1. Evoluzione e impatto sociale delle tecnologie di rete

1.1 Storia e evoluzione di Internet

1.1.1 Da ARPANET alla rete moderna

- **ARPANET (1969)**:
  - Primo nucleo di Internet, creato dall'agenzia ARPA (Advanced Research Projects Agency)
  - Inizialmente quattro nodi: UCLA, Stanford Research Institute, UC Santa Barbara, University of Utah
  - Scopo: condivisione di risorse di calcolo tra università
- **Sviluppi fondamentali**:
  - **1972**: Prima dimostrazione pubblica di ARPANET e introduzione dell'email
  - **1973**: Primi collegamenti internazionali (Regno Unito e Norvegia)
  - **1974**: Proposta del TCP/IP da parte di Cerf e Kahn
  - **1983**: Passaggio ufficiale da NCP a TCP/IP su ARPANET (considerato l'anno di nascita di Internet)
  - **1989**: Tim Berners-Lee propone il World Wide Web al CERN
  - **1991**: Prima pagina web pubblica
  - **1993**: Nascita di Mosaic, primo browser grafico di ampia diffusione
  - **1998**: Fondazione di Google
  - **2004**: Web 2.0 e nascita dei social network
- **Evoluzione della connettività**:
  - Da linee dedicate a commutazione di pacchetto
  - Evoluzione delle tecnologie di accesso: dial-up → ISDN → ADSL → fibra ottica
  - Introduzione delle reti mobili: 1G → 2G → 3G → 4G → 5G

1.1.2 Influenza dei protocolli sulla società digitale

- **TCP/IP e democratizzazione dell'accesso**:
  - Protocollo aperto e indipendente dall'hardware
  - Ha permesso l'interconnessione di reti eterogenee
  - Ha favorito l'adozione globale di Internet
- **HTTP e WWW**:
  - Ha trasformato Internet da strumento accademico a fenomeno di massa
  - Ha creato le basi per l'e-commerce e i servizi online
  - Ha cambiato il modo di accedere all'informazione
- **Protocolli di sicurezza (SSL/TLS, IPsec)**:

    - Hanno permesso lo sviluppo di servizi che richiedono confidenzialità:
        - Home banking
        - E-commerce
        - Comunicazioni sensibili
    - Hanno creato fiducia nell'uso della rete
- **DNS e struttura di Internet**:
    - Creazione di uno spazio dei nomi gerarchico
    - Centralizzazione vs decentralizzazione: il bilanciamento di Internet
    - Questioni di governance: ICANN e gestione globale

1.1.3 Implicazioni sociali dei cambiamenti tecnologici

- **Cambiamenti nella comunicazione**:
    - Da comunicazione asincrona (email) a comunicazione istantanea (chat, social media)
    - Evoluzione dei mezzi di comunicazione: testo → immagini → audio → video → realtà virtuale
    - Riduzione delle barriere geografiche
- **Globalizzazione dell'informazione**:
    - Accesso istantaneo a notizie globali
    - Disintermediazione delle fonti di informazione
    - Filter bubble e polarizzazione
- **Trasformazione del lavoro**:
    - Nascita del lavoro remoto e del telelavoro
    - Gig economy e piattaforme digitali
    - Automazione e impatto sull'occupazione
- **Cambiamenti economici**:
    - Nascita dell'e-commerce
    - Economia delle piattaforme
    - Disintermediazione in molti settori

1.2 Infrastrutture critiche di rete

1.2.1 Backbone di Internet e punti di scambio (IXP)

- **Backbone di Internet**:
    - Rete centrale ad alta velocità che connette reti regionali
    - Operatori Tier 1: possiedono reti globali e scambiano traffico senza costi (settlement-free peering)
    - Cavi sottomarini: trasportano oltre il 95% del traffico internazionale
    - Satelliti: copertura per aree remote e backup

- **Internet Exchange Point (IXP)**:
  - Infrastrutture fisiche dove diversi ISP si connettono per scambiare traffico
  - Vantaggi:
    - Riduzione dei costi di transito
    - Diminuzione della latenza
    - Maggiore resilienza della rete
  - Esempi: DE-CIX (Francoforte), LINX (Londra), MIX (Milano)
- **Autonomia e indipendenza delle reti**:
  - Concetto di Autonomous System (AS)
  - Sistemi di routing inter-AS: BGP (Border Gateway Protocol)
  - Implicazioni geopolitiche del controllo delle infrastrutture

1.2.2 Digital divide: aspetti tecnici e sociali

- **Definizione di digital divide**:
  - Disparità nell'accesso e nell'uso delle tecnologie digitali
  - Digital divide di primo livello: accesso fisico alle tecnologie
  - Digital divide di secondo livello: competenze e capacità di utilizzo
  - Digital divide di terzo livello: benefici ottenuti dall'uso
- **Cause tecniche**:
  - Costi infrastrutturali per aree remote o a bassa densità
  - Differenze tra connettività urbana e rurale
  - Limitazioni fisiche (montagne, mari, etc.)
  - Obsolescenza tecnologica in alcune aree
- **Fattori socio-economici**:
  - Costo dei dispositivi e delle connessioni
  - Disparità di reddito e di istruzione
  - Barriere linguistiche e culturali
  - Politiche pubbliche e investimenti
- **Strategie di mitigazione**:
  - Politiche di accesso universale
  - Tecnologie alternative (satellite, reti mesh)
  - Progetti come Internet.org, Starlink
  - Alfabetizzazione digitale e formazione

1.2.3 Internet come servizio essenziale: diritti e accesso

- **Internet come diritto fondamentale**:
  - Dichiarazione ONU del 2016: l'accesso a Internet come diritto umano
  - Paesi che hanno inserito l'accesso a Internet nella propria costituzione
  - Concetto di "servizio universale" applicato a Internet

- **Neutralità della rete (Net Neutrality)**:
  - Principio secondo cui tutto il traffico Internet deve essere trattato allo stesso modo
  - Dibattito sulla priorizzazione del traffico
  - Implicazioni per l'innovazione e la libertà di espressione
  - Legislazione in diverse aree geografiche (UE vs USA)
- **Impatto sociale della connettività**:
  - Accesso a servizi essenziali (sanità, istruzione, PA)
  - Partecipazione democratica e trasparenza
  - Opportunità economiche e lavorative
  - Inclusione sociale delle categorie svantaggiate
- **Sfide e problematiche**:
  - Censura e controllo governativo
  - Disconnessioni forzate in situazioni di crisi
  - Costi di accesso e affordability
  - Infrastrutture resilienti in caso di disastri

2. Sicurezza di base e privacy nelle reti

2.1 Fondamenti di sicurezza di rete

2.1.1 Principi di CIA (Confidenzialità, Integrità, Disponibilità)

- **Confidenzialità**:
  - Definizione: prevenire l'accesso non autorizzato alle informazioni
  - Tecniche: crittografia, controllo accessi, segmentazione delle reti
  - Sfide: gestione delle chiavi, bilanciamento tra sicurezza e usabilità
  - Esempi: VPN, HTTPS, crittografia end-to-end
- **Integrità**:
  - Definizione: garantire che i dati non siano alterati durante trasmissione o archiviazione
  - Tecniche: hash, firme digitali, checksum, controlli di ridondanza ciclica (CRC)
  - Sfide: rilevamento vs prevenzione delle manomissioni
  - Esempi: MD5, SHA, firme digitali nei certificati
- **Disponibilità**:
  - Definizione: assicurare che i sistemi e i dati siano accessibili quando necessario
  - Tecniche: ridondanza, backup, bilanciamento del carico, disaster recovery
  - Sfide: attacchi DDoS, single points of failure
  - Esempi: sistemi cluster, CDN, multi-homing
- **Altri principi complementari**:
  - **Autenticazione**: verifica dell'identità
  - **Autorizzazione**: definizione di privilegi e permessi

- **Non-ripudio**: impossibilità di negare azioni compiute
- **Controllo della privacy**: gestione delle informazioni personali

2.1.2 Vulnerabilità a livello 2, 3 e 4

- **Vulnerabilità a livello 2 (Data Link)**:
  - **ARP spoofing/poisoning**:
    - Manipolazione delle tabelle ARP
    - Permette attacchi Man-in-the-Middle in reti locali
    - Mitigazione: Inspection ARP, DHCP snooping
  - **MAC flooding**:
    - Saturazione delle tabelle CAM degli switch
    - Può portare lo switch a comportarsi come hub
    - Mitigazione: port security, limit MAC addresses
  - **Rogue DHCP**:
    - Server DHCP non autorizzato che fornisce configurazioni malevole
    - Può reindirizzare il traffico verso attaccanti
    - Mitigazione: DHCP snooping, autenticazione di rete
- **Vulnerabilità a livello 3 (Network)**:
  - **IP spoofing**:
    - Falsificazione dell'indirizzo IP sorgente
    - Utilizzato per attacchi DDoS o per aggirare filtri basati su IP
    - Mitigazione: ingress/egress filtering, RPF (Reverse Path Forwarding)
  - **ICMP attacks**:
    - Attacchi basati su ICMP (ping flood, smurf attack)
    - Possono causare DoS o rivelare informazioni sulla rete
    - Mitigazione: filtraggio ICMP, rate limiting
  - **Routing attacks**:
    - Manipolazione delle tabelle di routing
    - BGP hijacking, route poisoning
    - Mitigazione: RPKI, filtri sui prefissi BGP
- **Vulnerabilità a livello 4 (Transport)**:
  - **TCP SYN flood**:
    - Inondazione di richieste SYN senza completare l'handshake
    - Esaurisce le risorse del server
    - Mitigazione: SYN cookies, firewall stateful
  - **Session hijacking**:
    - Furto di sessioni TCP attive
    - Può permettere l'accesso non autorizzato a servizi
    - Mitigazione: cifratura, reset periodico delle sessioni

    - **UDP flood**:
        - Invio massivo di pacchetti UDP a porte diverse
        - Causa saturation dei servizi
        - Mitigazione: rate limiting, filtri sul traffico

2.1.3 Minacce comuni e contromisure base

- **Malware**:
    - **Tipi**: virus, worm, trojan, ransomware, spyware
    - **Vettori**: email, download, dispositivi USB, vulnerabilità
    - **Contromisure**: antivirus, patch regolari, sandbox, whitelisting
- **Attacchi di ingegneria sociale**:
    - **Phishing**: email o siti web fraudolenti che imitano entità legittime
    - **Pretexting**: creazione di scenari falsi per ottenere informazioni
    - **Baiting**: offrire qualcosa di allettante per indurre comportamenti rischiosi
    - **Contromisure**: formazione, verifica delle fonti, autenticazione multi-fattore
- **Denial of Service (DoS/DDoS)**:
    - **Volumetric**: sovraccarico della banda
    - **Protocol**: esaurimento delle risorse di rete
    - **Application**: attacchi mirati a servizi specifici
    - **Contromisure**: CDN, servizi anti-DDoS, filtri, ridondanza
- **Man-in-the-Middle (MitM)**:
    - Intercettazione delle comunicazioni tra due parti
    - Possibilità di visualizzare o alterare i dati scambiati
    - **Contromisure**: crittografia end-to-end, certificati, HSTS, pinning
- **Controllo degli accessi e autenticazione**:
    - Password sicure e gestione appropriata
    - Autenticazione multi-fattore (MFA)
    - Principio del privilegio minimo
    - Rotazione periodica delle credenziali

2.2 Privacy e anonimato nelle reti

2.2.1 Come i protocolli di rete possono rivelare informazioni personali

- **Indirizzo IP**:
    - Può rivelare posizione geografica approssimativa
    - Può essere collegato all'identità tramite i log ISP
    - Può essere tracciato attraverso diversi siti e servizi
- **DNS**:

    - Le query DNS rivelano i siti visitati
    - Spesso non criptate, permettendo la sorveglianza
    - Possono essere registrate dal provider DNS
- **HTTP e Header**:
    - User-Agent: rivela browser, sistema operativo, dispositivo
    - Referer: rivela la provenienza dell'utente
    - Cookie: permettono il tracciamento cross-site
- **Informazioni di livello 2**:
    - Indirizzo MAC: identificatore unico del dispositivo
    - Probe request Wi-Fi: rivelano SSIDs precedentemente connessi
    - Bluetooth: dispositivi in modalità discoverable
- **Metadati delle comunicazioni**:
    - Chi comunica con chi (graph analysis)
    - Quando e quanto spesso avvengono le comunicazioni
    - Volume dei dati scambiati

2.2.2 Tecniche di base per la protezione della privacy

- **VPN (Virtual Private Network)**:
    - Nasconde l'IP reale dell'utente agli siti visitati
    - Cifra il traffico verso il provider VPN
    - Limiti: il provider VPN può vedere il traffico non crittato
- **Proxy**:
    - Intermediario tra client e server
    - Diversi tipi: HTTP, SOCKS, web proxy
    - Vantaggi e svantaggi rispetto alle VPN
- **DNS over HTTPS (DoH) e DNS over TLS (DoT)**:
    - Cifratura delle query DNS
    - Protezione contro il monitoring dei siti visitati
    - Implementazioni: Firefox, Chrome, resolver pubblici
- **Navigazione anonima/incognito**:
    - Non salva cronologia, cookie, dati dei form
    - Non protegge da tracciamento IP o fingerprinting
    - Utile solo per privacy locale (stesso dispositivo)
- **Blocco dei tracker**:
    - Estensioni browser: uBlock Origin, Privacy Badger
    - Filtri a livello di rete: Pi-hole
    - Browser con protezione integrata: Firefox, Brave
- **Tor (The Onion Router)**:
    - Rete di relay che instradano il traffico attraverso nodi multipli

    - Cifratura a strati (come una cipolla)
    - Anonimato ma con compromessi di velocità

2.2.3 Bilanciamento tra sicurezza e privacy

- **Tensione intrinseca**:
    - Sicurezza spesso richiede identificazione e monitoring
    - Privacy richiede minimizzazione dei dati e anonimato
    - Trovare il punto di equilibrio adeguato al contesto
- **Privacy by Design**:
    - Incorporare la privacy fin dalla progettazione di sistemi e processi
    - Minimizzazione dei dati: raccogliere solo l'essenziale
    - Pseudonimizzazione vs. anonimizzazione
- **Proporzionalità delle misure**:
    - Valutazione dei rischi specifici
    - Misure adeguate allo scopo
    - Considerare l'impatto sui diritti fondamentali
- **Casi di studio**:
    - Tracciamento COVID-19: privacy vs. salute pubblica
    - Sorveglianza antiterrorismo vs. libertà civili
    - Sicurezza scolastica vs. privacy degli studenti
- **Approcci normativi**:
    - Consenso informato
    - Diritto alla cancellazione
    - Trasparenza e accountability
    - Valutazioni d'impatto sulla protezione dei dati

3. Applicazioni pratiche e casi d'uso

3.1 Reti domestiche e smart home

3.1.1 Architettura di una rete domestica moderna

- **Componenti principali**:
    - **Router/gateway**: connessione a Internet, NAT, DHCP, firewall
    - **Access point Wi-Fi**: copertura wireless, potenzialmente mesh
    - **Switch**: connessioni cablate ad alta velocità
    - **NAS (Network Attached Storage)**: archiviazione centralizzata
    - **Smart hub**: controllo dispositivi domotici (opzionale)
- **Topologia tipica**:
    - Router collegato al modem ISP

    - Zona demilitarizzata (DMZ) per servizi accessibili dall'esterno
    - Segmentazione in VLAN (rete principale, guest, IoT)
    - Cablaggio strutturato (ove possibile)
- **Tecnologie di connettività**:
    - **Cablata**: Ethernet (1/2.5/5/10 Gbps)
    - **Wireless**: Wi-Fi 5/6/6E (802.11ac/ax)
    - **Powerline**: comunicazione attraverso rete elettrica
    - **Tecnologie IoT**: Zigbee, Z-Wave, Bluetooth LE, Thread
- **Gestione e monitoraggio**:
    - Interfacce web di amministrazione
    - App mobili per controllo e diagnostica
    - Logging e alerting

3.1.2 IoT e interconnessione di dispositivi

- **Dispositivi smart comuni**:
    - **Entertainment**: smart TV, altoparlanti, streaming devices
    - **Controllo ambientale**: termostati, illuminazione, tende
    - **Sicurezza**: videocamere, serrature, sensori
    - **Elettrodomestici**: frigoriferi, lavatrici, robot aspirapolvere
    - **Assistenti vocali**: Amazon Echo, Google Home, Apple HomePod
- **Protocolli di comunicazione IoT**:
    - **Zigbee/Z-Wave**: basso consumo, mesh, per domotica
    - **Bluetooth LE**: comunicazione diretta a corto raggio
    - **Wi-Fi**: alta larghezza di banda, consumo elevato
    - **Thread/Matter**: standard emergenti per interoperabilità
    - **MQTT/CoAP**: protocolli leggeri per comunicazione device-to-cloud
- **Architetture IoT**:
    - **Cloud-centric**: dispositivi collegati principalmente al cloud
    - **Edge computing**: elaborazione locale dei dati
    - **Fog computing**: elaborazione distribuita tra edge e cloud
    - **Ibrida**: combinazione delle precedenti approcci
- **Interoperabilità**:
    - Sfide dell'ecosistema frammentato
    - Hub e bridge tra protocolli diversi
    - Standard emergenti (Matter, CHIP)
    - Piattaforme di integrazione (Home Assistant, SmartThings)

3.1.3 Problematiche di sicurezza e privacy nelle case connesse

- **Vulnerabilità comuni**:

    - Password di default o deboli
    - Mancanza di aggiornamenti di sicurezza
    - Comunicazioni non cifrate
    - Scarsa segmentazione di rete
    - Autenticazione insufficiente
- **Minacce principali**:
    - **Accesso non autorizzato**: controllo remoto dei dispositivi
    - **Botnet IoT**: dispositivi compromessi per attacchi DDoS (es. Mirai)
    - **Esfiltrazione dati**: raccolta non autorizzata di informazioni
    - **Violazione privacy**: microfoni/telecamere sempre attivi
    - **Impatto fisico**: controllo di serrature, termostati, allarmi
- **Strategie di mitigazione**:
    - **Segmentazione della rete**: VLAN dedicata per IoT
    - **Aggiornamenti regolari**: firmware e software
    - **Autenticazione forte**: password uniche, MFA ove possibile
    - **Monitoraggio traffico**: rilevare comportamenti anomali
    - **Dispositivi hub con sicurezza integrata**: Apple HomeKit, Google Nest
- **Considerazioni sulla privacy**:
    - Raccolta dati da parte dei produttori
    - Politiche di condivisione con terze parti
    - Conservazione e storage delle registrazioni
    - Diritto alla cancellazione dei dati personali
    - Trasparenza nell'elaborazione delle informazioni

3.2 Reti per servizi essenziali

3.2.1 Reti sanitarie e gestione dati sensibili

- **Tipologie di reti sanitarie**:
    - **HIS (Hospital Information System)**: gestione amministrativa
    - **PACS (Picture Archiving and Communication System)**: immagini mediche
    - **EMR/EHR (Electronic Medical/Health Record)**: cartelle cliniche
    - **Telemedicina**: visite remote, monitoraggio pazienti
    - **IoMT (Internet of Medical Things)**: dispositivi medici connessi
- **Requisiti specifici**:
    - **Alta disponibilità**: servizi critici 24/7
    - **Latenza garantita**: per applicazioni in tempo reale
    - **Sicurezza rafforzata**: protezione dati sanitari
    - **Interoperabilità**: standard come HL7, DICOM
    - **Conformità normativa**: GDPR, HIPAA, normative nazionali

- **Sfide di sicurezza**:
  - **Target privilegiato**: alto valore dei dati sanitari
  - **Legacy systems**: dispositivi datati difficili da proteggere
  - **Life-critical**: rischi potenzialmente letali
  - **Bilanciamento accesso emergenze vs. sicurezza**
  - **Insider threat**: accesso legittimo ma abusivo
- **Protezione dei dati sanitari**:
  - Crittografia a riposo e in transito
  - Controllo accessi basato sui ruoli (RBAC)
  - Audit trail completo
  - De-identificazione per scopi di ricerca
  - Backup sicuri e disaster recovery

3.2.2 Reti per istruzione e accesso equo

- **Infrastrutture educative**:
  - **Campus network**: copertura completa di istituti educativi
  - **E-learning platforms**: sistemi di gestione dell'apprendimento
  - **Educational resources network**: condivisione materiali didattici
  - **BYOD (Bring Your Own Device)**: integrazione dispositivi personali
  - **Research networks**: reti ad alte prestazioni per ricerca
- **Requisiti specifici**:
  - **Scalabilità**: gestire picchi di utenza
  - **Affidabilità**: supporto continuo all'attività didattica
  - **Flessibilità**: adattarsi a diverse modalità di insegnamento
  - **Sicurezza**: protezione dei minori e dati sensibili
  - **Bandwidth adeguata**: supporto a contenuti multimediali
- **Sfide dell'accesso equo**:
  - **Divario socioeconomico**: accesso a dispositivi e connettività
  - **Aree rurali vs urbane**: diverse disponibilità di infrastrutture
  - **Digital literacy**: competenze necessarie per l'utilizzo
  - **Accessibilità**: supporto a studenti con disabilità
  - **Multi-language**: supporto a diverse lingue e culture
- **Soluzioni innovative**:
  - **Connettività offline**: contenuti scaricabili per uso senza Internet
  - **Mobile learning**: ottimizzazione per dispositivi mobili più economici
  - **Educational ISP**: tariffe agevolate per scopi educativi
  - **Mesh networks**: copertura comunitaria a basso costo
  - **Open Educational Resources**: contenuti liberi e gratuiti

3.2.3 Reti per servizi pubblici

- **E-government e servizi digitali**:
  - **Portali di servizi al cittadino**: SPID, CIE, PagoPA
  - **Reti inter-istituzionali**: condivisione dati tra enti
  - **Open data**: accesso pubblico a dati non sensibili
  - **Sistemi di emergenza**: 112, protezione civile, alert pubblici
  - **Trasparenza amministrativa**: albo pretorio, amministrazione trasparente
- **Requisiti specifici**:
  - **Robustezza**: resistenza a guasti e attacchi
  - **Accessibilità universale**: usabile da tutti i cittadini
  - **Sicurezza certificata**: protezione da manomissioni
  - **Compliance normativa**: aderenza a leggi nazionali e sovranazionali
  - **Conservazione a norma**: archiviazione legale dei documenti
- **Infrastrutture critiche**:
  - **Reti elettriche smart grid**: gestione distribuzione energia
  - **Reti idriche**: monitoraggio e controllo
  - **Trasporti pubblici**: sistemi informativi, bigliettazione, traffico
  - **Telecomunicazioni pubbliche**: garantire comunicazioni essenziali
  - **Sistemi finanziari**: pagamenti, tesoreria pubblica
- **Resilienza e continuità operativa**:
  - Piani di disaster recovery
  - Sistemi ridondanti e geograficamente distribuiti
  - Esercitazioni periodiche
  - Coordinamento inter-agenzia
  - Comunicazione d'emergenza alternativa

4. Sostenibilità e reti

4.1 Impatto ambientale delle infrastrutture di rete

4.1.1 Consumo energetico di data center e reti

- **Dati sul consumo energetico**:
  - I data center rappresentano circa l'1-2% del consumo energetico globale
  - Una singola ricerca su Google produce 0,2-7g di CO_2
  - Il traffico Internet globale genera circa 1 miliardo di tonnellate di CO_2 all'anno
  - Crescita annuale del consumo: 10-15% (pre-ottimizzazione)
- **Componenti ad alto consumo**:
  - **Server**: elaborazione dati (CPU, RAM, storage)
  - **Sistemi di raffreddamento**: condizionamento, cooling

    - **UPS e power delivery**: conversione e distribuzione energia
    - **Networking equipment**: router, switch, transceiver ottici
    - **Storage systems**: dischi, array, sistemi di backup
- **Metriche di efficienza**:
    - **PUE (Power Usage Effectiveness)**: rapporto tra energia totale e energia IT
    - **WUE (Water Usage Effectiveness)**: consumo di acqua per raffreddamento
    - **CUE (Carbon Usage Effectiveness)**: emissioni di CO_2
    - **ERF (Energy Reuse Factor)**: energia riutilizzata (es. riscaldamento edifici)
- **Cause di inefficienza**:
    - Server sottoutilizzati (10-20% di utilizzo medio)
    - Raffreddamento eccessivo o inefficiente
    - Perdite nella distribuzione elettrica
    - Hardware obsoleto ed energivoro
    - Architetture non ottimizzate

4.1.2 Green networking: tecnologie e protocolli per ridurre il consumo

- **Efficienza hardware**:
    - **Processori a basso consumo**: ARM, design efficienti x86
    - **Raffreddamento liquido**: più efficiente dell'aria
    - **Virtualizzazione e consolidamento**: maggior utilizzo per server
    - **Componenti networking efficienti**: switch con sleep mode
    - **Sistemi di storage ottimizzati**: SSD vs HDD, tiering
- **Software e protocolli efficienti**:
    - **Energy-aware routing**: percorsi ottimizzati per efficienza
    - **SDN (Software-Defined Networking)**: gestione centralizzata e ottimizzata
    - **NFV (Network Function Virtualization)**: virtualizzazione di appliance fisiche
    - **Adaptive Link Rate**: adattamento velocità link al traffico
    - **Sleep modes**: spegnimento interfacce non utilizzate
- **Design dei data center**:
    - **Free cooling**: utilizzo aria esterna per raffreddamento
    - **Hot/cold aisle containment**: separazione flussi d'aria
    - **Localizzazione ottimale**: climi freddi, fonti rinnovabili
    - **Recupero calore**: riutilizzo per riscaldamento
    - **PV integration**: pannelli solari integrati
- **Energie rinnovabili**:
    - **On-site generation**: fotovoltaico, eolico in loco
    - **PPA (Power Purchase Agreement)**: acquisto diretto da rinnovabili
    - **Grid matching**: bilanciamento consumo con produzione rinnovabile

    - **Carbon offsetting**: compensazione emissioni
    - **24/7 carbon-free energy**: obiettivo di alcuni hyperscaler

4.1.3 E-waste: gestione sostenibile dell'hardware di rete

- **Dimensione del problema**:
    - 53,6 milioni di tonnellate di e-waste prodotte globalmente nel 2019
    - Solo il 17,4% riciclato correttamente
    - L'hardware di rete rappresenta circa il 10% dell'e-waste totale
    - Crescita annuale: 3-4% (più rapida di qualsiasi altro tipo di rifiuto)
- **Componenti critici**:
    - **Metalli rari e preziosi**: oro, argento, palladio, terre rare
    - **Materiali tossici**: piombo, mercurio, cadmio, ritardanti di fiamma bromurati
    - **Plastica**: spesso con additivi difficili da riciclare
    - **Batterie**: litio e altri materiali a rischio incendio/esplosione
    - **Componenti elettronici**: condensatori, circuiti integrati, cavi
- **Ciclo di vita dell'hardware di rete**:
    - **Durata media**: 3-5 anni per dispositivi consumer, 5-7 per enterprise
    - **Cause di obsolescenza**: nuovi standard, vulnerabilità di sicurezza, performance
    - **Second life**: riuso in mercati secondari o applicazioni meno esigenti
    - **Refurbishing**: ricondizionamento e aggiornamento
    - **Fine vita**: smaltimento o riciclo
- **Strategie di gestione sostenibile**:
    - **Progettazione ecocompatibile**: design modulare, riparabile, materiali sostenibili
    - **Estensione della vita utile**: aggiornamenti firmware, supporto a lungo termine
    - **Ritiro programmato**: programmi di buy-back e trade-in
    - **Riciclo certificato**: seguendo standard come R2 o e-Stewards
    - **Economia circolare**: recupero materiali per nuova produzione
- **Normative e certificazioni**:
    - **WEEE (UE)**: responsabilità del produttore per lo smaltimento
    - **RoHS**: restrizione sostanze pericolose nei dispositivi elettronici
    - **EPEAT**: valutazione dell'impatto ambientale dei prodotti
    - **Energy Star**: certificazione efficienza energetica
    - **TCO Certified**: standard completo di sostenibilità

4.2 Smart city e reti sostenibili

4.2.1 Ruolo delle reti nelle città intelligenti

- **Definizione di smart city**:
    - Ecosistema urbano che utilizza tecnologie digitali e dati per:

        - Migliorare l'efficienza dei servizi
        - Aumentare la sostenibilità
        - Migliorare la qualità della vita
        - Potenziare l'interazione e partecipazione cittadina
- **Infrastruttura di rete per smart city**:
    - **Rete di connettività urbana**: fibra ottica, 5G, Wi-Fi pubblico
    - **Reti di sensori**: monitoraggio ambientale, traffico, sicurezza
    - **Backbone municipale**: collega tutti i servizi cittadini
    - **Edge computing**: elaborazione locale per ridurre latenza
    - **Piattaforma di integrazione dati**: aggregazione e analisi
- **Componenti principali**:
    - **Smart governance**: processi decisionali data-driven
    - **Smart mobility**: trasporto pubblico connesso, traffico intelligente
    - **Smart environment**: gestione risorse, energia, rifiuti
    - **Smart living**: sicurezza, salute, qualità della vita
    - **Smart economy**: innovazione, imprenditorialità, produttività
- **Architettura tecnologica**:
    - **Sensing layer**: sensori IoT, dispositivi di raccolta dati
    - **Network layer**: connettività e trasmissione dati
    - **Data management layer**: storage, integrazione, analisi
    - **Application layer**: servizi e applicazioni per cittadini e amministrazione
    - **Security layer**: protezione trasversale a tutti i livelli

4.2.2 Monitoraggio ambientale tramite reti di sensori

- **Tipi di sensori ambientali**:
    - **Qualità dell'aria**: PM2.5, PM10, NO2, O3, CO, SO2
    - **Condizioni meteorologiche**: temperatura, umidità, pressione, vento
    - **Qualità dell'acqua**: pH, torbidità, contaminanti
    - **Rumore e inquinamento acustico**: decibel, pattern sonori
    - **Radiazioni UV e elettromagnetiche**: livelli di esposizione
- **Caratteristiche delle reti di sensori**:
    - **Wireless Sensor Network (WSN)**: nodi autonomi distribuiti
    - **Low-power protocols**: LoRaWAN, Sigfox, NB-IoT
    - **Mesh networking**: nodi che si auto-organizzano e ritrasmettono
    - **Energy harvesting**: auto-alimentazione tramite solare, vibrazione, etc.
    - **Edge intelligence**: pre-elaborazione dati in locale
- **Applicazioni pratiche**:
    - **Early warning**: allerta precoce per inquinamento o eventi meteorologici
    - **Urban planning**: dati per migliorare progettazione urbana

    - **Citizen awareness**: informazioni in tempo reale ai cittadini
    - **Policy evaluation**: misurazione impatto delle politiche ambientali
    - **Climate change adaptation**: monitoraggio effetti locali
- **Sfide e soluzioni**:
    - **Alimentazione**: batterie a lunga durata, energy harvesting
    - **Calibrazione**: mantenimento della precisione nel tempo
    - **Condizioni esterne**: resistenza a intemperie e vandalismo
    - **Copertura**: distribuzione ottimale dei sensori
    - **Big data**: gestione ed elaborazione di enormi quantità di dati

4.2.3 Mobilità connessa e riduzione dell'impatto ambientale

- **Smart transportation**:
    - **Intelligent Traffic Systems (ITS)**: semafori adattivi, gestione del traffico
    - **Public transit optimization**: monitoraggio flotte, info in tempo reale
    - **Connected vehicles**: V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure)
    - **Shared mobility**: bike/car sharing, ride hailing con ottimizzazione
    - **EV infrastructure**: stazioni di ricarica smart, grid integration
- **Vantaggi ambientali**:
    - **Riduzione congestione**: -15-20% di emissioni da traffico ottimizzato
    - **Fluidificazione traffico**: minor consumo da stop-and-go
    - **Route optimization**: percorsi più efficienti
    - **Modal shift**: incentivazione trasporto pubblico e mobilità dolce
    - **Logistics efficiency**: ottimizzazione consegne ultimo miglio
- **Tecnologie abilitanti**:
    - **GNSS ad alta precisione**: localizzazione centimetrica
    - **5G V2X**: comunicazione a bassa latenza veicolo-infrastruttura
    - **Edge computing**: elaborazione locale per decisioni in tempo reale
    - **AI/ML**: previsione traffico, ottimizzazione percorsi
    - **Digital twins**: simulazione scenari urbani per pianificazione
- **Case study: Smart parking**:
    - Riduce fino al 30% il traffico legato alla ricerca parcheggio
    - Sensori IoT per rilevamento posti disponibili
    - App per navigazione diretta verso posti liberi
    - Pricing dinamico basato su domanda
    - Integrazione con sistemi di pagamento e controllo

Conclusione

Lo studio del networking e del suo impatto sulla società digitale evidenzia come le tecnologie di rete abbiano profondamente trasformato non solo il modo in cui comunichiamo e

accediamo alle informazioni, ma anche l'intera organizzazione sociale, economica e politica.

La comprensione degli aspetti tecnici delle reti è fondamentale, ma altrettanto importante è l'analisi delle implicazioni che queste tecnologie hanno sulla privacy, sulla sicurezza, sull'equità dell'accesso e sulla sostenibilità ambientale.

In un mondo sempre più interconnesso, la consapevolezza delle opportunità e delle sfide poste dalle tecnologie di rete rappresenta un elemento essenziale di cittadinanza digitale consapevole. Le scelte tecnologiche che facciamo oggi, sia come individui che come società, plasmeranno l'ecosistema digitale di domani e il suo impatto sul pianeta.

La continua evoluzione delle reti richiederà professionisti non solo tecnicamente preparati, ma anche eticamente consapevoli, in grado di progettare e implementare soluzioni che bilancino efficienza, sicurezza, privacy e sostenibilità, contribuendo a un futuro digitale più inclusivo e responsabile.