazione che può essere posizionato ai bordi della rete stessa (nodo terminale (host) client o server) oppure al suo interno come nodo di transito ovvero di commutazione tra varie linee di uscita ad esempio nella rete di trasporto.

In questo caso il termine nodo è mutuato dalla teoria dei grafi con la quale è possibile rappresentare la topologia di una rete di telecomunicazioni attraverso il rispettivo grafo: un nodo è il punto in cui convergono o dipartono più link o collegamenti fisici con altri nodi.

Topologie elementari

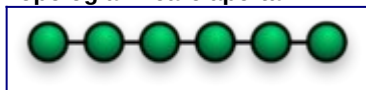
Una rete di complessità arbitraria può essere sempre scomposta in una combinazione di topologie elementari a loro volta interconnesse tra loro.

Le topologie elementari si possono ricondurre a cinque tipi fondamentali:

- le topologie lineari semplici, in cui ciascun nodo è collegato a due nodi adiacenti con un solo ramo; rientrano in questo tipo la topologia lineare aperta e la topologia ad anello;
- le topologie lineari complesse, a struttura gerarchica, in cui per ogni coppia di nodi esiste un solo percorso di collegamento e ogni nodo è collegato con uno o più rami ai nodi di gerarchia inferiore (rientrano in questo tipo le topologie ad albero propriamente dette e la topologia a stella);
- la topologia punto a punto, la più semplice, con un canale dedicato e diretto tra due endpoint;
- la topologia a maglia o magliata, in cui ogni nodo è connesso direttamente agli altri nodi, usando per ciascun collegamento un ramo dedicato;
- la topologia a bus, in cui tutti i nodi condividono lo stesso unico collegamento;

Ad esclusione della topologia a bus, in tutte le altre strutture lo scambio di informazioni tra due nodi qualsiasi della rete implica l'utilizzo di uno o più rami con l'attraversamento di nodi intermedi. Ogni ramo percorso costituisce un salto (*hop*): in queste strutture quindi il segnale trasmesso deve effettuare uno o più *hop* per giungere alla sua destinazione.

Topologia lineare aperta



Rappresentazione di una rete lineare

In questo tipo di topologia, spesso chiamata anche *daisy-chain*, ogni nodo è collegato con un ramo al nodo adiacente precedente e con l'altro ramo al nodo adiacente successivo. I nodi terminali sono invece adiacenti a un solo nodo. La comunicazione tra due nodi non adiacenti deve attraversare tutti i nodi intermedi, percorrendo i rami relativi: ogni passaggio tra due nodi viene detto *salto* o *hop*.

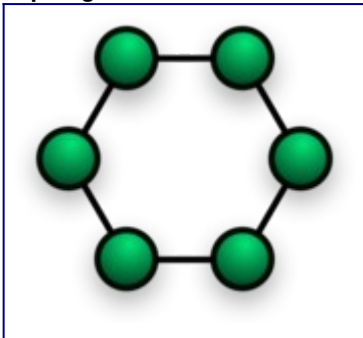
In una rete lineare aperta costituita da N nodi, il numero R di rami necessari per il collegamento tra tutti i nodi è dato dalla relazione:

$$R = N - 1$$

Questa relazione inoltre fornisce anche la formula del numero di *hop* necessari perché un'informazione generata da un nodo A raggiunga il nodo di destinazione B dovendo attraversare una sottorete composta complessivamente da N nodi (A, B e gli $N-2$ nodi intermedi).

Questa topologia possiede considerevoli svantaggi, primo tra tutti la scarsissima affidabilità: se un nodo si guasta o un ramo si interrompe, la rete viene divisa in due sottoreti isolate. Anche per quanto riguarda la scalabilità, questa struttura è poco efficiente, dato che comporta un'interruzione dell'attività di rete per aggiungere o eliminare un nodo intermedio.

Topologia rete ad anello



Rappresentazione di una rete ad anello

Una topologia ad anello è una topologia lineare di tipo chiuso, in cui a tutti i nodi fanno capo due rami. Tutti i nodi sono collegati con un ramo al nodo adiacente precedente e con l'altro ramo al nodo adiacente successivo.

In una rete ad anello costituita da N nodi, il numero di rami necessari per il collegamento tra tutti i nodi è dato dalla relazione:

$$R = N$$

Questa formula fornisce anche la relazione per determinare in modo algoritmico il numero di *hop* necessari per percorrere l'intero anello e viene usata anche per evitare situazioni in cui un'informazione continua a percorrere l'anello indefinitamente senza mai arrivare a destinazione, consumando banda.

Le topologie ad anello sono molto diffuse per via dell'alta tolleranza/robustezza ai guasti dato che l'informazione trasmessa può viaggiare in entrambi i versi/sensi dell'anello per raggiungere una certa destinazione, e non necessita di un nodo centrale per gestire la connessione tra i computer.

Consentono inoltre di ottimizzare l'utilizzo della banda disponibile, per esempio inviando alcuni pacchetti in un verso e altri pacchetti nel verso opposto, bilanciando così l'impiego delle risorse e limitando la possibilità che una parte dell'anello risulti congestionata mentre l'altra parte è scarica.

Di contro, la scalabilità presenta dei problemi, dato che l'aggiunta o la rimozione di un nodo presuppone una variazione della velocità della rete e l'apertura dell'intero anello e inoltre, a seconda delle tecnologie trasmissive e dei protocolli trasmissivi, potrebbe esserci un limite al numero massimo di nodi utilizzabili, per esempio per vincoli legati all'eventuale numero massimo di *hop* consentiti o al ritardo di propagazione ammesso.

Nel campo delle reti di computer, le più diffuse implementazioni della rete ad anello sono la Token ring[1] e la Token bus, in cui un pacchetto viene trasmesso da un nodo all'altro fino ad arrivare a destinazione, con un meccanismo di salvaguardia che evita che un pacchetto continui a girare indefinitamente nell'anello (quando il pacchetto viene ricevuto di nuovo nel nodo in cui è entrato nell'anello, ossia quando ha compiuto un giro completo senza riconoscere alcun nodo come destinazione, viene scartato, vedi relazione sul numero di *hop*).

Nel caso delle reti telefoniche, le strutture ad anello vengono usate per la distribuzione e aggregazione del traffico sia su area metropolitana che su area regionale, oltre che per collegamenti di lunghissima distanza come le reti sottomarine transcontinentali.

Topologia punto a punto

È la topologia più semplice con un collegamento dedicato tra due endpoint.

Il più semplice da comprendere, tra le variazioni della topologia punto-punto che appare, all'utente, in modo da essere associato permanentemente ai due endpoint.

Il telefono con i barattoli e il filo di stoffa che li collega è un esempio di canale fisico dedicato.

Utilizzando tecnologie di commutazione di circuito o commutazione a pacchetto, un circuito point-to-point può essere impostato dinamicamente e rilasciato quando non più necessario.

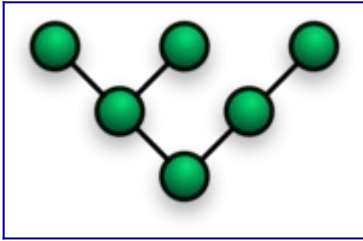
Le topologie commutate point-to-point sono il modello base della telefonia convenzionale.

Il valore di una rete punto-punto permanente è una comunicazione senza impedimenti tra i due endpoint.

Il valore di una connessione point-to-point su richiesta è proporzionale al numero di potenziali coppie di abbonati ed è stato espresso come Legge di Metcalfe.

Questa rete è utilizzata nei ponti radio wireless a lunga distanza e, quindi, le due stazioni sono collegate tramite un canale diretto.

Topologia ad albero



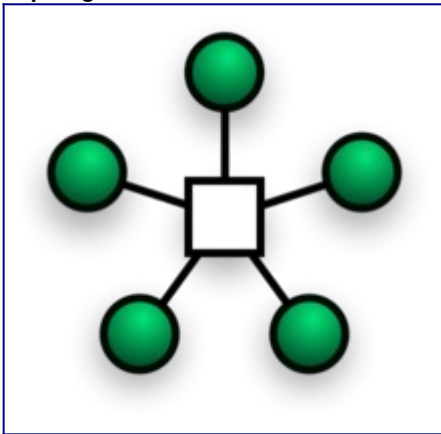
Topologia di rete ad albero

La topologia ad albero è una variante più complessa di una struttura lineare, caratterizzata dal fatto che da ciascun nodo possono dipartirsi più catene lineari distinte e non intersecantesi, realizzando così una struttura multilivello. Anche in questo tipo di topologia, per ogni coppia di nodi esiste un solo percorso di collegamento; ogni nodo è collegato a un solo nodo del livello superiore (nodo padre) tramite un solo ramo e a uno o più nodi del livello inferiore (nodi figli) tramite uno o più rami dedicati (diramazione). Il nodo da cui prende origine tutta la topologia viene denominato anche "nodo radice" (*root*) mentre i nodi terminali vengono denominati "foglie" (*leaf*).

Essendo sostanzialmente un'estensione della topologia lineare semplice, anche per questa topologia la relazione tra nodi e rami è data da: $R = N - 1$.

Una caratteristica di questa rete è che la comunicazione tra due nodi distinti dello stesso livello può avvenire solo risalendo la struttura fino al primo nodo padre comune, che deve quindi essere dotato di funzionalità di distribuzione più sofisticate per poter determinare la diramazione corretta verso cui instradare il segnale.

Topologia a stella



Topologia di rete a stella.

Le reti a stella sono le più comuni topologie di rete.

Questa topologia di rete consiste in un hub o switch che funge da punto centrale per la trasmissione delle informazioni e ogni host è connesso a tale punto (hub/switch).

I dati all'interno di una rete a stella attraversano l'hub prima di arrivare a destinazione. Inoltre l'hub gestisce e controlla tutte le funzionalità della rete (funziona anche come ripetitore per il flusso di dati).

Questa tipologia di rete riduce l'impatto di un guasto sulla linea trasmissiva collegando in modo indipendente ciascun host all'hub. Ogni host può comunicare con tutti gli altri e l'hub.

Il guasto di una linea trasmissiva che collega un host all'hub determinerà l'isolamento di tale host da tutti gli altri, ma il resto della rete continuerà a funzionare tranquillamente.

La configurazione a stella è tra le più comuni usate per i cavi a doppino e fibra ottica. Tuttavia può essere utilizzata anche con cavi di tipo coassiali.

Vantaggi e svantaggi

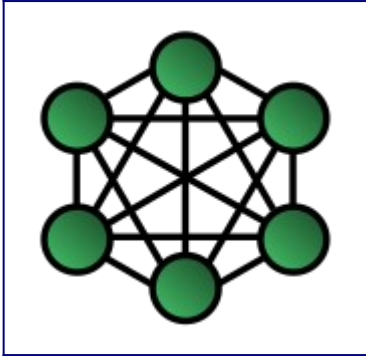
Le topologie ad albero presentano un elevato grado di affidabilità[2]: l'unico punto debole è costituito dai nodi padre, che, in caso di guasto, rendono impossibile l'accesso alla sottorete che si diparte da essi e che rimane quindi isolata. Va osservato che anche in questo caso la sottorete che rimane isolata, a meno che non sia costituita solo da nodi terminali, rimane comunque funzionante e operativa, essendo sempre possibile la comunicazione tra nodi della sottorete facenti capo a nodi padre comuni non guasti. Nella topologia a stella, invece, il guasto dell'*hub* comporta la perdita totale della funzionalità di rete, risultando di fatto isolati tutti i nodi componenti.

Altro vantaggio importante delle topologie ad albero è l'elevata scalabilità[2]: infatti è possibile aggiungere o togliere nodi e connessioni senza modificare la rete né la sua funzionalità, fino al numero massimo di diramazioni consentite dal nodo padre. Inoltre, è molto facile l'accorpamento di più reti in un'unica rete, collegando direttamente tra loro i relativi nodi radice, senza che questo abbia ripercussioni sulle reti preesistenti.

Questa struttura di rete presenta importanti vantaggi anche in termini di efficienza nella distribuzione del segnale: potendo infatti demandare le funzionalità di indirizzamento nei nodi padre (se dotati di opportuna intelligenza), è possibile smistare il segnale in

maniera ottimizzata, di fatto secondo il percorso disponibile più breve. Anche l'elaborazione dell'instradamento e i relativi tempi risultano ottimizzati: infatti, con questa struttura, l'elaborazione dell'indirizzamento è distribuita tra i vari nodi padre, per le relative sottoreti, e non concentrata in un unico dispositivo centrale, e nei dispositivi di instradamento non richiede la conoscenza dell'intera rete ma solo della porzione che serve per gestire correttamente il trasferimento dell'informazione. Per tutti questi motivi, questa topologia di rete trova larghissimo impiego nelle reti di calcolatori e di telefonia, in particolare per quanto riguarda la parte di rete di distribuzione verso le utenze finali. Per garantire un'elevata scalabilità è sempre meglio partire da un'accurata analisi delle esigenze presenti, valutare quelle future e pianificare la struttura in modo da poterla espandere in futuro[3].

Topologie a maglia



Topologia completamente magliata

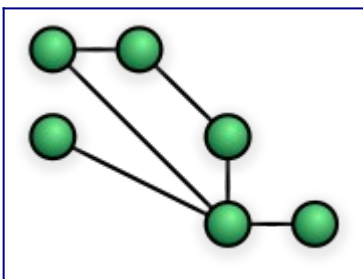
Topologia completamente magliata

La topologia completamente magliata o a maglia completamente connessa è quella di complessità più elevata in quanto prevede che ogni nodo sia collegato direttamente con tutti gli altri nodi della rete con rami dedicati. La relazione tra numero di nodi e rami è di tipo quadratico ed è data da:

$$R = N * (N - 1) / 2$$

La caratteristica più importante di questa rete è che, dato un nodo qualsiasi, esiste sempre almeno un percorso che consente di collegarlo a un altro nodo qualsiasi della rete.

Topologia parzialmente magliata



Topologia parzialmente magliata

La topologia parzialmente magliata o a maglia parzialmente connessa è una topologia che, dati N nodi, utilizza solo un sottoinsieme di tutti i collegamenti diretti definibili tra i nodi. Anche in questo caso la relazione tra numero di nodi e rami è non lineare, ma di tipo tendenzialmente quadratico, con una complessità inferiore rispetto al caso di rete completamente magliata e via via decrescente al decrescere dei rami utilizzati per i collegamenti tra i nodi, ed è espressa da una disuguaglianza:

$$(N - 1) < R < N * (N - 1) / 2$$

Da notare che gli estremi della disuguaglianza coincidono in un caso con la relazione che definisce le topologie lineari e nell'altro con la relazione che definisce la topologia completamente magliata. Questo indica che una topologia parzialmente magliata è data dalla combinazione di una o più sottoreti magliate con una o più sottoreti lineari.

Vantaggi e svantaggi

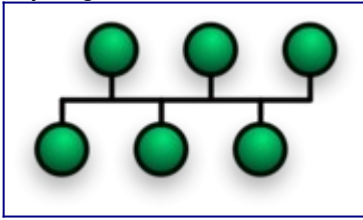
Il vantaggio principale delle topologie magliate è la robustezza di fronte ai guasti nei collegamenti tra i nodi. In una topologia completamente magliata, fino a quando un nodo non rimane completamente isolato, esisterà sempre almeno un percorso in grado di collegare tale nodo con il resto della rete. Questo vuol dire che in una rete di N nodi, prima che un nodo rimanga totalmente isolato devono interrompersi tutti gli

$N - 1$ collegamenti con gli altri nodi. Anche le topologie parzialmente magliate presentano un grado di robustezza analogo, via via decrescente a mano a mano che diminuiscono i rami usati per connettere direttamente tra loro i nodi.

Di contro, il rapporto quadratico tra numero di nodi e numero di rami costituisce un grosso ostacolo per la scalabilità: oltre un certo limite, aggiungere un nodo a una topologia completamente magliata richiede l'aggiunta di un numero sempre maggiore di rami, aumentando anche la complessità dell'intera rete. Di fatto, questo tipo di topologia risulta utilizzabile solo fino a quando il

numero dei nodi della rete è relativamente limitato e si usa principalmente per le dorsali di traffico (come per esempio l'infrastruttura ad alta capacità che unisce le centrali telefoniche regionali per la distribuzione a livello nazionale).

Topologia a bus



Rete con topologia a "bus"

Nella topologia a bus, tutti i nodi sono collegati tra di loro per mezzo di un unico ramo condiviso.

Questa topologia è molto efficiente dal punto di vista della scalabilità (l'aggiunta di un nodo non comporta aggiunta di collegamenti né interruzione dei collegamenti esistenti) e della robustezza (la rottura del bus porta ad avere comunque un partizionamento della rete in due topologie a bus) e per questi motivi è molto usata nelle reti dati: per esempio, la rete Ethernet nelle sue versioni iniziali *thickwire* e *thinwire*, era fisicamente strutturata a bus.

In questo tipo di topologia, la presenza di un unico collegamento condiviso tra tutti i nodi richiede di utilizzare meccanismi di controllo dell'accesso che evitino le collisioni o le interferenze tra i nodi.

Trasmissione nelle reti a bus

Un segnale proveniente dalla sorgente viaggia in entrambe le direzioni verso tutte le macchine collegate sul cavo bus fino a quando non trova il destinatario previsto. Se l'indirizzo della macchina non corrisponde all'indirizzo previsto per i dati, la macchina ignora i dati. In alternativa, se i dati corrispondono all'indirizzo della macchina, i dati vengono accettati. Poiché la rete di tipo bus è costituita da un solo filo, è piuttosto economica da implementare rispetto ad altre topologie. Tuttavia, il basso costo di implementazione della tecnologia è compensato dall'elevato costo di gestione della rete. Inoltre, poiché viene utilizzato un solo cavo, può essere il single point of failure. In questa topologia, i dati trasferiti possono essere accessibili da qualsiasi workstation.

Rete a bus lineare

Il tipo di topologia di rete in cui tutti i nodi della rete che sono collegati a un mezzo di trasmissione comune che ha esattamente due endpoints, tutti i dati trasmessi tra i nodi della rete vengono trasmessi su questo mezzo di trasmissione comune e possono essere ricevuti contemporaneamente da tutti i nodi della rete.






Nota: Quando il segnale elettrico raggiunge la fine del bus, il segnale viene riflesso indietro lungo la linea, causando interferenze indesiderate. Come soluzione, i due endpoint del bus sono normalmente terminati con un dispositivo chiamato terminatore che impedisce questa riflessione.


Rete a bus distribuito

La topologia di rete in cui tutti i nodi della rete, i quali sono connessi a un mezzo di trasmissione comune con più di due endpoint, creati aggiungendo rami alla sezione principale del mezzo di trasmissione, caratterizzano la topologia del bus distribuito, il quale funziona esattamente allo stesso modo della topologia del bus lineare (cioè, tutti i nodi condividono un mezzo di trasmissione comune).

(Rif. Bibliografici [31])

2.4 Classificazione dispositivi attivi (rif. fase 3)

Nome dispositivo	Immagine simbolica	In quale strato ISO/OSI lavora	In quale strato TCP/IP lavora	Descrizione e utilità
Router		3 (rete)	2 (rete)	Un router è un dispositivo di rete che lavora utilizzando indirizzi IP, effettua l'instradamento di pacchetti (routing) per far comunicare host/DTE appartenenti a reti diverse. Deve essere collegato ad almeno due network; in genere a due LAN o a due WAN o una LAN ed un network ISP. I router identificano il percorso da seguire utilizzando headers e tabelle di instradamento ed utilizzano protocolli di comunicazione per comunicare tra di loro e per stabilire l'instradamento ottimale tra due host.
Switch	 	2 (link)	1 (fisico)	Uno switch è un dispositivo di rete che permette la comunicazione di lavoro utilizzando indirizzi MAC, ovvero consente la commutazione dei frame filtrandoli e instradandoli direttamente verso un preciso host di destinazione tramite il suo indirizzo MAC. Nei livelli TCP/IP gli switch sono in grado di supportare qualsiasi protocollo dati, nel TCP/IP operano a livello fisico (liv 1) e nella pila ISO/OSI operano a livello collegamento. Con gli switch non condivide la lunghezza di banda (bandwidth) con tutte le sue porte (come avviene invece per l'HUB). Rispetto agli HUB gli switch gestiscono i pacchetti dati in maniera più efficiente e veloce ed è possibile configurare quanta % di bandwidth destinare ad ogni porta.
Bridge		2 (link)	1 (fisico)	Il bridge è un dispositivo di rete si colloca al livello collegamento (ovvero di collegamento) nel modello ISO/OSI e livello fisico nel modello TCP/IP. Svolge il ruolo di "smistatore di dati e pacchetti" tra i due o più router Wi-Fi o Ethernet dai quali a loro volta si originano le reti da mettere in comunicazione. Questo dispositivo di rete è quindi in grado di riconoscere, nei pacchetti che riceve, qual è l'indirizzo del mittente e quale quello del destinatario indipendentemente dalla rete di appartenenza e si occupa pertanto di indirizzare i pacchetti in transito verso il giusto nodo della giusta rete. Il bridge può tornare utile, quindi, per condividere e scambiare dati tra i dispositivi di reti differenti oppure per condividere la connessione ad Internet con una o più reti non dotate di uscite autonome verso il web.
HUB		1 (fisico)	1 (fisico)	Un Hub è un dispositivo di rete si colloca al livello collegamento (ovvero di collegamento) nel modello ISO/OSI e livello fisico nel modello TCP/IP. L' hub rappresenta un punto di collegamento comune per dispositivi in un network. Gli hub in genere sono utilizzati per collegare segmenti di una LAN. Un hub contiene molteplici porte. Quando un pacchetto dati arriva in una porta, viene immediatamente copiato anche sulle altre porte così che anche gli altri network possano vedere i pacchetti dati. L' hub condivide la lunghezza di banda (bandwidth) con tutte le sue porte, quindi se per esempio molteplici HOST inviano dati all'hub , la bandwidth sarà suddivisa tra tutti i sistemi attivi, tutto ciò a discapito della performance.
Repeater		1 (fisico)	1 (fisico)	Un repeater (ripetitore), nelle telecomunicazioni, indica un dispositivo elettronico che riceve in ingresso un segnale e lo ritrasmette in uscita tipicamente con un segnale a potenza maggiore cosicché la propagazione di questo può essere garantita anche a lunghe distanze senza eccessiva attenuazione e/o degradazione.
Modem		1 (fisico)	1 (fisico)	il modem (modulatore-demodulatore, dall'inglese modulator-demodulator), nelle telecomunicazioni ed elettronica, è un dispositivo di ritrasmissione che ha funzionalità logiche di modulazione/demodulazione (analogica o digitale) in trasmissioni analogiche e digitali. Nell'accezione più comune il modem è un apparecchio di collegamento telefonico di un terminale (ad esempio un computer) a una rete di trasmissione dati, che converte (modula) i segnali digitali in impulsi analogici e, in fase di

				ricezione, riconverte (demodula) gli impulsi analogici in segnali digitali.
Access Point		1 (fisico)	1 (fisico)	<p>Un Access Point (in inglese punto di accesso, anche indicato con l'acronimo AP) è un dispositivo di rete che consente l'accesso wireless, in ambito locale, a una rete di comunicazione elettronica.</p> <p>L'uso tipico di un Access Point è quello di collegarlo ad una LAN e consentire così ad utenti muniti di dispositivi wireless di usufruire dei servizi di rete LAN con in aggiunta il vantaggio della mobilità. In questa configurazione l'Access Point agisce da gateway per i client wireless.</p> <p>Un Access Point IEEE 802.11 può normalmente comunicare con circa 30 client nel raggio di circa 100 m, anche se il range di copertura può scendere sensibilmente in presenza di ostacoli fisici nella linea di vista. La banda di comunicazione può variare molto in funzione di diverse variabili come il posizionamento interno o esterno, l'altezza dal suolo, la presenza di ostacoli vicini, il tipo di antenna, le attuali condizioni meteo, la frequenza radio su cui opera e la potenza di output del dispositivo. La banda dell'Access Point può essere estesa attraverso l'utilizzo di Repeater (ripetitori).</p>

(Rif. Bibliografici [1],[2],[3],[4],[5],[30])

2.5 Scelta e analisi modalità di connessione (rif. fase 4)

le tipologie di collegamento (link) nelle reti si dividono principalmente in due macrocategorie:

- wireless (senza cavi fisici)
- Ethernet (tramite cavi fisici)

RETI CON CAVI ETHERNET

Ethernet è una famiglia di tecnologie standardizzate per reti locali che ne definisce le specifiche tecniche a livello fisico (ad esempio connettori, cavi, tipo di trasmissione) e a livello di collegamento di dati del modello architetturale di rete ISO/OSI.

Commercializzata nel 1980 e inizialmente standardizzata nel 1983 come IEEE 802.3, è ampiamente utilizzata nell'industria, il protocollo Internet viene comunemente trasmesso su Ethernet e pertanto è considerata una delle tecnologie chiave che compongono Internet; più in generale è utilizzata nelle reti locali (LAN), nelle reti metropolitane (MAN) e nelle reti geografiche (WAN).

La gestione delle collisioni viene regolata dal protocollo Carrier Sense Multiple Access / collision detect (CSMA/CD)

Il CSMA/CD (acronimo inglese di Carrier Sense Multiple Access with Collision Detection, ovvero accesso multiplo tramite rilevamento della portante con rilevamento delle collisioni) è un protocollo di accesso multiplo, evoluzione del protocollo di livello MAC CSMA, nato per la risoluzione dei conflitti di trasmissione, ovvero collisioni, dovuti al CSMA puro, presenti in un certo dominio di collisione su reti locali cablate di tipo broadcast.

In pratica, il protocollo CSMA/CD consente ad un computer di utilizzare la rete Ethernet soltanto se nessun altro elaboratore la sta già utilizzando.

Il protocollo implementa la direttiva: "Ascolta prima di trasmettere e mentre trasmetti. Se mentre trasmetti rilevi collisioni, fermati, segnala a tutte le altre stazioni la collisione e riprova più tardi secondo modalità di ritrasmissione stabilite."

Cavi ethernet in fibra ottica, nella scienza e tecnologia dei materiali, indica un materiale costituito da filamenti vetrosi o polimerici, realizzati in modo da poter condurre al loro interno la luce, trovando importanti applicazioni in telecomunicazioni, diagnostica medica e illuminotecnica: con un diametro di rivestimento (mantello) di 125 micron (circa le dimensioni di un capello) e peso molto ridotto, sono disponibili sotto forma di cavi, flessibili, immuni ai disturbi elettrici e alle condizioni atmosferiche più estreme, e poco sensibili a variazioni di temperatura.

Principali i cavi Ethernet usati:

- Ethernet base 10 BaseT (in rame), velocità massima 10Mbps, distanza max 100m (obsoleto);
- FastEthernet 100 Base-TX, (in rame), velocità massima 100Mbps, banda 125 MHz, distanza max 100m (più usato);
- FastEthernet 100 Base-FX, (in fibra ottica multimodale), velocità massima 100Mbps, banda 760Mhz, distanza max 2km;
- FastEthernet 100 Base-LX, (in fibra ottica monomodale), velocità massima 100Mbps, banda 650Mhz, distanza max 60km;
- GigaBit Ethernet 1000Base-CX (in rame), velocità massima 1.25 Gbps, distanza max 25m;
- GigaBit Ethernet 1000Base-TX (in rame), velocità massima 1Gbps, banda 100mhz, distanza max 100m;
- GigaBit Ethernet 1000Base-SX (in fibra ottica multimodali), velocità massima 1 Gbps, 62,5micron, banda 160Mhz, distanza max 220m;
- GigaBit Ethernet 1000Base-SX (in fibra ottica multimodali), velocità massima 1 Gbps, 62,5micron, banda 200Mhz, distanza max 275m;
- GigaBit Ethernet 1000Base-SX (in fibra ottica multimodali), velocità massima 1 Gbps, 50micron, banda 400Mhz, distanza max 500m;
- GigaBit Ethernet 1000Base-SX (in fibra ottica multimodali), velocità massima 1 Gbps, 50micron, banda 500Mhz, distanza max 550m;
- GigaBit Ethernet 1000Base-LX (in fibra ottica monomodali), velocità massima 1 Gbps, 62,5micron, banda 500Mhz, distanza max 550m;
- GigaBit Ethernet 1000Base-LX (in fibra ottica monomodali), velocità massima 1 Gbps, 50micron, banda 400Mhz, distanza max 550m;
- GigaBit Ethernet 1000Base-LX (in fibra ottica monomodali), velocità massima 1 Gbps, 50micron, banda 500Mhz, distanza max 550m;
- GigaBit Ethernet 1000Base-LX (in fibra ottica monomodali), velocità massima 1 Gbps, 62,5micron, distanza max 5km;

ANALISI COLLEGAMENTI WIRELESS

Le tipologie di rete wireless in base all'area di copertura:

- WPAN (Wireless Personal Area Network), a livello domestico
- WLAN (Wireless Local Area Network) propriamente dette come il Wi-fi.
- WAN (Wide Area Network) wireless
- BWA (Broadband Wireless Access), che sta conoscendo grande diffusione grazie alla tecnologia WiMA

Le tipologie di rete wireless in base al tipo di tecnologia:

- reti cellulari radiomobili come GSM, GPRS, EDGE, UMTS, HSPA, LTE
- reti WiFi (onde radio)
- reti Bluetooth
- reti IR (luce infrarossa)
- sistemi laser
- reti satellitari

Reti WiFi

Le reti WiFi (onde radio) trasmettono informazioni tramite l'aria utilizzando onde radio, che sono un tipo di radiazione elettromagnetica con lunghezze d'onda di 122 mm circa e più lunghe degli infrarossi. Le onde radio WiFi hanno tipicamente una frequenza di 2.4 gigahertz o 5.8 gigahertz. Queste due bande di frequenza WiFi sono poi suddivise in canali multipli, con ogni canale possibilmente condiviso da più reti diverse. il WiFi vengono utilizzate dalle reti che devono coprire ambienti eterogenei dove le diverse postazioni da collegare non sono necessariamente visibili, infatti possono essere separate da muri o da intercapedini.

Principali modalità di connessione WiFi usate:

WiFi 3, banda a 2.4GHz, standard 802.11g (2003), velocità max 54Mbps, distanza max 100m

WiFi 4, banda a 2.4GHz e 5Ghz, standard 802.11n (2009), velocità max 600 Mbps, distanza max 100m

WiFi 5, banda a 5Ghz, standard 802.11ac (2014), velocità max 1,3 Gbps, distanza max 100m

WiFi 6, banda tra 1 e 6 GHz, standard 802.11ax (2019), velocità max 11 Gbit/s, distanza max 100m
Wi-Fi 7: verrà rilasciato nel 2024, velocità max teorica 30 Gbit/s

Sicurezza rete Wi-Fi

i protocolli di sicurezza più usati nelle connessioni Wi-Fi:

protocollo WEP. Wired Equivalent Privacy

protocollo WPA. Wi-Fi Protected Access

protocollo WPA2. Wi-Fi Protected Access Versione 2 (anno 2004, cifratura AES)

WPA3. Wi-Fi Protected Access Versione 3, in arrivo nel 2023

Reti Bluetooth

Bluetooth (spesso abbreviato in BT) è uno standard tecnico-industriale di trasmissione dati per reti personali senza fili (WPAN: Wireless Personal Area Network). Fornisce un metodo standard, economico e sicuro per scambiare informazioni tra dispositivi diversi attraverso una frequenza radio sicura a corto raggio in grado di ricercare i dispositivi coperti dal segnale radio entro un raggio di qualche decina di metri mettendoli in comunicazione tra loro. Questi dispositivi possono essere ad esempio palmari, telefoni cellulari, personal computer, portatili, stampanti, fotocamere digitali, smartwatch, console per videogiochi, cuffie, purché provvisti delle specifiche hardware e software richieste dallo standard stesso. Il BT si è diffuso da tempo anche nel settore industriale (strumenti di misura, lettori ottici, ecc.) per il dialogo con i relativi datalogger.

Principali modalità di connessione Bluetooth usate:

Bluetooth 4.1, banda da 2.4 a 2.485, velocità max 24Mbps, distanza max 100m

Bluetooth 5, banda da 2.4 a 2.485, velocità max 48Mbps, distanza max 300m

Reti IR

Le reti basate su infrarossi (IR) vengono utilizzate per collegare dispositivi visibili direttamente, sono lente, spesso utilizzano dispositivi dedicati e come infatti sono in disuso sostituite quasi totalmente dai dispositivi Bluetooth. La radiazione infrarossa (IR), in fisica, è la radiazione elettromagnetica con banda di frequenza dello spettro elettromagnetico inferiore a quella della luce visibile, ma maggiore di quella delle onde radio, ovvero lunghezza d'onda compresa tra 700 nm e 1 mm (banda infrarossa). Il termine significa "sotto il rosso" (dal latino infra, "sotto"), perché il rosso è il colore visibile con la frequenza più bassa.

Reti satellitari

Le reti satellitari sono una forma di telecomunicazioni wireless a radiofrequenza per la comunicazione a distanza di informazione attraverso collegamenti radio satellitari fra stazioni ricetrasmittenti a terra e satelliti artificiali in orbita sotto forma di ponti radio satellitari, radiodiffusioni, telediffusioni, reti di telecomunicazioni e sistemi di radiolocalizzazione e navigazione.

frequenze utilizzate:

L'uso di una particolare frequenza di trasmissione dipende dall'applicazione di un dato sistema. La gamma di frequenze si estende dalla banda P alla banda Ka e oltre:

banda P (0,2–1 GHz)

banda L (1–2 GHz)

banda C (4–8 GHz)

banda Ku (12–18 GHz)

banda Ka (26,5–40 GHz)

Sistemi laser

Le reti basate su Laser vengono utilizzate normalmente per collegare sottoreti costruite utilizzando altre tecnologie. Il Laser viene utilizzato per la sua elevata velocità di trasmissione. Un tipico esempio è il collegamento delle reti di due edifici vicini. Il laser ha il problema di essere sensibile alle condizioni esterne e alle vibrazioni infatti anche queste tipologie di dispositivi sono considerati in disuso e quasi sempre sostituiti da collegamenti via onde radio.

Reti cellulari radiomobili

Una rete di telecomunicazione cellulare (anche rete cellulare o rete mobile) è una rete che permette la telecomunicazione in tutti i punti di un territorio suddiviso in aree di non grandi dimensioni, chiamate "celle" (da cui la definizione) per la telefonia radiomobile cellulare, ognuna servita da una diversa stazione radio base.

(Rif. Bibliografici da [18] a [28])

3.1 Indirizzamento IPv4

Un esempio di indirizzo IP è 172.16.254.1.

In informatica e nelle telecomunicazioni, un indirizzo IP (dall'inglese Internet Protocol address) è un codice numerico che identifica univocamente un dispositivo detto host collegato a una rete informatica

L'indirizzo IPv4 è costituito da 32 bit (4 byte) suddiviso in 4 gruppi da 8 bit (1 byte), separati ciascuno da un punto (notazione dotted, es. 11001001.00100100.10101111.00001111) quindi ogni numero varia tra 0 e 255 essendo $2^8=256$, ovvero le combinazioni disponibili ci dicono quanti numeri possiamo utilizzare in ogni gruppo identificato dal punto.

Viene assegnato a un'interfaccia (ad esempio una scheda di rete) che identifica l'host di rete, che può essere un personal computer, un palmare, uno smartphone, un router, o anche un elettrodomestico. Va considerato, infatti, che un host può contenere più di una interfaccia: ad esempio, un router ha diverse interfacce (minimo due) per ognuna delle quali occorre un indirizzo IP. Formato IPv4:

L'indirizzo IP si compone di due parti: indicatore di rete (Net_ID) e indicatore di host (Host_ID). La prima parte identifica la rete, chiamata network o routing prefix (Net_ID) ed è utilizzata per l'instradamento a livello di sottoreti.

La seconda parte invece identifica, all'interno della rete, l'host e le eventuali sottoreti (Host_ID) ed è utilizzato per l'instradamento a livello locale dell'host una volta raggiunta la sottorete locale di destinazione, cui segue la traduzione o risoluzione in indirizzo MAC per l'effettiva consegna del pacchetto dati al destinatario con i protocolli della rete locale. (Rif. Bibliografico [10])

Gli indirizzi IP sono suddivisi in classi. Le classi di indirizzi IP (o classful addressing) sono una formalità per dividere lo spazio di indirizzamento IPv4 introdotta dal RFC791 nel 1981 ed in uso fino all'introduzione nel 1993 del Classless Inter-Domain Routing (detta Annotazione CIDR). (Rif. Bibliografico [10])

		Utilizzo bit (N: Network; H: Host)	Subnet mask	Reti disponibili	Host disponibili per rete	Indirizzi totali	Note
Class e	A	0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH	255.0.0.0/8	128	16.777.216 (-2)	2.147.483.39 2	
	B	10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH	255.255.0.0/16	16.384	16.38465.536 (-2)	1.073.709.05 6	
	C	110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH	255.255.255.0/24	2.097.152	2.097.152256 (-2)	532.676.608	
	D	1110XXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX					Multicast
	E	1111XXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX					usi futuri

In questo modo il tipo di classe si può determinare sulla base dei bit più significativi. Vediamo come:

CLASSE A	bit fissi = 0 NET-ID assegnato a otetto 1 HOST-ID assegnato a otetto 2,3,4 -> 2^{24} host disponibili TOTALE= 0(bit fisso) + 7bit (net) + 24 bit (host) 00000000.00000000.00000000.00000000 0 - 01111111.11111111.11111111.11111111 cioè da 0.0.0.0(d) - 127.255.255.255	La maschera di rete è 255.0.0.0 (o anche detta /8 in quanto i bit di rete sono 8);	Da 0.0.0.0 a 127.255.255.255
CLASSE B	bit fissi = 1.0 NET-ID assegnato a otetto 1,2	La maschera di rete è 255.255.0.0 (o anche detta /16 in quanto i bit di	da 128.0.0.0 a 191.255.255.255

	<p>HOST-ID assegnato a ottetto 3,4-> 2¹⁶ host disponibili</p> <p>TOTALE= 1.0.(2 bits fissi) + 14bit (net) + 16 bit (host)</p> <p>10000000.00000000.00000000.00000000 0 - 10111111.11111111.11111111.11111111 cioè da 128.0.0.0 - > 191.255.255.255.</p>	rete sono 16);	
CLASSE C	<p>bit fissi = 1.1.0 NET-ID assegnato a ottetto 1,2,3 HOST-ID assegnato a ottetto 4 -> 2⁸ host disponibili</p> <p>TOTALE= 1.1.0(3 bits fissi) + 21bit (net) + 8 bit (host)</p> <p>1100000.00000000.00000000.00000000 - 11011111.11111111.11111111.11111111 cioè da 192.0.0.0 - > 223.255.255.255.</p>	La maschera di rete è 255.255.255.0 (o anche detta /24 in quanto i bit di rete sono 24);	da 192.0.0.0 a 223.255.255.255
CLASSE E	È riservata agli indirizzi multicast. Questi indirizzi in binario iniziano con i bit 1110.	Non è definita una maschera di rete, essendo tutti e 32 i bit dell'indirizzo utilizzati per indicare un gruppo, non un singolo host;	da 224.0.0.0 a 239.255.255.255
CLASSE E	Riservata per usi futuri; Questi indirizzi in binario iniziano con i bit 1111.	Non è definita una maschera di rete;	da 240.0.0.0 a 255.255.255.255

(Rif. Bibliografico [13])

3.2 Formule IPv4

Convertitore, binario, decimale, esadecimale, ottale <http://www.giulianosrl.com/Con-Esa.htm>

Convertire un indirizzo IP da decimale a binario http://www.electronic-sud.it/rubriche/reti_telecomunicazioni/convertire-ip-in-binario.php

Subnet Calculator per IPV4 <https://www.site24x7.com/it/tools/ipv4-sottorete-calcolatrice.html>

Subnet/HOST Calculator http://archivio.tuttureti.it/stru_subcalc.htm

Subnet, IP range, e altre utili informazioni <https://httplab.it/ipcalc.php>

Calcolo Subnet1 <https://www.iltuoip.it/calcolo-subnet.php>

Calcolo Subnet2 <http://www.piovaniconsulenze.com/CalcoloSubNet.htm>

Calcolatore di subnet <https://www.spaziolink.com/calcolatoredisubnet/>

CALCOLO HOST ASSEGNABILI PER CLASSI DI INDIRIZZAMENTO:

Classe A: $2^{24} = 6.777.216$ host disponibili

Classe B: $2^{16} = 65.536$ host disponibili

Classe C: $2^8 = 256$ host disponibili

PER TROVARE LA CLASSE DI INDIRIZZAMENTO DI UN IP:

si converte in binario il primo ottetto e si capisce subito in base ai bit fissi, 0=classe A, 1.0 = classe B, 1.1.0 = classe C

PER TROVARE LA NETMASK DI UNA NOTAZIONE /n_bit

si pongono a 1 tutti gli /n_bit iniziali ed a 0 il resto e poi si converte ogni singolo ottetto in decimale

ESTRARRE L'INDIRIZZO DI RETE DA UN IP:

si converte l'indirizzo IP e la sua subnetmask in binario, poi si effettua l'AND logico bit-a-bit tra i due indirizzi

CALCOLO SUBNET MASK MINIMA con 2 o più sottoreti

sia Rmax la sottorete con il maggior numero di host tra le presenti,

sia h_bit il numero di bit da dedicare agli host $\rightarrow h_bit = \text{round}(\log_2(Rmax)) / (\text{subnetmask}) = / (32-h_bit)$

CALCOLO NUMERO DI HOST POSSIBILI:

si segue la formula $2^{(32-x)} - 2$ con la x che rappresenta il numero della NetMask, inoltre si sottrae 2 perché è necessario escludere l'indirizzo di broadcast e di rete

CALCOLO NUMERO DI SOTTORETI POSSIBILI:

sia n_bit il numero di bit a 1 della subnetmask (da notazione CIDR /nbit),

sia A o B o C la classe di indirizzo della rete,

sia n_rete=numero di bit riservati alla rete di questa classe,

sia $S = n_bit - n_rete$ (ovvero S=il numero di bit dedicati SUBNET-ID)

\rightarrow il numero max di sottoreti è 2^S

CALCOLO INDIRIZZO BROADCAST:

L'ultimo indirizzo possibile dell'ottetto dedicato agli HOST

CALCOLO INDIRIZZO GATEWAY (per le reti non isolate dove si assegna un ip riservato al router)

In genere è il primo indirizzo possibile oppure il penultimo dell'ottetto dedicato agli HOST

CALCOLO RANGE IP POSSIBILI:

(da inserire)

3.3 Rete, sottorete e subnetting

In ambito di networking i termini "rete" e "sottorete" (o "subnet" in inglese) hanno significati distinti ma correlati.

1) Rete:

- Una rete, nel contesto di internetworking, è un insieme di dispositivi connessi che possono comunicare tra loro. Questa comunicazione avviene attraverso protocolli di rete come TCP/IP. Una rete può essere costituita da un insieme di computer, server, router, switch e altri dispositivi di rete. Dal punto di vista dell'indirizzamento IP, una rete è definita da un indirizzo IP e una maschera di sottorete che insieme determinano l'intervallo degli indirizzi IP appartenenti a quella rete.

2) Sottorete (Subnet):

- Una sottorete è una divisione più piccola di una rete più grande. La subnetting è una tecnica utilizzata per suddividere una rete IP in più reti più piccole, ognuna con la propria gamma di indirizzi IP unici. Questo si ottiene modificando la maschera di sottorete per allocare una parte degli indirizzi IP originariamente destinati alla rete a più sottoreti.

Le sottoreti sono utili per:

- Migliorare la gestione della rete, dividendo grandi reti in segmenti più facilmente amministrabili.
- Ridurre il traffico di broadcast.
- Ottimizzare l'uso degli indirizzi IP.

Esempio pratico:

Se hai una rete con indirizzo IP 192.168.1.0 e una maschera di sottorete 255.255.255.0, questa rete può ospitare indirizzi IP da 192.168.1.1 a 192.168.1.254.

Se vuoi creare sottoreti, potresti cambiare la maschera in 255.255.255.128, dividendo questa rete in due sottoreti:

- 192.168.1.0 - 192.168.1.127 (sottorete 1)
- 192.168.1.128 - 192.168.1.255 (sottorete 2)

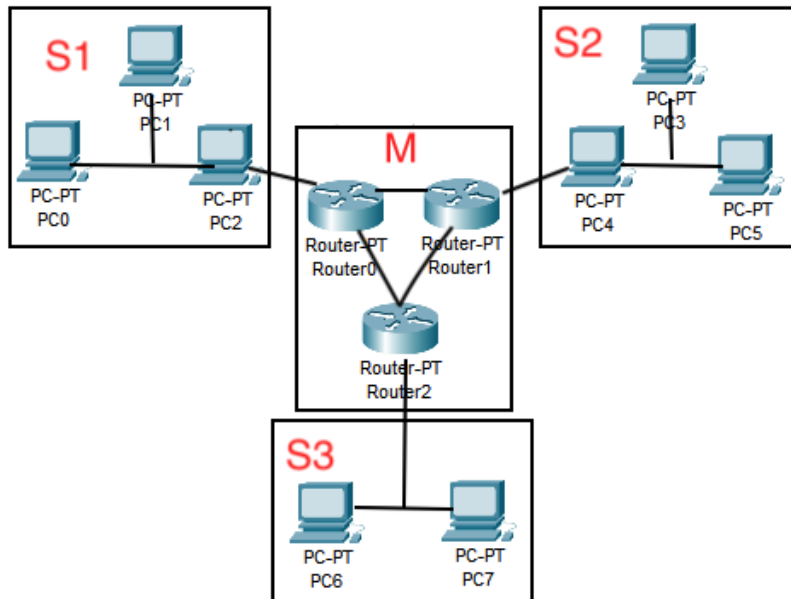
Ogni sottorete ha i propri indirizzi IP utilizzabili, indirizzi di broadcast e indirizzi riservati (come quello della rete stessa e quello di broadcast).

In sintesi, mentre una rete è un grande insieme di dispositivi interconnessi, una sottorete è una parte più piccola di questa rete, progettata per una gestione e un utilizzo più efficiente delle risorse di rete.

3) **il subnetting** è una tecnica utilizzata per suddividere una rete in sottoreti più piccole e può essere applicata a qualsiasi classe di indirizzo IP (A, B o C) con il fine di minimizzare il numero di indirizzi IP da assegnare agli host. Invece di assegnare un intero blocco di indirizzi IP a una singola rete, il subnetting consente di dividere quel blocco in segmenti più piccoli, riducendo il numero di indirizzi IP inutilizzati e migliorando l'efficienza nella gestione degli indirizzi.

Un altro vantaggio del subnetting è che può migliorare le prestazioni e la sicurezza della rete. Suddividendo una rete in sottoreti più piccole, è possibile limitare la quantità di traffico di broadcast e isolare segmenti di rete per proteggere meglio i dati sensibili.

3.4 Progetto SUBNETTING N.1



Tre sedi con S1=50 host, S2=40 host, S3=20 host, con 3 router per ogni rete e collegati a loro a 'maglia' formando una rete per la WAN (rete M), progettare una rete utilizzando la tecnica del 'subnetting' partendo da un piano di indirizzamento di classe C con indirizzo 200.69.96.0

OBIETTIVO PRINCIPALE: progettare una rete a livello logico significa trovare un piano di indirizzamento ottimale per host, reti e sottoreti con i seguenti vincoli:
1) limitare il numero di bit per gli ip

- dedicati agli host;
2) ogni rete o sottorete deve avere 1 ip di rete;
3) ogni host deve avere 1 ip;
4) per ogni rete o sottorete 1 indirizzo ip deve essere dedicato al broadcast (per convenzione deve essere l'ultimo indirizzo dell'intervallo della sottorete);
5) per ogni rete o sottorete 1 indirizzo ip deve essere dedicato al gateway (l'indirizzo gateway o indirizzo-router per convenzione è spesso l'indirizzo IP più basso utilizzabile in una sottorete).

PREMESSA1, perchè è utile ricorrere alla tecnica del subnetting?

con il subnetting si creano artificialmente delle sottoreti (ovvero reti più piccole derivate da reti più grandi) e sono utili per:

- Migliorare la gestione della rete, dividendo grandi reti in segmenti più facilmente amministrabili.
- Ridurre il traffico di broadcast.
- Ottimizzare l'uso degli indirizzi ip.

PREMESSA2: come utilizzare il gateway?

i gateway sono indirizzi ip che i dispositivi della sottorete usano per inviare pacchetti di dati verso altre reti.

La convenzione di usare il primo indirizzo ip utilizzabile non è obbligatoria ma comune. in alcune configurazioni, il gateway potrebbe essere un altro indirizzo all'interno della sottorete, ma per semplicità, spesso si utilizza il primo IP utilizzabile.

PREMESSA3: perchè limitare il numero di bit per gli ip dedicati agli host?

significa che l'obiettivo è minimizzare lo spreco di indirizzi IP assegnando solo il numero di bit necessari per il numero di host previsto, evitando di lasciare troppi indirizzi inutilizzati.

SOLUZIONE

DOMANDA 1) N-SUBNET: quanti possibili raggruppamenti (o sottoreti) di host (DTE e nodi) si individuano visivamente guardando la rete complessiva?

RISPOSTA? 4

DOMANDA 2) HOST-BIT , quanti bit sono necessari per riuscire ad assegnare 1 ip ad ogni host della la sottorete più grande?

RISPOSTA: (ditemelo voi),

poiché si parte dal piano assegnato 200.69.96.0 che viene classificata come la classe assegnata C (ovvero 24bit rete, 8 bit host) e facciamo alcuni calcoli:

- \log_2 della subnet con host più numerosi più grande (50 host)

- $\log_2 (50) = 5,64 \rightarrow 6$ bit

ciò significa che sono necessari al max non più di 6 bit della parte host, visto che le altre subnet sono più piccole di 50 host, quindi bastano 6 bit.

DOMANDA 3) NEW-CIDR, dopo aver trovato il numero minimo di bit per coprire la parte host, quale sarà la notazione CIDR della rete+sottorete?

RISPOSTA: 200.69.96.0/26,

poiché essendo che nella classe C l'ultimo ottetto è formato da 8 bit, ma a noi ce ne servono 6, i restanti 2 bit inutilizzati li agganciamo come bit di rete all'ottetto precedente. siccome nella classe C i primi 24 sono rete e 8 sono host, adesso avremo i primi 26 sono rete (24+2) e gli ultimi 6 sono host

DOMANDA 4) MAX-SUBNET, quante sottorete possiamo formare con la notazione CIDR trovata?

RISPOSTA: con 200.69.96.0/26 abbiamo 4 sottorete,

poiché 26 bit - 24 bit (della classe C di partenza) = 2 bit, ovvero 00,01,10,11

DOMANDA 5) con questi HOST-BIT e MAX-SUBNET il servizio è coperto?

RISPOSTA: Sì, perchè N-SUBNET = MAX-SUBNET e HOST-BIT copre la subnet più grande di 50 host

DOMANDA 6) per ogni sottorete abbiamo tutti i dati necessari per indicare (in rigoroso ordine) indirizzo di rete, indirizzo di gateway, indirizzo di broadcast, range di ip degli host?

RISPOSTA: Sì, ecco come,

la subnet S1 inizierà con i bit 00 e finiranno con i restanti 6 bit 0, quindi 00.000000, quindi 1a sottorete: 200.69.96.0;

la subnet S2 inizierà con i bit 01 e finiranno con i restanti 6 bit 0, quindi 01.000000, quindi 2a sottorete: 200.69.96.64;

la subnet S3 inizierà con i bit 10 e finiranno con i restanti 6 bit 0, quindi 10.000000, quindi 3a sottorete: 200.69.96.128;

la subnet "M" inizierà con i bit 11 e finiranno con i restanti 6 bit 0, quindi 11.000000, quindi 4a sottorete: 200.69.96.192;

gateway di S1 è l'ip più basso a partire dall'indirizzo di rete, ovvero 200.69.96.0 +1 ovvero 200.69.96.1;

gateway di S2 è l'ip più basso a partire dall'indirizzo di rete, ovvero 200.69.96.64 +1 ovvero 200.69.96.65;

gateway di S3 è l'ip più basso a partire dall'indirizzo di rete, ovvero 200.69.96.128 +1 ovvero 200.69.96.129;

gateway di "M" è l'ip più basso a partire dall'indirizzo di rete, ovvero 200.69.96.192 +1 ovvero 200.69.96.193;

broadcast di S1 è l'ultimo indirizzo dell'intervallo della sottorete, ovvero 200.69.96.64 (rete successiva) - 1 ovvero 200.69.96.63;

broadcast di S2 è l'ultimo indirizzo dell'intervallo della sottorete, ovvero 200.69.96.128 (rete successiva) - 1 ovvero 200.69.96.127;

broadcast di S3 è l'ultimo indirizzo dell'intervallo della sottorete, ovvero 200.69.96.192 (rete successiva) - 1 ovvero 200.69.96.191;

broadcast di "M" è l'ultimo indirizzo dell'intervallo della sottorete, quindi 200.69.96.255 essendo l'ultimo rete si prende l'ultimo host disponibile

range ip host di S1 (50), per S1 sottorete si prendono gli indirizzi rimasti per raggruppamenti togliendo rete, gateway e broadcast, quindi da 200.69.96.2 a 200.69.96.51;

range ip host di S2 (40), per S2 sottorete si prendono gli indirizzi rimasti per raggruppamenti togliendo rete, gateway e broadcast, quindi da 200.69.96.66 a 200.69.96.105;

range ip host di S3 (20), per S3 sottorete si prendono gli indirizzi rimasti per raggruppamenti togliendo rete, gateway e broadcast, quindi esercizio per casa;

range ip host di "M" (3), per S4 sottorete si prendono gli indirizzi rimasti per raggruppamenti togliendo rete, gateway e broadcast, quindi esercizio per casa;

DOMANDA 7) ma se per la prima sottorete S1 devo assegnare gli ip a solo 50 host, il broadcast è sempre 200.69.96.63?

RISPOSTA) Sì, esattamente.

Anche se decidi di assegnare indirizzi IP a solo 50 host nella sottorete 200.69.96.0/26, l'indirizzo di broadcast rimane 200.69.96.63.

L'indirizzo di broadcast è determinato dalla maschera di sottorete e non dal numero di host effettivamente utilizzati all'interno della sottorete. Una sottorete /26 ha sempre un intervallo di 64 indirizzi IP (di cui 62 sono utilizzabili per gli host), e l'ultimo di questi indirizzi è riservato come indirizzo di broadcast.

Quindi, indipendentemente dal fatto che tu utilizzi tutti i 62 indirizzi IP disponibili o solo una parte di essi, l'indirizzo di broadcast per questa sottorete sarà sempre 200.69.96.63.

DOMANDA 8) essendo la 4a sottorete una rete M formata da soli 3 router (come si vede in foto), ha senso assegnare per questa sottorete 3 ip di gateway?

RISPOSTA) Non è esplicitamente vietato, ma non è comune né consigliabile avere più di 1 indirizzo 'default gateway' per ogni sottorete per ovvi motivi di gestione del traffico e del broadcast.

invece un router all'interno della rete M può essere tranquillamente selezionato come l'unico gateway per tutta la rete M, quindi questo router ad esempio avrà la responsabilità di inoltrare il traffico verso e dai router che collegano direttamente a S1 e S3.

DOMANDA 9) nell'esercizio ho visto che c'è un'immagine raffigurante l'intera rete e c'è anche una sottorete "M" formata solo da 3 router (si chiamano router 0, router 1, router 2), ha senso metterne 3 invece di 1 solo router?

RISPOSTA)

Mettere tre router nella sottorete M invece di uno solo ha assolutamente senso in diversi scenari di rete:

- Redundanza e Affidabilità:

avere più router permette di fornire percorsi alternativi per il traffico. Se un router fallisce, gli altri possono continuare a gestire il traffico, migliorando l'affidabilità della rete.

- Load Balancing (ovvero Distribuzione del Carico):

con tre router, è possibile distribuire il carico di rete tra di loro, migliorando le performance complessive della rete. Questo è particolarmente utile se la rete M collega sottoreti con alto traffico.

- Segmentazione della Rete (ovvero Gestione di Sottoreti Multiple):

se ogni router di M è collegato a una diversa sottorete (come S1, S2, S3), allora avere tre router aiuta a segmentare la rete in modo più efficiente, permettendo a ciascun router di gestire e ottimizzare il traffico per la sua sottorete.

- Scalabilità (ovvero Espansione Futura):

anche se attualmente ci sono solo tre router, questo setup permette una facile espansione. Aggiungere nuove sottoreti o nuovi dispositivi può essere fatto senza dover riconfigurare drasticamente la rete esistente.

- Routing Dinamico (Protocolli di Routing) :

Con più router, si possono implementare protocolli di routing dinamico come OSPF o EIGRP, che non solo offrono percorsi ridondanti ma anche la capacità di adattare automaticamente le rotte in base alle condizioni della rete.

- Isolamento e Sicurezza:

avere più router può facilitare l'implementazione di politiche di sicurezza e controllo del traffico più granulari tra le diverse parti della rete.

- Topologia di Rete (Mesh o Star):

La configurazione con tre router può supportare una topologia di rete più complessa o resiliente, come una rete mesh dove ogni router è collegato agli altri, o una topologia a stella dove uno dei router funge da hub per gli altri.

In conclusione, avere tre router nella sottorete M, come descritto nell'esercizio, non solo ha senso ma è anche una pratica comune in ambienti di rete dove l'affidabilità, la performance, e la scalabilità sono priorità. Questo approccio permette una gestione più robusta e flessibile della rete.

3.5 alcune possibili configurazioni sul subnetting partendo da un piano di indirizzi di classe C (24 rete, 8 host)

- 1) **notazione CIDR /25**, possiamo configurare gli ip di 2 (2^1) sottoreti e 128 ip (2^7) per gli host;
- 2) **notazione CIDR /26**, possiamo configurare gli ip di 4 (2^2) sottoreti e 64 ip (2^6) per gli host;
- 3) **notazione CIDR /27**, possiamo configurare gli ip di 8 (2^3) sottoreti e 32 ip (2^5) per gli host;
- 4) **notazione CIDR /28**, possiamo configurare gli ip di 16 (2^4) sottoreti e 16 ip (2^4) per gli host;
- 5) **notazione CIDR /29**, possiamo configurare gli ip di 32 (2^5) sottoreti e 8 ip (2^3) per gli host;
- 6) **notazione CIDR /30**, possiamo configurare gli ip di 64 (2^6) sottoreti e 4 ip (2^2) per gli host;
- 7) **notazione CIDR /31**, possiamo configurare gli ip di 128 (2^7) sottoreti e 2 ip (2^1) per gli host;
- 8) **notazione cidr /24**, (con 24 bit dedicati alla rete è rappresentata una singola rete di classe C standard, senza suddivisione in sottoreti, quindi $2^0 = 1$), possiamo configurare l'ip di 1 (2^0) rete e 256 ip (2^8) per gli host;
- 9) **notazione cidr /23** (rispetto alla rete di classe C (/24) stiamo "prendendo in prestito" 1 bit dalla parte di rete) possiamo configurare l'ip di 2 (2^1) reti e 512 (2^9) per gli host;
- 10) **notazione cidr /22** (rispetto alla rete di classe C (/24) stiamo "prendendo in prestito" 2 bit dalla parte di rete) possiamo configurare l'ip di 4 (2^2) rete e 1.024 (2^{10}) per gli host;

4.1 Router e le tecniche di Routing

Il Router

Fondamenti di Routing

Il Default Gateway

Routing Statico

Routing Dinamico

Gli algoritmi di Dijkstra e di Bellman-Ford

Il RIP, OSPF e EIGRP

Cenni di Routing gerarchico, concetto di area id

4.2 Il Router

Un router è un dispositivo di rete che agisce come un nodo centrale per il trasferimento di dati tra reti diverse, permettendo la comunicazione tra dispositivi su reti separate, inclusa la connessione a Internet. Questi dispositivi sono responsabili dell'inoltro dei pacchetti di dati basati sugli indirizzi IP di destinazione, utilizzando tabelle di routing per determinare il percorso più efficiente. I router moderni offrono una vasta gamma di funzionalità oltre al semplice inoltro dei pacchetti. Tra queste, la [traduzione degli indirizzi di rete \(NAT\)](#) permette a più dispositivi di condividere un singolo indirizzo IP pubblico per accedere a Internet, migliorando la sicurezza e l'efficienza dell'uso degli indirizzi IP. Funzionalità di firewall forniscono protezione contro attacchi esterni, mentre il [supporto per il subnetting](#) consente una gestione più granulare degli indirizzi IP all'interno della rete. I router possono essere fisici, con hardware dedicato che include più interfacce di rete per collegare diverse reti, o virtuali, dove il routing è gestito da un software su hardware generico. La capacità dei router di aggiornare le tabelle di routing attraverso il [routing statico](#) o dinamico li rende essenziali per la scalabilità e la gestione delle reti moderne. Inoltre, i router possono eseguire funzioni avanzate come la qualità del servizio (QoS) per prioritizzare il traffico critico, il supporto per reti wireless (Wi-Fi), e l'implementazione di VPN per fornire connettività sicura tra siti remoti.

4.3 Fondamenti di Routing

Il routing è il meccanismo fondamentale per la navigazione dei pacchetti di dati attraverso una rete di nodi interconnessi. Alla base di questo processo ci sono le tabelle di routing, che contengono istruzioni dettagliate su come raggiungere diverse reti o sottoreti. Queste tabelle possono essere costruite in due modi: routing statico, dove le rotte sono configurate manualmente dall'amministratore di rete, e [routing dinamico](#), dove le rotte si adattano automaticamente ai cambiamenti della rete tramite protocolli di routing. Il routing si basa su [algoritmi per determinare il percorso più efficiente](#), considerando fattori come il numero di hop, la larghezza di banda, il costo del percorso o la latenza. La decisione su quale percorso prendere è determinata da [metriche che possono includere costi, hop count](#), o altre misure di distanza o qualità del collegamento. Comprendere i fondamenti del routing è cruciale non solo per la progettazione e la configurazione delle reti ma anche per la loro manutenzione e ottimizzazione, specialmente in ambienti complessi o in crescita. Questo implica la gestione del traffico, la risoluzione di problemi di connettività, l'implementazione di politiche di routing che bilanciano carico, sicurezza e performance, e l'uso di tecniche avanzate per migliorare l'affidabilità e l'efficienza delle comunicazioni di rete.

4.4 Il Default Gateway

Il [default gateway](#) rappresenta il punto di uscita predefinito per i pacchetti di dati che devono lasciare una rete locale per raggiungere destinazioni esterne. Questo concetto è fondamentale per la connettività Internet, permettendo ai dispositivi di inviare pacchetti verso indirizzi IP non presenti nella rete locale. Quando un dispositivo non trova una destinazione nella sua tabella di routing locale, inoltra il pacchetto al default gateway. Il router che agisce come default gateway utilizza quindi le sue tabelle di routing per determinare il percorso del pacchetto verso la destinazione finale, che potrebbe essere su Internet o su un'altra rete interna. Il default gateway è generalmente l'indirizzo IP del router più vicino alla rete locale, configurato su ogni dispositivo come parte delle impostazioni di rete. Questo setup consente ai dispositivi di non dover conoscere le complesse strutture delle reti globali per comunicare esternamente, facilitando la gestione della rete e migliorando l'esperienza utente. Configurare correttamente il default gateway è essenziale per garantire che il traffico di rete sia instradato correttamente, evitando problemi di connettività o perdita di pacchetti.

4.5 Routing Statico

Il routing statico implica la [configurazione manuale delle rotte](#) nella tabella di routing di un router. Questo metodo è utilizzato in ambienti dove la topologia della rete è stabile e prevedibile, o in reti piccole dove il traffico non cambia frequentemente. Ogni rotta è definita manualmente, specificando la destinazione e il prossimo hop verso quella destinazione. I vantaggi del routing statico includono la semplicità, la sicurezza (poiché non è suscettibile agli attacchi che potrebbero alterare le tabelle di routing dinamiche), e il controllo totale sulla gestione delle rotte. Tuttavia, il routing statico non si adatta automaticamente ai cambiamenti nella topologia della rete, come il guasto di un link, l'aggiunta di nuove reti o variazioni nel carico di rete, richiedendo intervento manuale per aggiornare le rotte. Questo può rendere il routing statico meno pratico per reti che richiedono alta disponibilità e ridondanza o che sono soggette a cambiamenti frequenti.

4.6 Routing Dinamico

Il routing dinamico permette ai router di adattarsi automaticamente e in tempo reale ai cambiamenti nella topologia della rete senza necessità di intervento umano. Questo è realizzato attraverso protocolli di routing che facilitano lo scambio di informazioni tra router, aggiornando dinamicamente le tabelle di routing. Protocolli come [RIP](#), [OSPF](#), [EIGRP](#) e [BGP](#) sono esempi di routing dinamico. Questo tipo di routing è particolarmente vantaggioso in reti complesse o in crescita, dove la topologia può variare frequentemente a causa dell'aggiunta o rimozione di reti, guasti ai collegamenti o variazioni nel carico di rete. Il routing dinamico offre vantaggi in termini di scalabilità, affidabilità (può reagire rapidamente a guasti della rete) e ottimizzazione del traffico secondo criteri come il costo minimo, la latenza o la larghezza di banda. Tuttavia, comporta un uso maggiore delle risorse di rete per lo scambio di informazioni di routing, e può essere più complesso da configurare e gestire, richiedendo una buona comprensione dei protocolli di routing e delle loro metriche per essere implementato efficacemente.

4.7 Algoritmo di Dijkstra

L'[algoritmo di Dijkstra](#), noto anche come algoritmo del percorso più breve, è utilizzato per trovare il percorso di costo minimo da un nodo sorgente a tutti gli altri nodi in una rete dove i pesi degli archi sono non negativi. È ampiamente implementato in protocolli di routing come OSPF per calcolare i percorsi di routing. L'algoritmo funziona in modo iterativo, selezionando il nodo non visitato con la distanza minore dal nodo iniziale e aggiornando le distanze degli altri nodi attraverso il nodo appena visitato. Questo processo continua fino a quando tutti i nodi sono stati considerati o si è trovato il percorso minimo verso una destinazione specifica. L'efficienza di Dijkstra risiede nel suo approccio che garantisce il percorso più breve a ogni nodo, rendendolo ideale per grafi non orientati con pesi positivi. Tuttavia, in grandi reti, l'algoritmo può diventare computazionalmente oneroso, motivo per cui spesso è utilizzato in combinazione con tecniche di ottimizzazione come il routing gerarchico per ridurre la complessità.

4.8 Algoritmo di Bellman-Ford

L'[algoritmo di Bellman-Ford](#) è un altro algoritmo di ricerca del percorso più breve che può funzionare anche in presenza di pesi negativi sugli archi, distinguendosi dall'algoritmo di Dijkstra che richiede pesi non negativi. Questo algoritmo è alla base di protocolli di routing come RIP. Funziona attraverso un processo di rilassamento degli archi, dove ogni arco viene esaminato per verificare se può fornire un percorso più breve al nodo di destinazione. Questo processo viene ripetuto per un numero di volte pari al numero di nodi meno uno, permettendo di trovare il percorso più breve anche in grafi con cicli di pesi negativi (a patto che non ci siano cicli di peso negativo totale). La capacità di gestire pesi negativi rende Bellman-Ford utile in scenari dove potrebbero esserci costi negativi, come in alcuni modelli di routing economico, ma la sua natura iterativa lo rende più lento rispetto a Dijkstra per grafi con pesi non negativi, specialmente in termini di complessità temporale.

4.9 Il RIP, OSPF e EIGRP

- 4.10.1 RIP (Routing Information Protocol) è uno dei protocolli di routing più vecchi, basato sull'algoritmo di Bellman-Ford. RIP utilizza il concetto di "hop count" come metrica per determinare il percorso più breve, con un limite massimo di 15 hop, il che lo rende adatto per reti piccole e semplici. Le sue versioni, RIP v1 e v2, offrono funzionalità di base come l'aggiornamento periodico delle tabelle di routing ma mancano di supporto per la subnetting variabile (VLSM) nella versione 1.
- 4.10.2 OSPF (Open Shortest Path First) è un protocollo di routing link-state che utilizza l'algoritmo di Dijkstra per calcolare i percorsi ottimali. OSPF è noto per la sua scalabilità, supportando suddivisioni della rete in aree per migliorare la gestione e la performance. Utilizza una metrica basata sul costo dei link, che può essere configurata in base a vari parametri di rete, permettendo un routing più intelligente e flessibile. OSPF supporta VLSM, routing basato su autenticazione e può essere esteso per supportare MPLS (Multiprotocol Label Switching).
- 4.10.3 EIGRP (Enhanced Interior Gateway Routing Protocol) è un protocollo proprietario di Cisco che combina elementi di distanza-vettore e link-state. EIGRP si distingue per la sua capacità di convergere rapidamente dopo un cambiamento nella topologia della rete grazie a meccanismi come DUAL (Diffusing Update Algorithm). Offre una metrica composita che include larghezza di banda, ritardo, affidabilità, carico e costo dei link, permettendo un routing più sofisticato e ottimizzato. EIGRP supporta VLSM, autenticazione del routing e può essere configurato per un routing basato su politiche complesse.

4.10 Cenni di Routing Gerarchico, Concetto di Area ID

Il routing gerarchico è una strategia per gestire la complessità delle grandi reti suddividendole in aree più piccole e gerarchicamente organizzate. Questo approccio riduce il numero di aggiornamenti di routing che ogni router deve gestire, migliorando la scalabilità e l'efficienza. OSPF utilizza il concetto di "area ID" per questa suddivisione, dove ogni area può avere

una propria topologia interna indipendente. La "[backbone area](#)" (area 0) funge da nucleo per la comunicazione tra le aree, permettendo un flusso efficiente delle informazioni di routing. Ogni area mantiene la propria base di dati di routing link-state, che riduce la complessità delle tabelle di routing globali e il carico computazionale sui router. Questo sistema non solo migliora la performance della rete ma anche la gestione, permettendo di isolare problemi a livello di area, ottimizzare il traffico su base locale e facilitare l'espansione della rete senza dover ricostruire completamente la topologia di routing. Il concetto di area ID in OSPF è quindi fondamentale per creare una rete più gestibile, resiliente e performante.

La gerarchia delle aree permette anche di [implementare politiche di routing locali](#), garantire la sicurezza attraverso l'[isolamento delle aree](#), e migliorare la stabilità riducendo la propagazione di aggiornamenti di routing inutili tra parti della rete che non hanno bisogno di conoscere i cambiamenti in altre aree.

5.1 Bibliografia:

- [1] https://it.wikipedia.org/wiki/Dispositivo_di_rete
- [2] <https://blog.hostingperte.it/differenza-switch-router-hub/>
- [3] <https://labs.warian.net/che-cose-un-bridge-di-rete/>
- [4] <https://it.wikipedia.org/wiki/Modem>
- [5] <https://it.wikipedia.org/wiki/Ripetitore>
- [6] https://telematics.poliba.it/images/file/boggia/retitlc/Standard802_retiLAN_14.pdf
- [7] <http://informatica.abaluth.com/reti/reti-locali/standard-ieee-802/>
- [8] Nuovo Sistemi e Reti Volume 1 - L.Lo Russo, E. Bianchi – HOEPLI
- [9] https://it.wikipedia.org/wiki/Scheda_di_rete
- [10] https://it.wikipedia.org/wiki/Indirizzo_IP
- [11] https://it.wikipedia.org/wiki/Indirizzo_MAC
- [12] [https://it.wikipedia.org/wiki/Interfaccia_\(informatica\)](https://it.wikipedia.org/wiki/Interfaccia_(informatica))
- [13] <https://www.tuttorreti.it/index.php/corsi/100-nozioni-sulle-reti-indirizzi-ip-e-classi-di-indirizzi-ip.html>
- [14] https://it.wikipedia.org/wiki/Maschera_di_sottorete
- [15] https://it.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
- [16] <https://it.wikipedia.org/wiki/Bluetooth>
- [17] <https://www.netspotapp.com/it/blog/all-about-wifi/what-is-wifi.html>
- [18] <https://it.wikipedia.org/wiki/Wireless>
- [19] https://it.wikipedia.org/wiki/Fibra_ottica
- [20] https://it.wikipedia.org/wiki/Gigabit_Ethernet
- [21] <https://www.ionos.it/digitalguide/server/know-how/ethernet/>
- [22] https://it.wikipedia.org/wiki/Rete_di_telecomunicazione_cellulare
- [23] https://it.wikipedia.org/wiki/Telecomunicazioni_satellitari
- [24] <https://www.centrostudihelios.it/la-connezione-alla-rete>
- [25] <https://www.tuttoandroid.net/approfondimenti/bluetooth-5-0-699004/>
- [26] https://en.wikipedia.org/wiki/Fast_Ethernet
- [27] https://en.wikipedia.org/wiki/Gigabit_Ethernet
- [28] <https://it.wikipedia.org/wiki/CSMA/CD>
- [29] [https://it.wikipedia.org/wiki/IEEE_802.11#802.11be_\(Wi-Fi_7\)](https://it.wikipedia.org/wiki/IEEE_802.11#802.11be_(Wi-Fi_7))
- [30] https://it.wikipedia.org/wiki/Access_point
- [31] https://it.wikipedia.org/wiki/Topologia_di_rete