Susanna Anelli | Paolo Macchi

GATEWAY

Sistemi e Reti

TERZA EDIZIONE

3

DEASCUOLA | Petrini

Accendi la conoscenza con HUB Scuola

Nuova, intuitiva, dinamica.
HUB Scuola è la piattaforma che accompagna docenti, studentesse e studenti nel loro percorso educativo. Sempre più ricca di risorse, lezioni e strumenti per una didattica digitale efficace e coinvolgente, è l'alleata ideale per le sfide di ogni giorno.

Tutta l'autorevolezza di **Mondadori Education**, **Rizzoli Education** e **Deascuola** in un solo ambiente digitale: HUB Scuola rappresenta la sinergia di tre grandi editori attenti alle esigenze di una scuola in continua evoluzione.

Esplora il **Sito libro, il luogo dove i tuoi libri prendono vita**. Qui puoi immergerti nella versione digitale dei volumi e scoprire tutti i materiali, le app e gli strumenti correlati.

Se sei docente, nelle **Aree Docenti** trovi l'ambiente perfetto per **personalizzare le lezioni** grazie a proposte, approfondimenti e strumenti specifici per ogni tua materia.

Anche la sezione **Test e Verifiche** è una **miniera di risorse**: gli studenti vi trovano materiali per esercitarsi, mentre i docenti possono attingere a vasti database e creare test per ogni materia e grado scolastico.

HUB Scuola ti offre i contenuti digitali dei tre editori, integrati in un'**unica piattaforma** e accessibili con un'**unica email e password**.
Entra in HUB Scuola!



Scopri di più
su HUB Scuola
inquadrando il QR code.

www.hubscuola.it

Scopri un mondo di risorse su misura per te





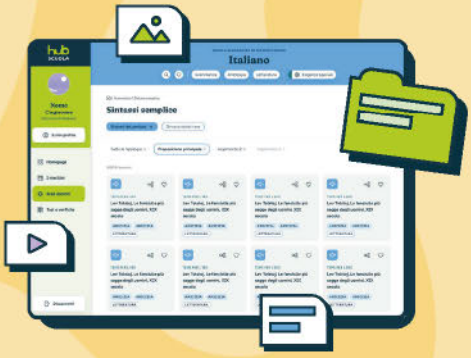


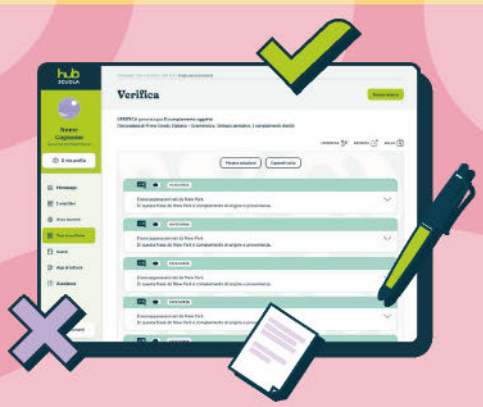
Sito libro

La versione digitale
del tuo libro cartaceo,
con tutti i contenuti extra.

Aree Docenti

Percorsi didattici e materiali
pronti all'uso per ogni materia
che insegni.

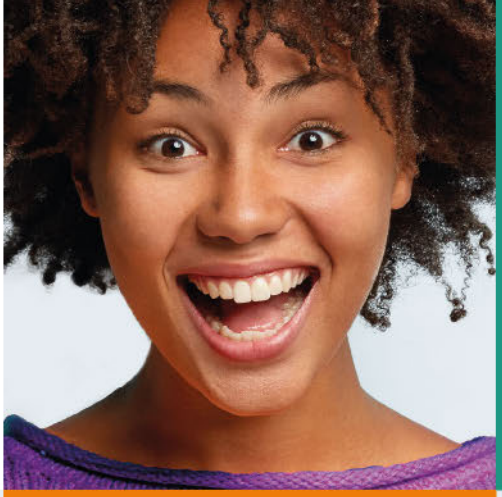




Test e Verifiche

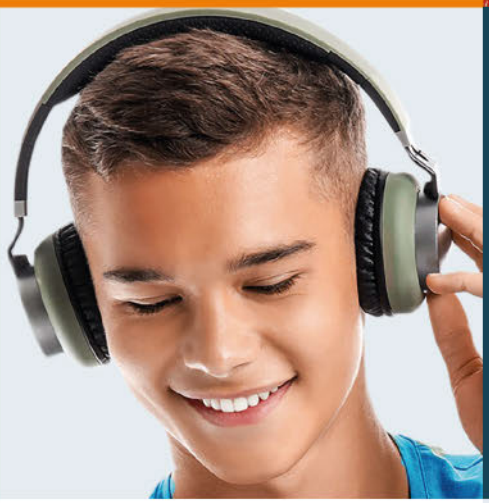
Un ampio database
di quesiti ed esercizi per creare
verifiche e allenarsi.

FUTURO IN CORSO











IL DOMANI INIZIA IN CLASSE





La scuola sta affrontando **nuove sfide**: l'ingresso dell'intelligenza artificiale, le novità nel campo dell'orientamento e dell'educazione civica, la crescente, e necessaria, attenzione verso inclusione e parità di genere.

In Deascuola lavoriamo ogni giorno per il **futuro** di studentesse e studenti, affiancando i docenti e le famiglie in questo momento di grande cambiamento.

Il nostro progetto **FUTURO IN CORSO** nasce per supportare chi insegna e chi studia, in questo momento di rapida trasformazione. Un **progetto** che riassume e integra tutti i valori di Deascuola per accompagnare ragazzi e ragazze verso un modo nuovo di abitare il mondo.

INCLUSIONE

L'istruzione deve essere alla portata di tutti. Ecco perché offriamo risorse e contenuti sempre accessibili, adeguati allo stile di apprendimento di ognuno, con i suoi bisogni e le sue specificità.

PARITÀ DI GENERE

Una scuola inclusiva valorizza le pari opportunità; per questo adottiamo un linguaggio attento a rappresentare la diversità/pluralità della società in cui viviamo.

EDUCAZIONE CIVICA

Le nuove generazioni devono saper affrontare le sfide globali. Per raggiungere questo obiettivo, proponiamo materiali che mettono al centro l'educazione ambientale, digitale, la cittadinanza attiva e il rispetto dei diritti umani.

ORIENTAMENTO

Guidare studentesse e studenti nella scoperta delle loro attitudini è essenziale per aiutarli a prendere decisioni consapevoli sul loro futuro scolastico e professionale. I nostri strumenti di orientamento sono utili per supportarli in questo importante percorso.

STEM

Le discipline STEM (Scienza, Tecnologia, Ingegneria e Matematica) rappresentano una chiave per comprendere il futuro. Nei nostri percorsi didattici, adottiamo un approccio interdisciplinare e pratico per avvicinare studentesse e studenti alle materie scientifiche e digitali.

INNOVAZIONE DIGITALE

Un mondo in continua evoluzione necessita di nuovi approcci didattici. Facciamo ricerca per offrire strumenti innovativi e rendere l'apprendimento più interattivo, coinvolgente ed efficace.

INTELLIGENZA ARTIFICIALE

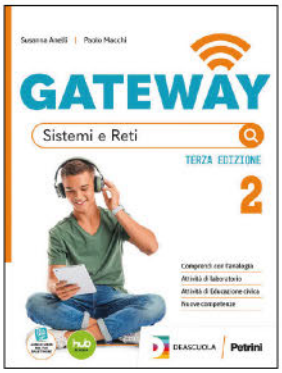
L'intelligenza artificiale arricchisce l'insegnamento, offrendo soluzioni capaci di adattarsi a ogni studentessa e a ogni studente. Supportiamo i docenti con soluzioni innovative per creare un percorso formativo più inclusivo e personalizzato.

Gateway: il percorso didattico

Benvenuto nel corso di Sistemi e Reti! Durante il corso di studi triennale, affronterai i seguenti temi.



- L'architettura e l'utilizzo dei sistemi di elaborazione
- Introduzione alle reti e l'accesso alla rete



- Le reti locali
- Il livello di rete
- La progettazione di reti
- Il livello di trasporto



- Il Web e i servizi Internet
- L'IoT
- La sicurezza di un sistema informatico
- Il Cloud computing

Il corso di *sistemi e reti* ruota intorno al concetto di sistema. Partendo dal semplice **sistema di elaborazione**, vengono trattati via via sistemi sempre più complessi, come i **sistemi di controllo**, fino ad arrivare alle reti informatiche e alla rete di reti, ossia Internet.
Il massimo grado di complessità, in questo contesto, è dato dall'Internt of Thing, un **ecosistema** costituito da oggetti, persone e dispositivi di varia natura. La catena dell'IoT inizia con l'acquisizione di dati dal mondo esterno, prosegue con la trasmissione dei dati tramite infrastruttura di rete, fino ad arrivare alla memorizzazione e all'analisi dei dati raccolti (big data) al fine di aumentare la conoscenza.

Nel **volume 1** vengono poste le basi per comprendere che cos'è un sistema con particolare riferimento ad un sistema di elaborazione secondo l'architettura di von Neumann.
Si inizia inoltre a studiare la catena dell'IoT, che utilizza sistemi di controllo che consentono l'interazione con la realtà e con gli oggetti che ci circondano. A questo punto si introducono l'architettura di rete secondo il modello TCP/IP per capire come è fatta Internet e come funziona. Nel volume 1 si analizzano i livelli più bassi del protocollo, più vicini alla parte fisica e all'hardware.

Il **volume 2** è incentrato sul funzionamento delle reti LAN e WAN e sull'infrastruttura necessaria per trasmettere messaggi tra reti diverse. Studiando questo volume imparerai quello che serve per capire come avviene la trasmissione dei dati in rete.

Il **volume 3** tratta argomenti collegati con le altre discipline di indirizzo.
Gli argomenti trattati sono spesso interdisciplinari con «Informatica» e «Tecnologie di progettazione di sistemi informatici e di telecomunicazioni», qualche volta anche con «Telecomunicazioni».
Partendo dallo studio del web e dei protocolli di livello applicazione, si completa la catena dell'IoT aggiungendo gli elementi di trasmissione dati e le applicazioni che li utilizzano. Particolare rilevanza viene data alla sicurezza di un sistema informatico, tema fondamentale, e anch'esso trasversale.

La rilevanza data all'IoT è anche dovuta al fatto che esso costituisce una delle fonti dei big data.
La tecnologia legata ai big data è stretamente connessa all'Intelligenza Artificiale.
Le attività a essa dedicate vogliono stimolare una riflessione critica sull'utilizzo di questo strumento, sulla scelta dei dati e sul ruolo degli algoritmi dell'AI.

Presentazione del corso

Com'è fatto il tuo libro?

Gateway Terza Edizione è il libro di testo che ti accompagnerà nello studio di Sistemi e Reti. Con Gateway potrai apprendere in modo guidato e graduale i concetti complessi e appartentemente astratti che caratterizzano questa materia, acquisendo la terminologia tecnica specialistica e le competenze (tecniche e trasversali) che ti serviranno negli studi successivi e nella futura professione.

Le spiegazioni teoriche utilizzano un linguaggio familiare, sono ricche di schemi e tabelle riassuntive e contengono molte immagini, che favoriscono un approccio visuale ai contenuti.

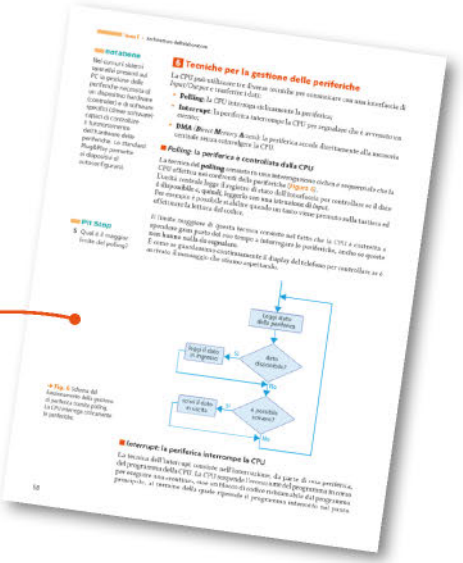
Il corso è organizzato in *Aree Tematiche*, ognuna delle quali è suddivisa in *Unità*. Ogni Area Tematica si apre con una pagina che contiene i prerequisiti necessari per affrontarne i contenuti e le principali conoscenze, abilità e competenze che acquisirai durante lo studio.

Guardiamo in dettaglio gli elementi caratteristici del libro.



Apertura di Unità

L'apertura di unità contiene una mappa e tre frasi introduttive, per orientarti tra gli argomenti che affronterai nell'Unità.



Trattazione teorica e rubriche

La trattazione teorica è schematica, arricchita con disegni e tabelle.

Numerose rubriche accompagneranno il tuo apprendimento.


Comprendi con l'analogia

Le architetture CISC e RISC possono essere comprese con i mattoncini delle costruzioni

Utilizzare un'architettura RISC è un po' come avere a disposizione solo i mattoncini fondamentali delle costruzioni. L'architettura CISC, invece, permette di avere anche pezzi di forme strane e diverse, le quali possono essere comunque ottenute combinando tra loro i pezzi base.

Nella rubrica **Comprendi con l'analogia** i concetti astratti e complessi vengono paragonati a situazioni e ad aspetti noti della realtà quotidiana, così da aiutarti a capirli più facilmente.


Pit Stop

3 Quali sono le componenti del case?

4 Come viene trasformata l'energia elettrica dall'alimentatore?


La parola a... Ada Byron Lovelace, la madre di tutti i programmatori

Ada Byron Lovelace (1815-1852) può essere considerata la «madre di tutti i programmatori». Fu lei che cento anni prima che il calcolatore fosse inventato ebbe l'intuizione che «rendere un meccanismo capace di combinare simboli generali, in sequenze illimitate per varietà ed estensione, vuol dire avere trovato un punto di unione fra le operazioni della materia e i processi astratti della mente». Ada prefigura una macchina che può rappresentare, oltre ai numeri, qualsiasi elemento simbolico della realtà, come testi e musica. Non solo. Ada immagina la capacità di apprendere delle macchine, anticipando le soluzioni di Intelligenza Artificiale e mostrandone i limiti: «la macchina analitica non ha alcuna pretesa di concepire alcunché», ma solo di eseguire i compiti che noi le assegniamo.

Man mano che procedi nello studio, le domande contenute nei **Pit stop** ti serviranno per verificare se hai compreso e ricordi quanto hai studiato.

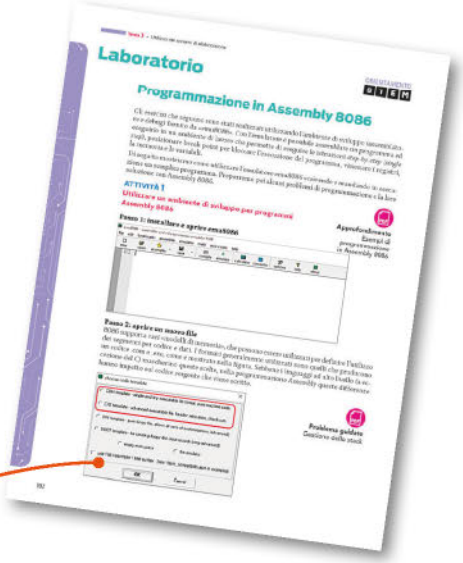
Le rubriche **Personaggi** e **La parola a...** ti fanno incontrare alcuni importanti protagonisti della disciplina, attraverso la loro storia e le loro parole.

Approfondimenti


Approfondimento - Tecnologia

L'evoluzione dei calcolatori: dalle valvole ai computer quantistici

Nelle pagine di **Approfondimento** verranno trattati argomenti specialistici.


Laboratorio

Programmazione in Assembly 8086

ATTIVITÀ 1

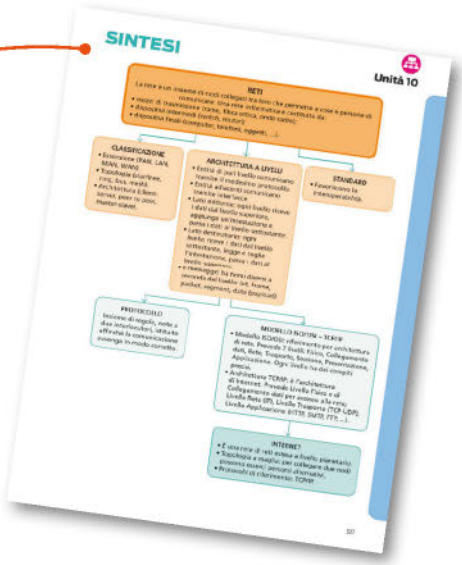
Utilizzare un ambiente di sviluppo per programmi Assembly 8086

Attività di laboratorio

Le **Attività di laboratorio** consentono di applicare immediatamente i concetti teorici, consolidando e ampliando le conoscenze attraverso la pratica. Ti metterai alla prova nel "lavoro sul campo" e svilupperai numerose competenze, anche al di là di quelle strettamente legate alla disciplina (come lavorare in gruppo e gestire consapevolmente il tempo).

Sintesi visuale

La mappa di apertura di Unità viene ripresa al termine della trattazione teorica per riassumere in uno sguardo i contenuti dell'Unità. Puoi utilizzare la **SINTESI** visuale durante lo studio e il ripasso.



Verifica delle conoscenze, Verifica delle abilità e CLIL English for Internetworking



Nelle pagine dedicate alla **Verifica delle CONOSCENZE** e alla **Verifica delle ABILITÀ** potrai verificare quanto hai appreso, rispondendo a domande a risposta multipla o vero/falso e domande aperte.

Le attività della pagina **CLIL English for Internetworking** consentono di acquisire il lessico tecnico in lingua inglese e di migliorare le tue abilità di reading, writing e listening.

Attività di fine tema



Al termine di ogni Area Tematica trovi attività per consolidare il tuo apprendimento. Gli esercizi **Verifica delle COMPETENZE** abbracciano i contenuti di tutte le Unità, anche trasversalmente, e ti consentiranno di ripassare i contenuti dell'Area Tematica.

Nelle interviste **Orientamento al lavoro** i grandi protagonisti della disciplina raccontano il loro lavoro e le sfide che devono affrontare.

La **Sfida finale** è un'attività con cui potrai metterti alla prova risolvendo un problema reale.

Educazione civica



Le attività di **Educazione civica** propongono un percorso di approfondimento, da svolgere individualmente e in gruppo, su temi di attualità.

Lavoriamo con l'Intelligenza Artificiale



Alla fine di ogni Area Tematica sono proposte attività per imparare a usare in modo consapevole i chatbot basati sull'**Intelligenza Artificiale**.

Risorse digitali

Nell'eBook del corso sono disponibili **mappe concettuali interattive**, **esercizi interattivi**, **esercizi in più**, **audio sintesi** in inglese, ulteriori **attività** ed **esercitazioni** di laboratorio, **approfondimenti**, **codici completi** pronti per essere eseguiti, **gallerie di immagini**, **video interviste** a professionisti del settore. Le sintesi audio e le video interviste sono fruibili anche attraverso l'**App DEALINK**.

Sommario

1 Il Web e i servizi Internet

Unità 1: Protocollo HTTP e Web 3

1 Introduzione 4
2 l livello applicazione 4
3 Architettura Client-Server 6
Comprendi con l'analogia Il client e il server sono come due attori che hanno parti diverse dello stesso copione di una recita 7
Comprendi con l'analogia Il server è in attesa della richiesta di un client come il demone della porta attende che qualcuno bussi 8
4 Il protocollo HTTP 8
5 Il Web 13

Approfondimento - Tecnologia 1
Versioni HTTP 20

Approfondimento - Tecnologia 2
API REST 22

Approfondimento - Storia dell'informatica
La nascita del Web 26

Laboratorio
ATTIVITÀ 1 Esplorare una richiesta HTTP con Google Chrome 28
ATTIVITÀ 2 Collegarsi a google.it con Putty sulla porta 80 30
ATTIVITÀ 3 Visualizzare il traffico http con Wireshark 31
ATTIVITÀ 4 Esplorare il protocollo QUIC con Wireshark 32
ATTIVITÀ 5 Interagire con le API REST di JSONPlaceholder 33

- **Sintesi** 36
- **Verifica delle conoscenze** 38
- **Verifica delle abilità** 39
- **CLIL – The HTTP protocol** 40

Risorse digitali - Unità 1

Mappa interattiva 37
Esercizi interattivi 38
Esercizi in più 39
Audio sintesi in inglese 40
Esercizi interattivi in inglese 40

Unità 2: Servizi Internet 41

1 Introduzione 42
2 DNS 42
3 La posta elettronica 53
Comprendi con l'analogia La posta elettronica come la posta ordinaria 54
4 Il protocollo FTP (File Transfer Protocol) 65
5 RTP: il protocolli delle videoconferenze 68

Approfondimento - Tecnologia 1 DNS e sicurezza 71

Approfondimento - Tecnologia 2
Sicurezza e utilizzo delle porte 72

Approfondimento - Tecnologia 3
Emoticon, smile ed emoji 75

Laboratorio
ATTIVITÀ 1 DNS: visualizzare i record DNS presenti nella cache del proprio computer 76
ATTIVITÀ 2 DNS: utilizzo del comando nslookup 77
ATTIVITÀ 3 DNS: risoluzione del nome di host tramite DNS 77
ATTIVITÀ 4 Posta elettronica: invio di un messaggio con STMP e lettura di un messaggio con POP3 utilizzando Packet Tracer 84
ATTIVITÀ 5 Posta elettronica: utilizzo dei comandi di POP da riga di comando 89
ATTIVITÀ 6 Posta elettronica: utilizzo dei comandi di ICMP da riga di comando 91
ATTIVITÀ 7 FTP: utilizzo dei comandi di FTP da riga di comando 92
ATTIVITÀ 8 FTP: utilizzo del protocollo FTP dall'interfaccia grafica di un client 93
ATTIVITÀ 9 Il protocollo SRTP con Wireshark 94

- **Sintesi** 96
- **Verifica delle conoscenze** 98
- **Verifica delle abilità** 99
- **CLIL – The HTTP protocol** 100

Risorse digitali - Unità 2

DNS con Wireshark 52
Mappa interattiva 97
Esercizi interattivi 98
Esercizi in più 99
Audio sintesi in inglese 100
Esercizi interattivi in inglese 100

Verifica delle competenze 101
Orientamento al lavoro Applicazioni Web 103
Sfida finale L'evoluzione di Internet 106
Lavoriamo con l'Intelligenza Artificiale
Interroghiamo l'Intelligenza Artificiale 109

2 Sicurezza di un sistema informatico

Unità 3: La sicurezza informatica 113

1 Introduzione 114
2 La cybersecurity 115
3 Il lato oscuro della cybersecurity 116
Comprendi con l'analogia Una vulnerabilità di un sistema è come il tallone di Achille: anche se è l'unico punto debole, può essere fatale 119
Comprendi con l'analogia Un exploit è come un ladro con un grimaldello che apre un lucchetto non sicuro 120
Comprendi con l'analogia Un malware è come un missile che trasporta una testata esplosiva 123
4 Le strategie dell'attacco informatico 126
Comprendi con l'analogia Virus biologici e informatici 126
Comprendi con l'analogia L'attacco malware di tipo "watering hole" è simile all'agguato di un predatore 129
5 La difficile arte della difesa informatica 130
Comprendi con l'analogia Gli honeypot per gli hacker sono come barattoli di miele per le api. 131
Comprendi con l'analogia Il modello NIST per gli attacchi informatici è come una strategia per difendersi dall'influenza 135
Comprendi con l'analogia Il primo livello di analisi del SOC (Security Operations Center) funziona come un triage ospedaliero 137
Approfondimento - Tecnologia
Le armi della guerra convenzionale vs "Cyber Warfare" 138
Laboratorio
ATTIVITÀ 1 Caso di studio: WannaCry 139
ATTIVITÀ 2 Caso di studio: LockBit 141
ATTIVITÀ 3 Caso di studio: un attacco APT 143
ATTIVITÀ 4 Caso di studio: matrice MITRE ATTACK 145
ATTIVITÀ 5 Scanner delle vulnerabilità: Nmap, Kali Linux e YARA 147
ATTIVITÀ 6 Convalida dell'input e SQL Injection 153
▪ **Sintesi** 154
▪ **Verifica delle conoscenze** 156
▪ **Verifica delle abilità** 157
▪ **CLIL — Computer system security** 158

Risorse digitali - Unità 3

Approfondimento: Cryptolocker 138
Attività: Convalida dell'input e SQL Injection 153
Mappa interattiva 155
Esercizi interattivi 156
Esercizi in più 157
Audio sintesi in inglese 158
Esercizi interattivi in inglese 158

Unità 4: Crittografia e autenticazione 159

1 Introduzione 160
2 La crittografia 160
3 L'autenticazione 166
4 La Firma Digitale 172
Comprendi con l'analogia Il passaporto rilasciato dal governo è come un token rilasciato da un provider d'identità 173
5 I certificati digitali 175
6 Le funzioni di hash 177
7 Server AAA 178
Comprendi con l'analogia AAA e carta di credito 178
Approfondimento - Storia
Da Giulio Cesare a Enigma 179
Approfondimento - Tecnologia 1
Tipi di firme elettroniche 181
Approfondimento - Tecnologia 2
La rivoluzione della blockchain 182
Approfondimento - Tecnologia 3
Crittografia quantistica 184
Laboratorio
ATTIVITÀ 1 Sicurezza sui router Cisco – Password enable 185
ATTIVITÀ 2 Sicurezza sui router Cisco – Protezione delle vie di accesso al router 188

ATTIVITÀ 3 Sicurezza sui router Cisco – Abilitare il protocollo SSH 190
ATTIVITÀ 4 Cifratura delle password su un database 192
- **Sintesi** 194
- **Verifica delle conoscenze** 196
- **Verifica delle abilità** 197
- **CLIL - Encryption and Authentication** 198

Risorse digitali - Unità 4

Approfondimento: Lo SPID 169
Approfondimento: Crittografia quantistica 184
Mappa interattiva 195
Esercizi interattivi 196
Esercizi in più 197
Audio sintesi in inglese 198
Esercizi interattivi in inglese 198

Unità 5: La sicurezza perimetrale

1 Introduzione 200
2 Proteggere la rete 200
Comprendi con l'analogia Il varco (il controllo degli accessi) 202
3 I firewall 202
Comprendi con l'analogia Il firewall e le ACL sono come il ponte levatoio di un castello medioevale 206
4 ACL 206
5 Proxy Server 214
Comprendi con l'analogia La "quarantena" di un file è come l'isolamento di un paziente durante un'epidemia 215
6 DMZ e Port forwarding 218
Approfondimento - Tecnologia
Intelligenza Artificiale e sicurezza 221
Laboratorio
ATTIVITÀ 1 Realizzare una DMZ impostando le ACL su un router di confine 222
ATTIVITÀ 2 Realizzare una DMZ con un firewall 224
- **Sintesi** 228
- **Verifica delle conoscenze** 230
- **Verifica delle abilità** 231
- **CLIL - Perimeter Security** 232

Risorse digitali - Unità 5

Mappa interattiva 229
Esercizi interattivi 230
Esercizi in più 231
Audio sintesi in inglese 232
Esercizi interattivi in inglese 232

Unità 6: VPN e protocolli sicuri

233
1 Introduzione 234
2 Cos'è una VPN 234
3 La classificazione delle VPN 235
Comprendi con l'analogia Lo studio di una VPN è come l'analisi degli stati di un gas 237
Comprendi con l'analogia Il Web è come un mare insidioso, pieno di risorse ma infestato da pirati 244
4 Sicurezza dei protocolli dal livello Rete al livello Applicazione 244
5 Internet Protocol Security (IPsec) 245
6 Transport Layer Security (TLS) 248
7 HTTPS – HyperText Transfer Protocol Secure 252
8 Conclusione 252
Approfondimento - Tecnologia 1
L'intestazione IPsec 254
Approfondimento - Tecnologia 2
PGP: posta elettronica sicura 255
Laboratorio
ATTIVITÀ 1 VPN Site-to-Site sicura 258
ATTIVITÀ 2 VPN Remote Access 264
ATTIVITÀ 3 Studio del protocollo HTTP all'interno di TLS 267
ATTIVITÀ 4 Utilizzo di una VPN 269
ATTIVITÀ 5 Applicazione di PGP 269
- **Sintesi** 270
- **Verifica delle conoscenze** 272
- **Verifica delle abilità** 273
- **CLIL - VPN and secure protocols** 274

Risorse digitali - Unità 6

Attività: Utilizzo di una VPN 269
Attività: Applicazione di PGP 269
Mappa interattiva 271
Esercizi interattivi 272
Esercizi in più 273
Audio sintesi in inglese 274
Esercizi interattivi in inglese 274

Unità 7: Le reti senza fili

1 Introduzione 276
2 Panoramica dei protocolli nelle reti senza fili 276
3 Wi-Fi e la sicurezza 278
4 WPA2 – Wi-Fi Protected Access II 279
5 WPA3 (Wi-Fi Protected Access III) 281
6 RFID e NFC 282
7 Bluetooth 284
8 ZigBee 285
9 WiMAX 288
10 LoRaWAN 289
11 MQTT 290
Comprendi con l'analogia La comunicazione tra insegnanti e studenti è analoga a quella tra gateway e nodi finali della rete LoRaWAN 291
12 Reti mobili 5G 293
Approfondimento - Tecnologia 1 L'attacco KRACK e il passaggio a WPA3 295
Approfondimento - Tecnologia 2 Il protocollo RADIUS 295
Approfondimento - Tecnologia 3 Indirizzi IP per sistemi mobili 296
Approfondimento - Salute L'esposizione delle persone ai campi elettromagnetici 297
Laboratorio
ATTIVITÀ 1 WLAN con WiFi e protocollo WPA2 Personal (PSK) 298
ATTIVITÀ 2 WLAN con WiFi e protocollo WPA2 Enterprise con WLC 300
▪ **Sintesi** 303
▪ **Verifica delle conoscenze** 304
▪ **Verifica delle abilità** 305
▪ **CLIL - Wireless networks** 306

Risorse digitali - Unità 7

Mappa interattiva 303
Esercizi interattivi 304
Esercizi in più 305
Audio sintesi in inglese 306
Esercizi interattivi in inglese 306

Verifica delle competenze 307
Orientamento al lavoro Sicurezza Informatica 309
Sfida finale Fiutare i pacchetti SSH con Wireshark 311
Lavoriamo con l'Intelligenza Artificiale Interroghiamo l'Intelligenza Artificiale 314

3 Cloud Computing e IoT

Unità 8: I data center

1 Introduzione 318
2 I data center 318
3 La Virtualizzazione 324
Comprendi con l'analogia Una cena tra amici e... i data center 331
4 Sicurezza e continuità operativa nei data center 332
Approfondimento - Tecnologia La storia delle virtualizzazioni: da VM/SP a VMware 337
Laboratorio
ATTIVITÀ 1 Introduzione alle Macchine Virtuali con Oracle VirtualBox 338
ATTIVITÀ 2 Creazione di un server per la virtualizzazione con Microsoft Hyper-V 340
▪ **Sintesi** 343
▪ **Verifica delle conoscenze** 344
▪ **Verifica delle abilità** 345
▪ **CLIL - Data center** 346

Risorse digitali - Unità 8

Approfondimento: Il Virtual Networking 328
Approfondimento: RAID 334
Approfondimento: La gestione della rete virtuale 337
Mappa interattiva 343
Esercizi interattivi 344
Esercizi in più 345
Audio sintesi in inglese 346
Esercizi interattivi in inglese 346

Unità 9: Il Cloud Computing

1 Introduzione: un viaggio nel tempo 348
2 Il Cloud Computing: dal "possesso" al "servizio" 348
3 Caratteristiche essenziali 349
4 Modelli di Servizio 349
Comprendi con l'analogia I Servizi di Cloud Computing (Tradizionale, IaaS, PaaS, SaaS) sono come le modalità di preparazione del caffè 350

5 Container e microservizi 352
Comprendi con l'analogia I container virtuali sono come i container fisici 353
6 Modelli di distribuzione 355
Approfondimento - Tecnologia 1
I container e la loro gestione automatizzata 357
Approfondimento - Tecnologia 2
Le pietre miliari del Cloud Computing 358
Laboratorio
ATTIVITÀ 1 Introduzione all'utilizzo della IBM Cloud Platform 359
ATTIVITÀ 2 IBM Cloud Platform: creazione di un programma in Java e sua esecuzione in Cloud 360
ATTIVITÀ 3 IBM Cloud Platform: Creazione di un cluster Kubernetes e deploy di un'applicazione containerizzata 364
ATTIVITÀ 4 IBM Cloud Platform: introduzione e utilizzo delle Function Serverless 365
ATTIVITÀ 5 IBM Cloud Platform: creazione di un'applicazione mobile (Android o iOS) per l'accesso a un Data Base in Cloud 365
ATTIVITÀ 6 Una Panoramica per un laboratorio scolastico virtuale con OpenStack 365
▪ **Sintesi** 366
▪ **Verifica delle conoscenze** 368
▪ **Verifica delle abilità** 369
▪ **CLIL - Cloud Computing** 370

Risorse digitali - Unità 9

Approfondimento: Modelli di sviluppo del codice in Cloud 359
Approfondimento: Ingegnerizzazione dell'App 360
Altre attività di Laboratorio 365
Mappa interattiva 367
Esercizi interattivi 368
Esercizi in più 369
Audio sintesi in inglese 370
Esercizi interattivi in inglese 370

Unità 10: IoT – Internet of Things

1 Introduzione 372
2 L'ecosistema IoT 372
3 Architettura di un sistema IoT 373
4 Campi di applicazione 375
Comprendi con l'analogia Un giorno di ordinaria follia digitale 377
5 La sicurezza dei sistemi IoT 377
Approfondimento - Tecnologia 1
Edge Computing e Fog Computing: due punti di vista 379
Approfondimento - Tecnologia 2
Intelligenza Artificiale: i modelli probabilistici 379
Approfondimento - Società
Dal transistor all'Intelligenza Artificiale 381
Laboratorio
ATTIVITÀ 1 Collegare simulazione e realtà: utilizzo delle API REST in un Ambiente IoT con Cisco Packet Tracer 383
ATTIVITÀ 2 Domotica con registration server 386
ATTIVITÀ 3 Domotica con home gateway 388
ATTIVITÀ 4 Utilizzo di Packet Tracer per programmare un MCU (Arduino) o un SBC (Raspberry) 391
▪ **Sintesi** 393
▪ **Verifica delle conoscenze** 394
▪ **Verifica delle abilità** 395
▪ **CLIL - Internet of Things** 396

Risorse digitali - Unità 10

Approfondimento: Algor-etica: per uno sviluppo umano della società digitale 380
Mappa interattiva 393
Esercizi interattivi 394
Esercizi in più 395
Audio sintesi in inglese 396
Esercizi interattivi in inglese 396

Verifica delle competenze 397
Orientamento al lavoro L'ecosistema IoT (Internet of Things) 399
Sfida finale XOLOMON – Monitoraggio del livello di un fiume a carattere torrentizio 401
Lavoriamo con l'Intelligenza Artificiale
Interroghiamo l'Intelligenza Artificiale 405
File Aggiuntivi: Codice completo pronto per l'esecuzione 404
Problemi svolti: Implementzione del codice Python 404

Educazione civica

La cyber war e la nostra vita 406
Le parole dei Social 409

Appendice

Guida allo svolgimento dell'esame di Stato 412
Prove d'esame
Esame di Stato luglio 2024 416
Esame di Stato luglio 2019 426
Esame di Stato luglio 2018 435
Simulazione ministeriale aprile 2019 442
Simulazione ministeriale febbraio 2019 452
Proposta di simulazione 461

Risorse digitali - Appendice

Approfondimento: Troubleshooting 425
Tema d'esame 2016 444
Svolgimento simulazione 462

Indice analitico

463

Legenda delle icone degli strumenti digitali

- Video
- Galleria di immagini
- Esercizi interattivi
- Approfondimento
  Esercizi in più
  Attività di laboratorio
  Problemi guidati
- Link a sito
- Sintesi audio (in inglese)
- Mappa concettuale interattiva

Ringraziamenti

Noi abbiamo scritto queste pagine, ma siamo stati solo il tramite dei molti che hanno contribuito alla realizzazione del libro. In particolare, studenti e colleghi con i quali abbiamo dibattuto e sperimentato. Siamo debitori al team che è stato nostro compagno di viaggio: i redattori Andrea De Porti, Francarturo Bertolotti, Vittoria Varesio, Stefano Parravicini e Paola Sardella, e il responsabile tecnico Gianni Cupelli, che ci hanno corretto, aiutato e sostenuto, dalla progettazione alla revisione dei testi. Ringraziamo Roberto Vanzetto, che a nome della casa editrice ci ha dato fiducia e non ci ha mai fatto mancare il suo incoraggiamento.

Un grazie particolare va a Dario Albé per la consulenza tecnica e a coloro che si sono prestati a rispondere alle interviste nelle pagine di "Orientamento al lavoro": Francesco Guastavino, Domenico La Fauci, Giancarlo Zicchieri, Giovanni Luca Favalli, Andrea Minigozzi, Paolo Bossi, Enthonj Franco. Il loro contributo è stato fondamentale per superare il difficile valico che separa la scuola dalla realtà aziendale.

Durante la stesura di queste pagine ci siamo trovati spesso a un bivio: affrontare un nuovo argomento o approfondire un'esercitazione? Speriamo di aver preso sempre la decisione migliore. Quello che è certo è che la scelta di andare a sinistra potrebbe invogliare qualcun altro ad andare a destra, o a esplorare una strada mai percorsa prima. Questo è il nostro augurio a studenti e docenti.

Susanna Anelli

Paolo Macchi

Petrini

Organizzazione D Scuola SpA con sistema di gestione Qualità UNI EN ISO 9001 certificato da Bureau Veritas Italia SpA.

internet: deascuola.it
e-mail: info@deascuola.it

Redattore responsabile: Andrea De Porti
Redazione e ricerca iconografica: Andrea De Porti, Paola Sardella
Redazione multimediale: Matteo Giacomelli
Tecnico responsabile: Giovanni Cupelli
Impaginazione e prestampa: Grande for Edit (MB)
Disegni: Andrea De Porti, Francesco Guaita
Progetto grafico: Matteo Rossi
Copertina: Matteo Rossi
Ricerca iconografica per la copertina: Alice Graziotin

Si ringraziano: Serena Aren per il contributo sulla Crittografia Quantistica; Paolo Benanti per le riflessioni sull'Intelligenza Artificiale; Ferdinando Gorga per la consulenza prestata sui casi di studio su IBM Cloud Platform; Francarturo Bertolotti per la collaborazione alla progettazione editoriale e alla revisione del testo; Paolo Bossi, Enthonj Franco e Andrea Minigozzi per le interviste nelle pagine di Orientamento al Lavoro.

Le fotografie di questo volume sono state fornite da: Adobe Stock, iStockphoto, Shutterstock.
Immagine in copertina: Shutterstock

DEALINK, DEAFLIX sono marchi concessi in licenza da De Agostini SpA.

L'editore dichiara la propria disponibilità a regolarizzare eventuali omissioni o errori di attribuzione. Nel rispetto del DL 74/92 sulla trasparenza nella pubblicità, le immagini escludono ogni e qualsiasi possibile intenzione o effetto promozionale verso i lettori. Tutti i diritti riservati. Nessuna parte del materiale protetto da questo copyright potrà essere riprodotta in alcuna forma senza l'autorizzazione scritta dell'Editore.
I testi ad alta leggibilità sono realizzati con il font TestMe ideato da Luciano Perondi e Leonardo Romei sulla base del Titillium, modificato secondo le specifiche D Scuola SpA. TestMe è un font «libero» per volontà degli autori, work in progress, basato sui principi del Design for All. È pensato come strumento per permettere di verificare alcune delle caratteristiche tipografiche rilevanti nel processo di lettura e per consentire di adattare il carattere a casi specifici.
I nostri testi sono disponibili in formato accessibile e possono essere richiesti a: Biblioteca per i Ciechi *Regina Margherita* di Monza (www.bibliotecaciechi.it) o Biblioteca digitale dell'Associazione Italiana Dislessia (www.aiditalia.org).

L'Editore promuove e tutela il diritto d'autore, riconoscendone il ruolo fondamentale nel sostenere la creatività e la libertà di espressione. L'Editore esprime la propria gratitudine per il rispetto delle normative sulla proprietà intellettuale dimostrato con l'acquisto di una copia autorizzata del presente volume. Qualsiasi utilizzo non autorizzato, inclusi quelli connessi a tecnologie di intelligenza artificiale o all'estrazione di testo e dati, costituisce una violazione dei diritti dell'editore e dell'autore, e comporta l'applicazione di sanzioni civili e penali secondo quanto previsto dalla Legge 633/1941 e successive integrazioni e modifiche.

Fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941 n. 633. Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana, 108 – 20122 Milano – e-mail: *autorizzazioni@clearedi.org* e sito web *www.clearedi.org*.
Eventuali segnalazioni di errori, refusi, richieste di chiarimento di funzionamento tecnico dei supporti multimediali o spiegazioni sulle scelte operate dagli autori e dalla Casa Editrice possono essere inviate all'indirizzo di posta elettronica *info@deascuola.it*.

Proprietà letteraria riservata
© 2025 D Scuola SpA – Milano
1ª edizione: gennaio 2025
Questo ebook contiene materiale protetto da copyright e non può essere copiato, riprodotto, trasferito, distribuito, noleggiato, licenziato, trasmesso in pubblico, o utilizzato in alcun altro modo ad eccezi-one di quanto è stato specificamente autorizzato dall'editore in base ai termini e alle condizioni alle quali è stato acquistato o di quanto esplicitamente previsto dalla legge applicabile. Qualsiasi utilizzo non autorizzato di questo testo, inclusi quelli connessi a tecnologie di intelligenza artificiale o all'estrazione di testo e dati, così come l'alterazione delle informazioni elettroniche sul regime dei diritti costituisce una violazione dei diritti dell'editore e dell'autore e comporta l'applicazione di sanzioni civili e penali secondo quanto previsto dalla Legge 633/1941 e successive integrazioni e modifiche. Gli ALT TEXT sono stati generati con l'ausilio di sistemi di intelligenza artificiale.
Questo ebook non potrà in alcun modo essere oggetto di scambio, commercio, prestito, sublicenza o altrimenti diffuso o messo a disposizione di terzi senza il preventivo consenso scritto dell'editore.

Tema 1

Il Web e i servizi Internet

Unità

1 Protocollo HTTP e Web
2 Servizi Internet

Prerequisiti

- Architettura di Internet
- Architettura Client/Server
- Protocollo IP
- Protocolli TCP/UDP

Conoscenze

- Il livello Applicazione in Internet
- Architettura Client/Server
- Il protocollo HTTP
- Il Web
- Il DNS
- Il sistema di posta elettronica
- Il protocollo FTP
- I protocolli per la videoconferenza

Abilità

- **Conoscere** l'architettura delle applicazioni di rete
- **Identificare** le caratteristiche di un servizio di rete
- **Identificare** una risorsa di rete
- **Comprendere** il sistema dei nomi di Internet
- **Comprendere** il funzionamento del World Wide Web
- **Utilizzare** l'interfaccia di comunicazione di applicazioni Client/Server
- **Utilizzare** la sintassi e i comandi dei protocolli Internet di livello Applicazione

Competenze

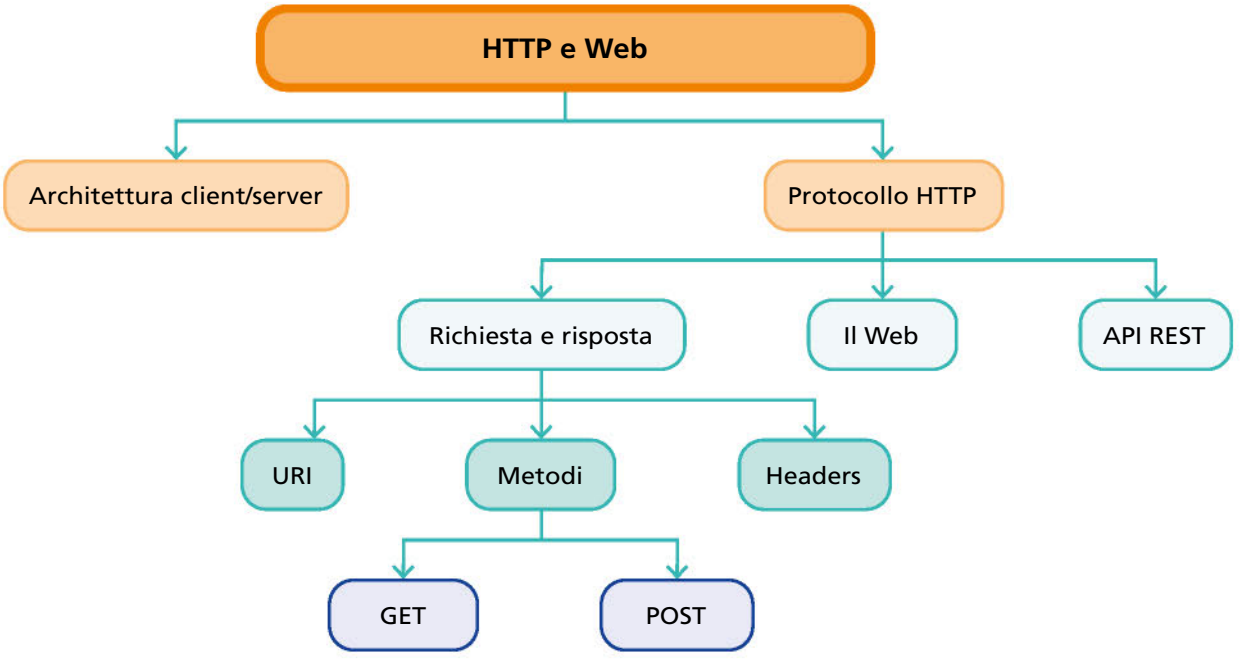
- **Configurare**, **installare** e **gestire** sistemi di elaborazione dati e reti
- **Utilizzare** i comandi dei protocolli di rete di livello applicazione con consapevolezza
- **Progettare** e realizzare una pagina web statica e dinamica
- **Progettare** un'applicazione Client/Server



Unità

1

Protocollo HTTP e Web



Visione d'insieme

- Architettura delle applicazioni di rete – architettura client/server.
- Il protocollo HTTP: richieste e risposta.
- Il Web.

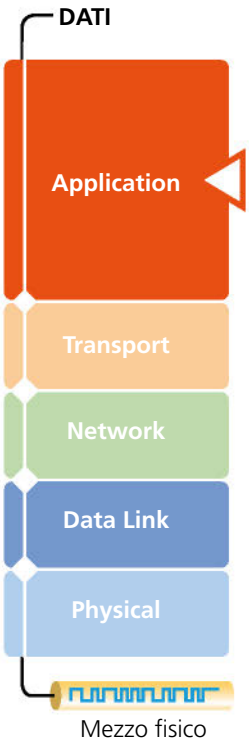
1 Introduzione

Nel 1989 Tim Berners-Lee, al CERN di Ginevra, con l'obiettivo di condividere informazioni scientifiche tra università e ricercatori, concepì il World Wide Web (WWW). Questa invenzione ha rivoluzionato le abitudini di miliardi di persone in tutto il mondo. La chiave del successo del Web risiede nella visione strategica del CERN e di Berners-Lee: anziché mantenere l'invenzione segreta, hanno reso tutto il software disponibile con licenza aperta.
Ma che cos'è e come funziona il Web? In questa unità, esploreremo i meccanismi alla base del WWW, partendo dal protocollo che lo sostiene. Internet, inizialmente solo un'infrastruttura di cavi e dispositivi, è diventata una rete auto-organizzata e complessa. Con l'avvento del Web, la rete è diventata un ambiente di comunicazione mondiale, decentralizzato e paritario.
Tuttavia la rapida crescita dell'Intelligenza Artificiale sta rivoluzionando molti settori, a partire dal Web. Insieme ai benefici, l'uso improprio di queste tecnologie può comportare dei rischi.
Come affrontare queste sfide e comprendere l'evoluzione tecnologica? Queste domande ci spingono a riflettere e, dove possibile, a cercare di fare luce sulle tecniche comunicative e sui protocolli utilizzati a livello applicazione.

2 Il livello applicazione

Il livello Applicazione (*Application Layer*), è il livello più alto del modello TCP/IP (Figura 1). Oltre a essere utilizzato per il Web, il livello applicazione è fondamentale per la comunicazione tra dispositivi connessi a Internet e fornisce le interfacce e i protocolli necessari alle applicazioni degli utenti.
È costituito da applicazioni distribuite, cioè applicazioni suddivise in due o più parti residenti su nodi diversi di Internet. Le applicazioni possono essere utilizzate dagli utenti o da altre applicazioni utente.
Lato mittente, un protocollo di livello applicazione genera un messaggio (*payload*) e lo passa al livello Trasporto (TCP o UDP) che aggiunge l'intestazione. Nell'intestazione di livello Trasporto sono presenti il numero di porta mittente (applicazione che ha generato il messaggio) e il numero di porta di destinazione (applicazione alla quale è destinato il messaggio.
Lato ricevente, il livello Trasporto legge l'intestazione, la rimuove e passa il payload all'applicazione identificata dal numero di porta di destinazione.
La Tabella 1 elenca i principali protocolli di livello applicazione di Internet.
I compiti del livello Applicazione sono:

- **fornire agli utenti un'interfaccia**. Per esempio, per utilizzare il Web si utilizzano pagine web scritte in HTML;
- **utilizzo di un linguaggio universale e regole di sintassi comuni** necessari per garantire l'interoperabilità tra sistemi diversi;
- **utilizzo della crittografia**. Il livello applicazione può utilizzare algoritmi di crittografia per codificare i dati trasmessi e garantire la riservatezza dei dati, rendendoli inaccessibili ai non autorizzati;
- **identificazione univoca delle risorse di rete**. Per esempio utilizzando il DNS;
- **controllo degli accessi e autenticazione degli utenti**. L'autenticazione permette solo agli utenti che ne hanno diritto di accedere alle proprie risorse. Ad esempio, nei protocolli di posta elettronica SMTP, POP3 e IMAP l'autenticazione è necessaria per accedere alle caselle di posta. Altri sistemi di autenticazione più sofisticata permettono agli utenti di accedere alle proprie risorse in modo sicuro.



↑ Fig. 1 Il livello Applicazione del modello TCP/IP corrisponde agli ultimi tre livelli del modello ISO/OSI: Sessione (5), Presentazione (6) e Applicazione (7).

Protocollo	Utilizzo	Protocollo di livello Trasporto	Porta standard
HTTP (HyperText Transfer Protocol)	Trasferimento di risorse (ad es. pagine web)	TCP	80 443 (con crittografia
HTTPs (HyperText Transfer Protocol Secure)	Versione sicura di HTTP	TCP	443
DNS (Domain Name System)	Risoluzione dei nomi in Internet. Traduce i nomi di dominio (come www.nasa.gov) nei corrispondenti indirizzi IPi	UDP	53
SMTP (Simple Mail Transfer Protocol)	Trasferimento di messaggi di posta elettronica	TCP	25 587 (con crittografia)
POP3 (Post Office Protocol)	Accesso alla propria casella di posta elettronica	TCP	110 995 (con crittografia)
IMAP (Internet Message Access Protocol)	Accesso alla propria casella di posta elettronica senza scaricare i messaggi in locale	TCP	143 993 (con crittografia)
FTP (File Transfer Protocol)	Accesso al file system da remoto. Trasferimento di file in modo affidabile	TCP	20 (per il trasferimento dei dati in modalità attiva). 21 (per il controllo della connessione).
TFTP (Trivial File Transfer Protocol)	Trasferimento file in modo non affidabile	UDP	69
Telnet (TErminaL NETwork)	Accesso a un computer remoto	TCP	23
SSH (Secure Shell)	Accesso a un computer remoto in modo sicuro	TCP	22
DHCP (Dynamic Host Configuration Protocol)	Assegnazione della configurazione di rete a un host in modo dinamico	UDP	67 per il server 68 per il client
IRC (Internet Relay Chat)	Messaggistica istantanea	TCP	6667

notabene

Il livello Applicazione combina le funzionalità dei livelli di Sessione, Presentazione e Applicazione del modello ISO/OSI.

← Tab. 1

Pit Stop

1 Quali sono i compiti del livello Applicazione?

I protocolli applicativi si basano sui protocolli del livello Trasporto. La scelta tra i protocolli TCP e UDP dipende dalla natura del servizio richiesto (**Figura 2**): TCP è preferibile quando l'affidabilità è prioritaria, UDP è la scelta ideale quando si privilegia la velocità.

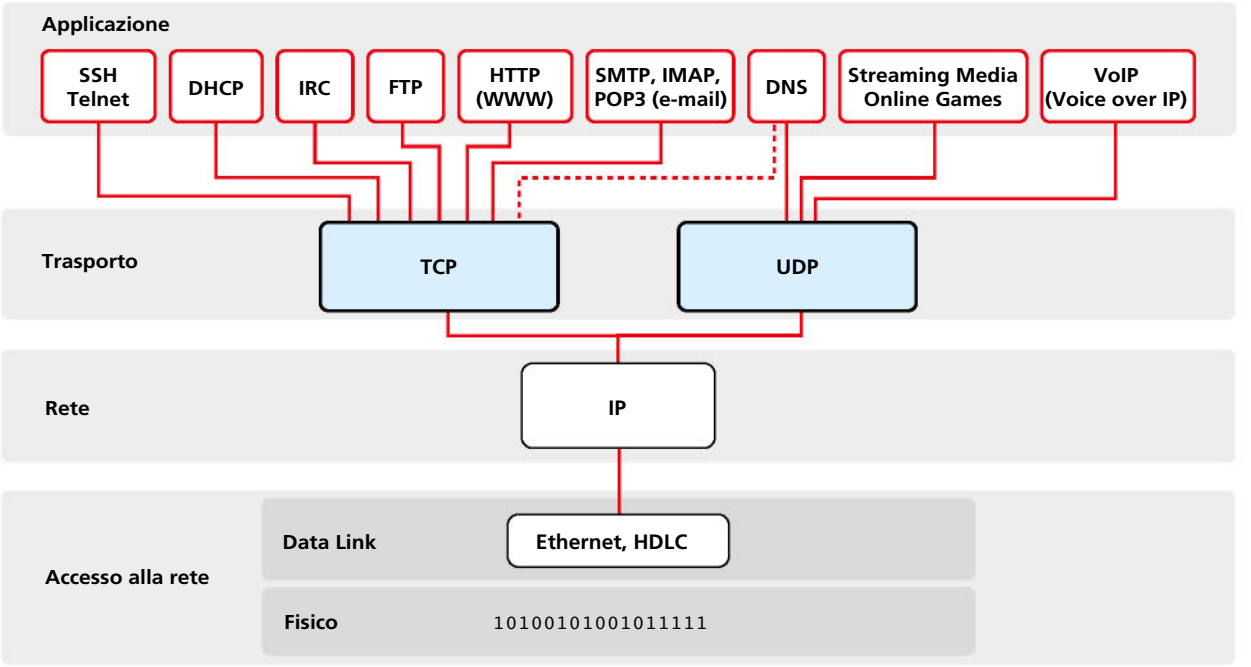


Fig. 2 I principali protocolli del livello Trasporto del modello TCP/IP e il loro collegamento con i protocolli dei livelli sottostanti. TCP offre un servizio orientato alla connessione, affidabile. UDP è senza connessione, più rapido, ma non garantisce l'affidabilità.

3 Architettura Client-Server

La maggior parte dei protocolli di livello Applicazione di Internet sono basati su una architettura client-server, in cui un'applicazione di rete è divisa in due moduli software: il client effettua una richiesta al server e il server invia una risposta al client.

Client e server indicano due ruoli assunti da due moduli software. Questi, in genere, sono residenti su due nodi diversi (con indirizzo IP diverso) della rete Internet, ma comunicano tra loro utilizzando il medesimo protocollo, come definito nel modello ISO/OSI secondo il quale entità di pari livello comunicano utilizzando lo stesso protocollo.

Il modulo client di livello Applicazione genera un messaggio utilizzando una determinata sintassi e delle regole note al modulo server. Il server riceve il messaggio e, utilizzando le medesime regole del client, lo interpreta per fornire una risposta al client. Queste regole costituiscono il protocollo.

Affinché la comunicazione tra client e server avvenga in modo corretto, il server deve essere in esecuzione in attesa che un client gli invii una richiesta. Si dice che il server è in attesa su una porta. Questo significa che un server è in attesa che un client gli invii un messaggio utilizzando il protocollo identificato da un determinato numero di porta. Per esempio, il server HTTP deve essere in attesa sulla porta 80, il server SMTP sulla porta 25, etc.

- il primo ad andare in esecuzione deve essere il server;
- il primo a mandare un messaggio (richiesta) è il client. A livello Trasporto, il processo associato al client farà partire il Three-Way Handshake per l'apertura della connessione TCP.

Comprendi con l'analogia

Il client e il server sono come due attori che hanno parti diverse dello stesso copione di una recita

Il copione è la conversazione nel suo insieme, ma ciascuno dei due attori, il client e il server, hanno una propria parte. Le due parti si integrano tra loro, in una conversazione intelligibile.

Al bar

Cliente: Buongiorno!
Barista: Buongiorno, desidera?
Cliente: Un caffè.
Barista: Un caffè come?
Cliente: Lungo e macchiato.
Barista: Ecco il caffè Può pagare alla cassa.
Cliente: Grazie, buona giornata.
Barista: Grazie a lei!

COPIONE DEL CLIENTE

Cliente: Buongiorno!
Cliente: Un caffè.
Cliente: Lungo e macchiato.
Cliente: Grazie, buona giornata.

COPIONE DEL BARISTA

Barista: Buongiorno, desidera?
Barista: Un caffè come?
Barista: Ecco il caffè Può pagare alla cassa.
Barista: Grazie a lei!

Client

C >
C >
C >

Server

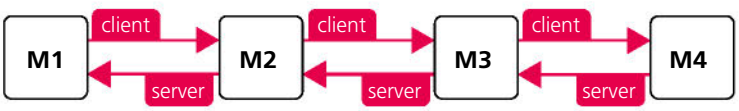
S >
S >
S >

Client/Server

C >
S >
C >
S >
C >
S >



Studiare i protocolli di livello Applicazione significa studiare le regole con cui il client e il server si scambiano i messaggi relativi a un determinato protocollo.
Per i protocolli standard, come HTTP, SMTP, ... le regole sono già predefinite. È però possibile scrivere delle applicazioni client-server proprie, definendo un protocollo e scrivendo il software lato client e il software lato server.
Il server è una sorta di interprete dei comandi. È molto importante sottolineare che in questo contesto client e server sono due moduli di una stessa applicazione, quindi si tratta di software! Sono dei processi identificati dall'indirizzo IP del dispositivo su cui sono in esecuzione e dal numero di porta (socket).
Se l'applicazione è costituita da soli due moduli, si parla di applicazione a due livelli. In realtà un'applicazione di rete è costituita da molti moduli. In questo caso si parla di **applicazione multilayer** e i vari moduli assumono il ruolo di client o di server a due a due (Figura 3).



← Fig. 3 Applicazione costituita da più moduli (multilayer): M1 è client rispetto a M2, che è server rispetto a M1. M2 è client rispetto a M3, che è server rispetto a M2, e così via.

Pit Stop

2 Che cosa significa studiare i protocolli di livello Applicazione?

notabene

Il concetto di API REST è illustrato negli Approfondimenti a fine Unità.

I vari moduli possono essere autonomi e indipendenti (**microservizi**) e composti tra loro per ottenere applicazioni più complesse. La comunicazione tra client e server di una applicazione multilayer può avvenire in vari modi. Uno dei più diffusi è l'uso di **API REST**, basate sul protocollo HTTP, che forniscono interfacce per la comunicazione tra applicazioni attraverso richieste e risposte HTTP. La composizione dei moduli può essere varia e i moduli, in genere, sono autonomi e residenti su nodi diversi della rete .

Comprendi con l'analogia

Il server è in attesa della richiesta di un client come il demone della porta attende che qualcuno bussi

La parola "demone" deriva dalla lingua greca e nelle religioni primitive rappresentava uno spirito benevolo in una posizione intermedia tra l'uomo e la divinità. Il demone software (*daemon*) è solitamente un programma che si attiva per eseguire delle azioni quando riceve un input. Un server web utilizza un demone HTTPd che invia i dati agli utenti quando questi si collegano. Un server, solitamente, prevede la possibilità di fornire più servizi su "porte" diverse, come la porta 80 o 8080, che sono riservate al servizio Web.



Metaforicamente il demone è un soggetto molto pigro: passa la maggior parte del tempo dormendo aggrappato alla porta che deve custodire. Quando qualcuno bussa, si sveglia all'istante e, il più velocemente possibile, risponde alla chiamata. Riceve dalla feritoia un foglio con le istruzioni da eseguire (ad esempio recuperare dall'archivio un certo documento, o un'immagine, o una foto), assegna al figlio la richiesta da evadere e si rimette a dormire aspettando che altri bussino.

I demoni vivono al medesimo indirizzo, in una grande casa comune. Ogni demone occupa una stanza contrassegnata con un numero e offre servizi diversi: nella stanza numero 80 risiede il demone della cucina, nella numero 23 c'è il demone del bagno, nella 21 quello della camera, e così via.

Una casa di demoni può possedere ben 65536 porte, di cui però le prime 1024 sono sempre riservate a servizi definiti e "ben noti" (80, 21, 23, …).

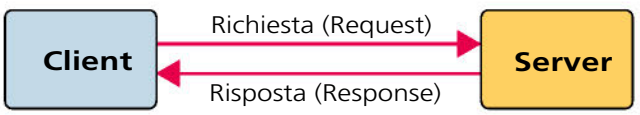
Oltre il numero 1023 si può configurare una stanza per un nuovo servizio (solarium, granaio, palestra…) e associarle un nuovo demone che la gestisca.

4 Il protocollo HTTP

Il protocollo **HTTP** (**H***ypertext* **T***ransfer* **P***rotocol*) è fondamentale per il funzionamento del web e di tutte le web application, compresi i social media. Ecco alcuni punti chiave relativi a HTTP:

- **Client/Server**. HTTP è un protocollo client/server. Quando visiti un sito Web, il browser agisce come un'applicazione client che si collega al server che ospita il sito, tramite Internet.
- **Porta 80**. HTTP lavora sulla porta 80. Questo significa che un server HTTP è in ascolto su quella porta, pronto a ricevere richieste dai client.
- **Scambio di Risorse**. Inizialmente, HTTP è stato progettato per trasferire pagine web (file HTML ipertestuali). Tuttavia, oggi è ampiamente utilizzato per lo scambio di risorse tra server e client. Una risorsa può essere un file, un'immagine o qualsiasi altra informazione.
- **URI**. Le risorse sono identificate da stringhe di indirizzo chiamate URI (Unified Resource Identifier). Ad esempio, l'URI per la homepage di Deascuola è "HTTPs://deascuola.it/"

- **Verbi o Metodi HTTP**. Le operazioni eseguibili su queste risorse sono definite verbi o metodi HTTP. Alcuni esempi includono:
  - `GET`: richiede una risorsa dal server;
  - `POST`: invia dati al server;
  - `PUT`: aggiorna una risorsa esistente;
  - `DELETE`: rimuove una risorsa dal server.
- **Flusso di Comunicazione** (Figura 4):
  - il server HTTP è in ascolto (listen) sulla porta 80 in attesa che un client HTTP invii una richiesta di connessione TCP (connect);
  - il client HTTP stabilisce una connessione TCP con il server HTTP;
  - il client invia una richiesta di risorsa al server (ad esempio, `GET /index.html HTTP/1.1`);
  - il server riceve la richiesta, analizza l'URI e restituisce una risposta (ad esempio, il contenuto della pagina index.html);
  - al termine la connessione TCP è chiusa.

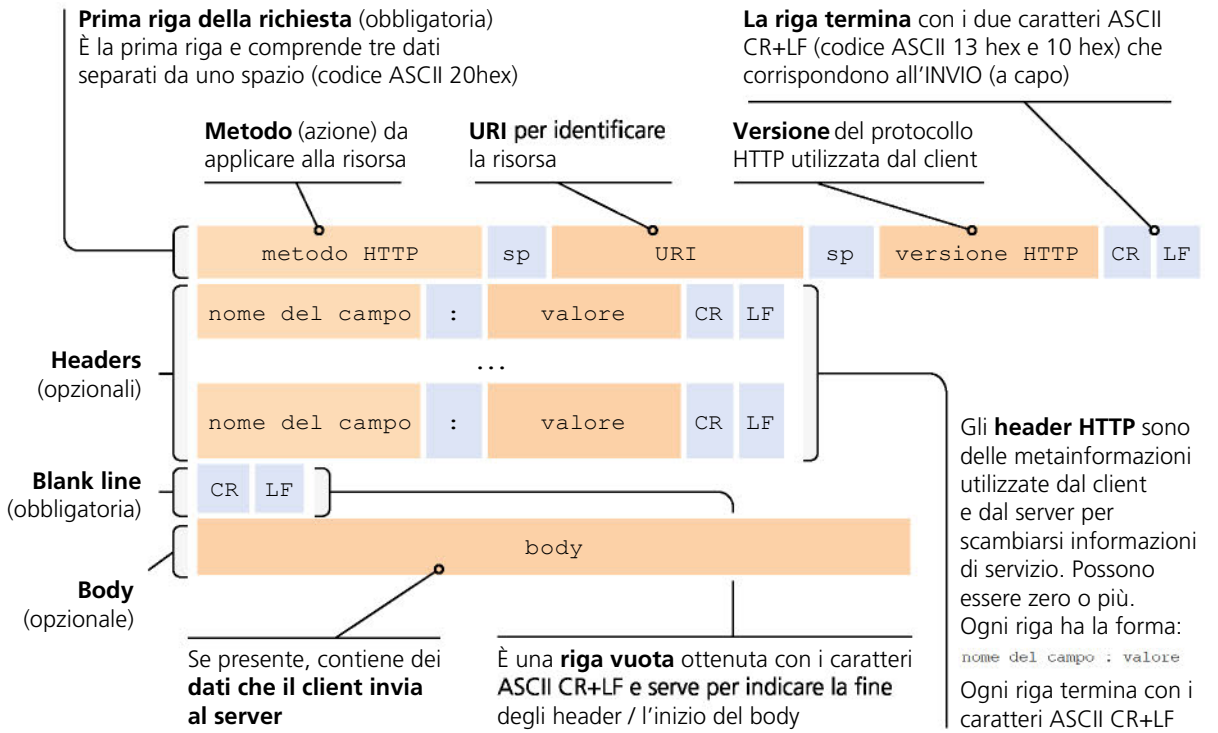


← **Fig. 4** Il client invia una richiesta al server, il server invia la risposta al client.

Il messaggio di richiesta (HTTP Request)

L'obiettivo di una richiesta HTTP è accedere a una "risorsa" identificata da una URI, presente su un server in Internet. HTTP non si cura della natura della risorsa, ma definisce semplicemente il modo per accedere a essa.
Un messaggio di richiesta HTTP è costituito da una stringa ASCII formata da 4 parti (alcune obbligatorie e altre opzionali) costruita con la sintassi descritta nella Figura 5.

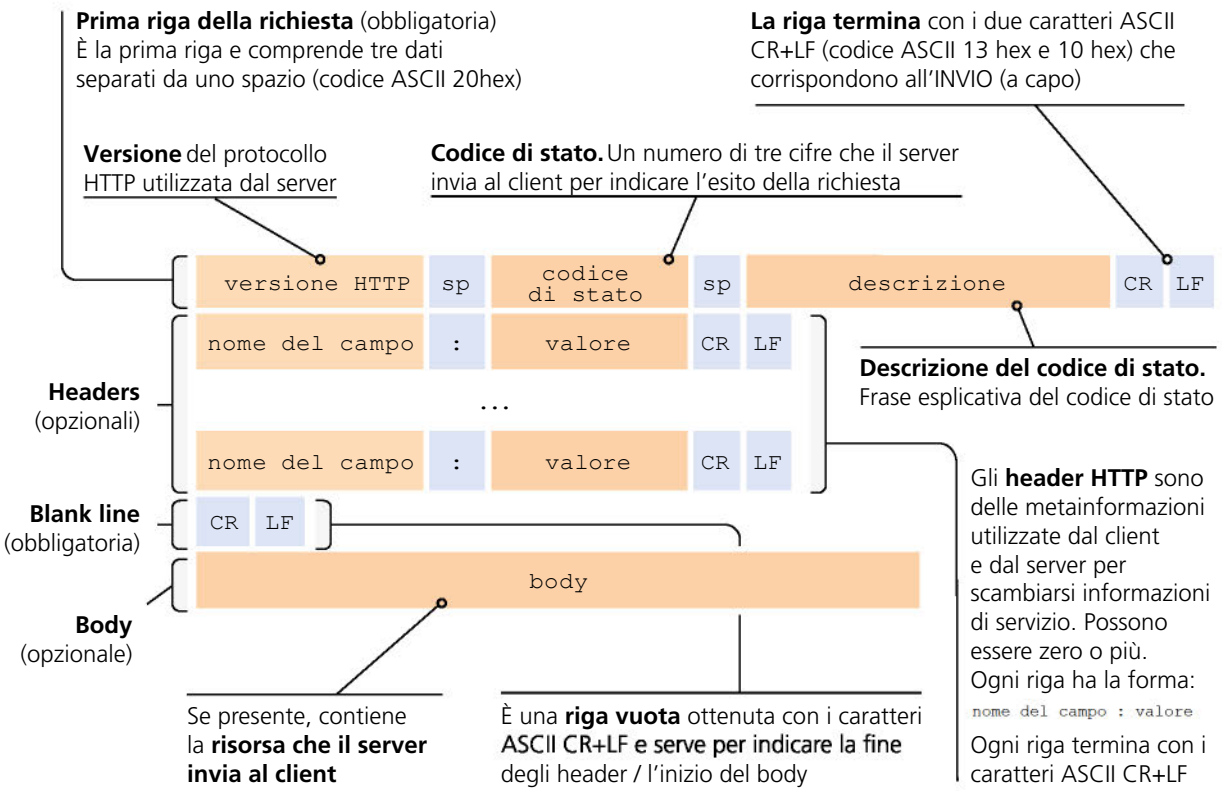
↓ **Fig. 5** Sintassi del messaggio di richiesta HTTP.



Il messaggio di risposta (HTTP response)

Un messaggio di risposta HTTP è costituito da una stringa ASCII, anch'essa formata di 4 parti (alcune obbligatorie, altre opzionali) e costruita con la sintassi descritta nella **Figura 6**.

Fig. 6 Sintassi del messaggio di risposta HTTP.



URI

Un **URI** (**U***niform* **R***esource* **I***dentifier*) è una stringa che identifica univocamente una risorsa in Internet.
La risorsa può essere qualsiasi cosa: un documento di testo, un file HTML, un'immagine o qualsiasi altro oggetto accessibile dalla rete.
L'URI è composta da tre parti principali:

```
protocollo://indirizzo internet/risorsa
```

dove:

- `protocollo` è il protocollo utilizzato dal client per richiedere la risorsa. Ad esempio, nel caso di una pagina web, lo schema potrebbe essere "HTTP" (per HTTP) o "HTTPs" (per HTTP sicuro);
- `indirizzo internet`. Questa parte dell'URI rappresenta l'indirizzo IP o il nome dell'host a cui inviare la richiesta. Opzionalmente comprende anche la porta. Ad esempio in `http://www.esempio.com:80/index.html`, `www.esempio.com:80` è l'indirizzo Internet e `80` è la porta;
- `risorsa` è un percorso organizzato in una struttura ad albero che consente di raggiungere la risorsa. Ad esempio `index.html` è la risorsa specifica.

Esempio 1

`http://www.ricettario.it/torte/tortadimele.html`

è un URI utilizzato da un client HTTP per richiedere un file HTML. In esso:

- HTTP è il protocollo utilizzato da client e server
- `www.ricettario.it` è il nome dell'host su cui il server è in esecuzione. Può essere sostituito dall'indirizzo IP. Di default il server HTTP è in ascolto sulla porta 80. Diversamente occorre specificare, dopo il nome dell'host, il numero di porta. Per esempio `www.ricettario.it:81`
- `torta/tortadimele.html` è il nome del file richiesto comprensivo di path.

Il file `tortadimele.html` è nella cartella `torte` sull'host `www.ricettario.it` .

notabene

Il nome dell'host sarà tradotto dal DNS nel corrispondente indirizzo IP, che insieme al numero di porta costituisce il socket per l'accesso al server.

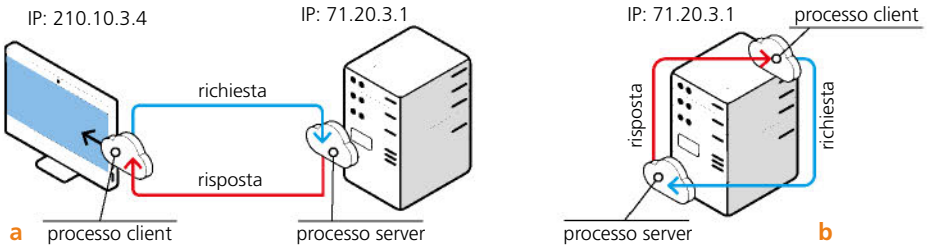
Esempio 2

`http://www.miosito.it/utenti/123` per accedere all'utente 123

notabene

Nel Web il protocollo HTTP è utilizzato per la richiesta di un file HTML, ma in generale l'URI specifica come accedere a una risorsa. L'azione da fare è specificata nel metodo.

È importante notare che, quando si parla di client e server, ci si riferisce a software o hardware a seconda dei contesti. In un'architettura client/server è un processo client che fa una richiesta a un processo server. Client e server possono essere in esecuzione su macchine diverse (Figura 7a), ma anche sulla stessa macchina (Figura 7b).



← Fig. 7 Client e server in esecuzione su macchine diverse (a.) o sulla stessa macchina (b.).

Metodi HTTP

I metodi HTTP specificano le azioni che il client intende fare rispetto alla risorsa specificata tramite l'URI. Nella Tabella 2 riportiamo i principali.

↓ Tab. 2 Principali metodi HTTP.

Metodo	Richiesta del client	Risposta del server
GET	Il client richiede al server la risorsa identificata tramite l'URI.	Il server invia la risorsa nel body della risposta.
POST	Il client invia al server i dati presenti nel body della richiesta. Potrebbero essere una nuova risorsa o dei parametri.	Il server invia al client la risorsa creata o il file HTML generato in base ai parametri ricevuti.
PATCH	Il client chiede l'aggiornamento della risorsa con la sostituzione di quella esistente. Nel body sono passati i dati da modificare.	Il server invia al client la risorsa aggiornata.
PUT	Il client chiede l'aggiornamento parziale di una risorsa. Nel body sono passati i dati da modificare.	Il server invia al client la risorsa aggiornata.
DELETE	Il client chiede l'eliminazione della risorsa specificata nell'URI.	Il body della risposta è vuoto.

Pit Stop

3 Quali sono le principali caratteristiche del protocollo HTTP?

Codice di stato

La risposta del server contiene un codice di stato per comunicare l'esito della richiesta. Questo codice è un numero di tre cifre e ha il seguente significato:

- **2xx**: La richiesta è stata eseguita con successo. Ad esempio, il codice 200 OK indica che tutto è andato bene e la risorsa richiesta è stata restituita correttamente.
- **3xx**: ridirezione. Ad esempio, il codice 301 Moved Permanently indica che la risorsa è stata spostata in modo permanente in un'altra posizione.
- **4xx**: la richiesta non può essere soddisfatta per un errore nella richiesta del client. Ad esempio, il codice 404 Not Found indica che la risorsa richiesta non è presente sul server.
- **5xx**: la richiesta non può essere soddisfatta per un problema del server. Ad esempio, il codice 500 Internal Server Error indica un errore interno del server.

La Tabella 3 riassume i principali codici di stato.

Tab. 3 I principali codici di stato.

Codice di stato	Descrizione	Note
200	Document Follows	La richiesta è stata eseguita con successo, il server invia la risorsa nel body.
301	Moved Permanently	Il documento è stato spostato.
401	Unauthorized	Non è possibile accedere senza autenticazione.
402	Payment Required	Tariffa da pagare.
403	Forbidden	Accesso vietato.
404	Not Found	La risorsa richiesta non è stata trovata. Si verifica, in genere, se c'è un errore nell'URI oppure la risorsa è stata rimossa.
502	Bad Gateway	
503	Service Unavailable	Servizio non disponibile.

La Figura 8 mostra il messaggio di risposta a una richiesta HTTP andata a buon fine; in Figura 9 si vede la risposta a una richiesta HTTP non andata a buon fine.

```
GET / HTTP/1.1

HTTP/1.1 200 OK
Date: Sun, 07 Apr 2024 18:05:21 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-sr
c 'nonce-1KePgopAlqcEwDwaCKONsg' 'strict-dynamic' 'report-sample' 'unsafe-eval'
'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
-hp
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: AEC=AQTF6HwkJYb7dGzLWU1WhhiabnhM2e78Wl5ebo8gSaoAg3Y42iUmClpeR1I; exp
ires=Fri, 04-Oct-2024 18:05:21 GMT; path=/; domain=.google.com; Secure; HttpOnly
; SameSite=lax
Accept-Ranges: none
Vary: Accept-Encoding
Transfer-Encoding: chunked

49b5
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="it"
><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta
content="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop=
"image"><title>Google</title><script nonce="1KePgopAlqcEwDwaCKONsg">(function(){
```

Fig. 8 Richiesta HTTP andata a buon fine.

```
HTTP/1.0 400 Bad request
Cache-Control: no-cache
Connection: close
Content-Type: text/html

<html><body><h1>400 Bad request</h1>
                                Your browser sent an invalid request.
                                                                    </body>
</html>
```

Fig. 9 Richiesta HTTP non andata a buon fine.

Headers HTTP

Le intestazioni HTTP sono meta-informazioni che il client e il server si scambiano durante la comunicazione. Queste intestazioni forniscono dettagli aggiuntivi sulla richiesta o sulla risposta HTTP. La Tabella 4 mostra alcuni dei principali tipi di intestazioni:

Tab. 4 Le principali intestazioni HTTP.

Nome campo	Descrizione	Esempio
Accept	Content-Types accettati	Accept: text/plain
Accept-Charset	Set di caratteri accettati	Accept-Charset: UTF-8
Accept-Encoding	Codifica accettata	Accept-Encoding: gzip, deflate
Connection	Tipo di connessione preferita dal client	Connection: keep-alive
Content-Length	Lunghezza del campo "body" (in byte)	Content-Length: 1234
Content-Type	Il tipo MIME usato nel campo body (tipicamente in una POST)	Content-Type: text/html; charset=ISO8859-1 Content-Type: application/json
Date	Data di invio del messaggio	Date: Tue, 01 Dec 2024 09:15:00 GMT
Host	Il nome del server	Host: www.google.it
User-Agent	Il nome del browser che invia la richiesta	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:12.0) Gecko/20100101 Firefox/12.0
Authorization	Utilizzata per autenticare il client presso il server	Authorization: Basic cGNlcm5hbWU6xFazc3dvcm=Q
Cookie	Trasmette i cookie dal client al server	Cookie: c1_cookie=red; c2_cookie=yellow

5 Il Web

Verso la fine degli anni Ottanta del secolo scorso, Internet era limitata agli ambienti scientifici universitari e a piccoli gruppi di appassionati sparsi per il mondo. Mancavano ancora strumenti facili che permettessero alla maggior parte delle persone di entrare in rete e scambiarsi informazioni. L'unico strumento sufficientemente versatile era la posta elettronica, giunta fino a noi con poche modifiche.

Nel 1990, le cose cambiarono improvvisamente. Tim Berners-Lee, ricercatore presso il CERN di Ginevra, propose un progetto per utilizzare Internet allo scopo di condividere, in modo semplice e rapido, le informazioni con gli altri ricercatori sparsi sul pianeta. I testi si trasformarono in "ipertesti", scritti nel linguaggio HTML che divenne la lingua franca di Internet, trasmessi con il protocollo HTTP. Così nacque il World Wide Web, la cui diffusione esplosiva avrà effetti allora inimmaginabili.

notabene

Si veda l'Approfondimento "La nascita del WWW" alla fine di questa Unità.

La parola a... Tim Berners-Lee e il Web



In un'intervista («The World Wide Web Turns 30 Today. Here's How Its Inventor Thinks We Can Fix It») rilasciata alla rivista "Time" nel 2019, nel trentennale della nascita del Web, Tim Berners-Lee, parlando del futuro della rete Internet, ha sollevato il problema della diffusione di disinformazione e della violazione della privacy.

«Ho una visione per un mondo alternativo, in cui i dati esistono, ma sono a completa disposizione dell'utente. Dove le app sono effettivamente separate dalla fonte dei dati. Quando usi un'app, ti viene chiesto dove memorizzare i dati. In questo modo hai il controllo completo su chi ha accesso a essi. [...] Penso che la regolamentazione della privacy possa essere molto importante. [...] Fin dall'inizio sapevamo che se si trattava di una tecnologia potente, che sarebbe stata utilizzata nel bene e nel male, come tutte le altre tecnologie. Ma inizialmente sentivamo, filosoficamente, che il Web dovesse essere un mezzo neutrale. [...] Questa era la nostra speranza. [...] All'improvviso ci siamo resi conto che dobbiamo assicurarci che il Web sia al servizio dell'umanità. Non solo mantenendolo libero e aperto, ma assicurandoci che le cose costruite dalle persone in questo spazio "senza permessi" aiutino effettivamente la democrazia.»

Web Founder Tim Berners-Lee on the Future of the Internet | TIME

notabene

La richiesta HTTP potrebbe partire anche da CLI. Il vantaggio di utilizzare un browser è che si dispone di una interfaccia utente. Il browser, inoltre, è in grado di interpretare il codice HTML e visualizzare la pagina ricevuta.

Come funziona il Web: la richiesta di una pagina web

Il funzionamento del Web è basato sul protocollo HTTP in cui la risorsa richiesta dal client è un file HTML (**Figura 10**) e la risorsa inviata dal server tramite il body della risposta è il codice HTML della pagina richiesta.
In questo contesto l'URI assume la forma di **URL** (**U***niform* **R***esource* **L***ocator*) ed è utilizzato per identificare il file richiesto.
Il client può essere un qualsiasi browser, come per esempio Google Chrome, Microsoft Edge, Mozilla Firefox, Safari.
Il server coinvolto è un server HTTP, come per esempio Apache HTTP Server (sviluppato dalla Apache Software Foundation) o Internet Information Services (IIS, sviluppato da Microsoft).

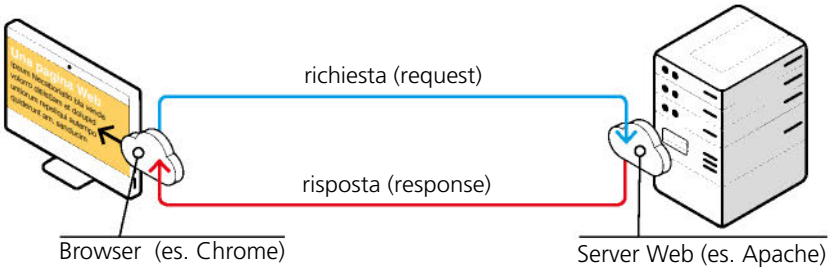


Fig. 10 Il client HTTP effettua la richiesta HTTP al server web.

Per quanto riguarda il file richiesto dal client, a meno di eventuali errori, si possono verificare due casi:

- Il file HTML è già presente nella memoria del server. In questo caso il server non fa altro che recuperarlo e inviarlo al client, che lo visualizza sul monitor dell'utente. Il file HTML rappresenta una **pagina web statica**. Il codice HTML è scritto e salvato in un file (**Figura 11**).

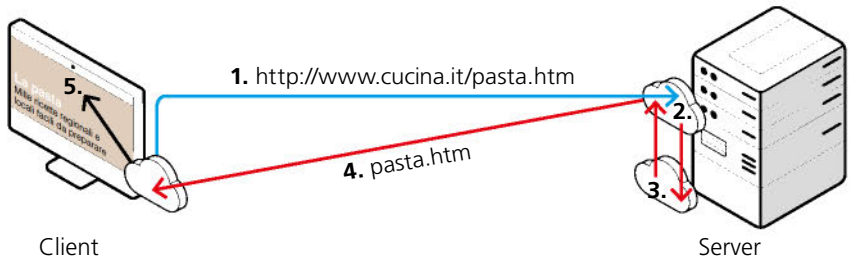


Fig. 11 Richiesta di una pagina Web statica. **1.** Il client effettua richiesta di una pagina HTML (chiede il codice HTML del file pasta.htm). **2.** Il server accede alla memoria. **3.** Legge il file. **4.** Invia la pagina. **5.** Il client interpreta e visualizza il codice HTML sul dispositivo dell'utente.

- Il codice HTML è generato dall'esecuzione di un programma di script eseguito dal server. L'esecuzione dello script genera un codice HTML che viene inviato al client (**Figura 12**). In questo caso si parla di **pagina Web dinamica**, una pagina, cioè, generata dinamicamente che può essere diversa di volta in volta. In questo caso nell'URL non è specificato il nome del file HTML, ma il nome del file che contiene lo script da eseguire, per esempio il nome di un file PHP.

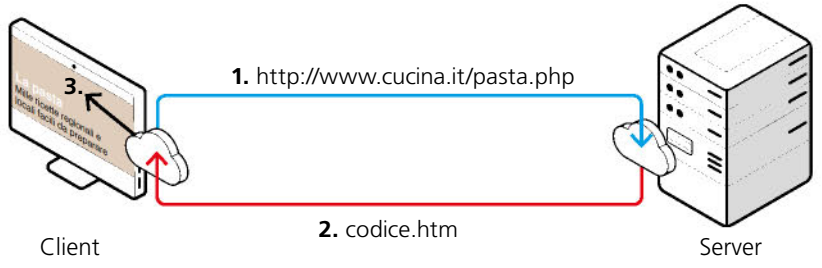


Fig. 12 Richiesta di una pagina Web dinamica. **1.** Il client effettua una richiesta con un file .php (chiede l'output dello script contenuto nel file pasta.php). **2.** Il server esegue lo script, genera un codice HTML e lo invia al client. **3.** Il client visualizza il codice HTML sul dispositivo dell'utente.

Utilizzando un browser, la richiesta di una pagina web può essere fatta in diversi modi, tra cui:

- digitando un URL nella barra degli indirizzi del browser.
  Per esempio: `http://www.cucina.it/pasta.html`
- cliccando sul link di una pagina web che si sta consultando. In questo caso l'URL è il valore dell'attributo `href` del tag `<a>`
  Per esempio: `<a href="http://www.cucina.it/pasta.html" > le nostre paste </a>`
- utilizzando un form HTML per inserire dei dati. In questo caso l'URL è il valore dell'attributo `action` del tag `<form>`.
  Per esempio `<form action: "http://www.cucina.it/pasta.html">`

notabene

In genere una pagina dinamica dipende da parametri che il client invia al server. Solitamente i parametri vengono passati mediante la compilazione di un modulo o tramite URL.

Esempio 3

Richiesta di una pagina statica tramite metodo GET

Supponiamo che l'utente digiti nella barra degli indirizzi del browser il seguente URL:

`http://www.paperus.org/nonna/applepie.htm`

Viene generata una richiesta che usa il metodo GET a cui seguirà una risposta da parte del server. Più precisamente, si ha l'apertura di una connessione TCP sulla porta 80 del server www.paperus.org e la generazione della seguente richiesta che usa il metodo GET:

```
GET /nonna/applepie.htm HTTP/1.1
User-agent: Mozilla
Accept: text/html, image/jpeg, image/png
```

La stessa richiesta sarebbe generata nel caso in cui un utente cliccasse sul link "torta di mele":

Codice pagina html

```
<html>
<head> <title> torte </title>
</head>
esempio di pagina Web con link </p>
<a href="http://www.paperus.org/nonna/applepie.htm"> torta di mele </a>
</html>
```

Link visualizzato



Uno dei motivi più frequenti per cui si usa uno script lato server (server side) è eseguire l'accesso ai dati. L'architettura di un'applicazione su tre livelli, prevede:

1. interfaccia utente. Il client, tramite un'interfaccia web, effettua una richiesta HTTP al server HTTP;
2. logica di funzionamento: il server HTTP chieda i dati (tramite codice SQL embedded) a un DBMS server;
3. accesso ai dati: il DBMS server esegua il codice SQL e fornisca i dati al server Web; il server genera il codice HTML e lo invia al client; il client lo visualizzi sul dispositivo dell'utente (**Figura 13**).

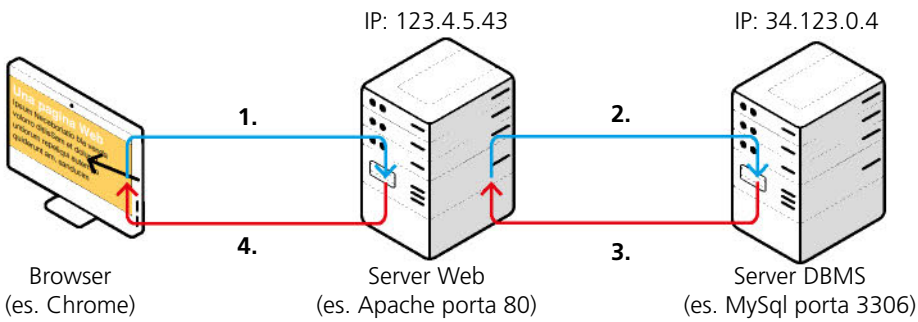


Fig. 13 Richiesta di una pagina Web dinamica che accede a DBMS. **1.** Il client stabilisce una connessione con il server Web (porta 80) in esecuzione sul server 123.4.5.43 [123.4.5.43:80] per richiedere il codice HTML. **2.** Il server Web stabilisce una connessione con server DBMS (MySql – porta 3306) in esecuzione sul server 34.123.0.4 [34.123.0.4:3306]. **3.** Il server DBMS esegue l'accesso ai dati e risponde al server Web. **4.** Il server Web genera il codice HTML e lo invia al client.

Il passaggio di parametri e i metodi GET e POST

Il codice HTML di una pagina web dinamica può dipendere da parametri che il client invia al server nella richiesta HTTP. Un parametro è passato dal client al server nella richiesta HTTP utilizzando la sintassi

```
nome _ parametro = valore
```

Nel caso in cui debbano essere passati più parametri, le stringhe sono concatenate e separate dal carattere &:

```
nome _ param1=valore1&nome _ param2=valore2&….
```

La lettura dei paramentri da parte del server, non è altro che un parsing sulla stringa ricevuta.
Per esempio, progettiamo uno script che genera una pagina HTML dinamica che visualizza:

"Buongiorno nome e cognome !!!"

dove nome e cognome sono due dati che il client invia al server.
La stringa con i parametri avrà la forma:

```
nome=Anna&cognome=Rossi
```

Nella richiesta del client i parametri occupano una posizione diversa a seconda del metodo utilizzato.

- Con il metodo **GET** sono concatenati all'URL e separati da esso con il carattere ?. Quando la richiesta arriva al server la stringa dei parametri è posta in una variabile di ambiente (superglobale) di nome **QUERY_STRING**, e da qui letta con la tecnologia lato server utilizzata. Per esempio, in php il valore della query_string è posto in un array associativo $_GET

Esempio 4

```
GET  www.miosito.it/benventuo.php?nome=Anna&cognome=Rossi
HTTP/1.1

query_string = "nome=Anna&cognome=Rossi"

Lettura tramite php:
$nome=$_GET['nome']
$cognome =$_GET['cognome']
```

- Con il metodo POST i parametri sono nel body della richiesta. Quando la richiesta arriva al server, la stringa dei parametri è letta come da standard input. L'header content-length indica il numero di caratteri da leggere. Per esempio, in PHP la stringa dei parametri letta dal body è posta nell'array associativo $_POST.

Esempio 5

```
POST www.miosito.it/benventuo.php HTTP/1.1
Content-Length:23

nome=Anna&cognome=Rossi

Lettura tramite php:
$nome=$_POST['nome']
$cognome =$_POST['cognome']
```

Il diverso modo di passare i parametri con GET e con POST, implica altre differenze tra i due metodi .
La Tabella 5 che segue sintetizza il confronto tra metodo GET e metodo POST.

notabene

Il formato dei dati passati con POST è specificato nell'header *Content-Type*.
I due formati comuni sono:

- Content-Type: application/x-www-form-urlencoded: formato predefinito per i form HTML.
  I parametri sono codificati come una stringa come quella usata da GET.
- Content-Type: multipart/form-data: formato usato per l'upload di file tramite form. È più complesso e include anche i dati binari dei file.

Pit Stop

4 Che cos'è il Web?

5 Come avviene lo scambio di pagine web in Internet?

→ Tab. 5 Metodo GET e metodo POST.

GET, metodo	GET, metodo
• I parametri (i dati che devono essere inviati al server) sono concatenati all'URL separati da "?"; • i parametri sono visibili nella barra degli indirizzi del browser, e quindi è possibile condividerli facilmente e salvarli come segnalibri; • la stringa dei parametri ha una lunghezza limitata; • lato server i parametri sono letti dalla QUERYSTRING.	• I parametri sono inseriti nel body della richiesta; • i parametri non sono visibili nella barra degli indirizzi del browser e quindi sono apparentemente più sicuri. Tuttavia, essendo trasmessi in chiaro, per vederli basta utilizzare un semplice monitor di rete; • la lunghezza della stringa dei parametri non ha limiti ed è specificata nell'header *Content_length*.

HTTP stateless

Il protocollo HTTP è stateless (senza stato). Questo significa che quando viene inviata una richiesta, il server risponde e non tiene "memoria" di quanto già fatto da quel client, non riconosce lo stato di una sessione. Ogni richiesta è indipendente dalle altre. Se, per esempio, stiamo navigando nel Web e passiamo da una pagina a un'altra e poi a un'altra ancora, per HTTP ogni accesso è come se fosse il primo.
A volte però c'è la necessità di mantenere memoria di alcune scelte o alcune azioni effettuate da un utente (per esempio la scelta di una lingua).
Una particolare problematica legata al fatto che HTTP è stateless riguarda l'accesso a un'area riservata.
Consideriamo un servizio disponibile via Web. Per esempio, la prenotazione di un corriere per l'invio di pacchi. Un utente può navigare liberamente nel sito del fornitore per consultare le offerte, ma quando decide di avvalersi del servizio deve registrarsi e fornire i propri dati. Successivamente, per prenotare il ritiro di un pacco e seguirne il tracciamento, dovrà autenticarsi ed entrare in un'area ad accesso riservato. Questa area è costituita, in genere, da più pagine. Per non richiedere l'autenticazione ogni volta, sarebbe necessario tenere traccia del fatto che l'autenticazione è già avvenuta.
La soluzione a questo problema è quella di scrivere su un file (su memoria permanente) ciò che si desidera memorizzare. Quando l'utente fa una scelta o compie un'azione di cui si vuole tenere traccia, queste vengono scritte su un file che poi verrà letto all'occorrenza.
Session e **cookie** sono le modalità con cui realizzare la soluzione:

- un **cookie** è un piccolo file di testo che è **salvato sul dispositivo del client**. Il server e il client si mandano i cookies come header HTTP.
- L'utilizzo dei cookie è regolamentato dal GDPR, il Regolamento Generale sulla Protezione dei Dati, una Direttiva che regola il trattamento dei dati personali, pubblicato sulla **Gazzetta Ufficiale dell'Unione Europea** applicabile in tutti gli Stati Membri, Italia inclusa, dal **25 maggio 2018**.
- Un file **session** è un file **salvato sul server** in una determinata cartella. Su questi file possono essere scritte le informazioni che devono essere conservate per identificare lo stato in cui si trova l'utente durante la "navigazione" in una sessione (transazione).

Nella sezione di laboratorio vedremo degli esempi di uso dei cookie e delle session in PHP.

Pit Stop

6 Cosa significa che HTTP è stateless?

La Tabella 6 seguente riassume le principali differenze tra cookie e session (con riferimento all'ambiente PHP):

Tab. 6 Cookie e session.

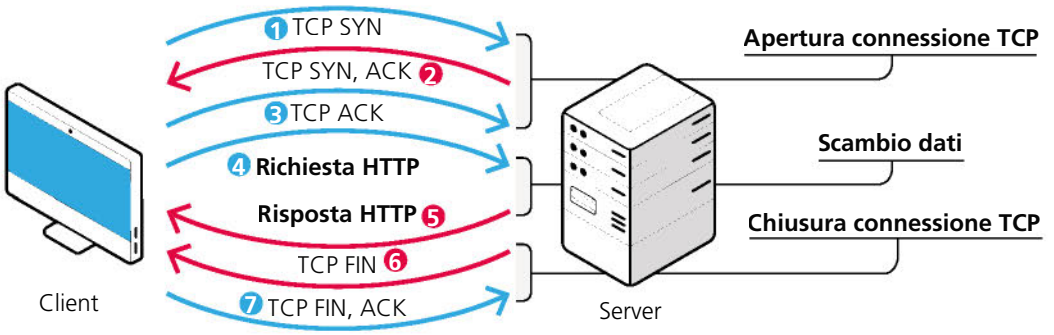
Cookie	Session
I cookie sono file memorizzati sul client	Le sessioni sono file memorizzati sul server
La durata massima di un cookie è impostata come parametro quando il cookie è creato.	La durata massima di una sessione è specificata nel file php.ini tramite `session.gc _ maxlifetime`
Un cookie è caricato, per essere usato, nell'array associativo `$ _ COOKIE`	Un file di session è caricato, per essere usato, nell'array associativo `$ _ SESSION`
Per utilizzare i cookie non servono inizializzazioni.	Il caricamento del file di sessione nella ram in `$ _ SESSION`, avviene quando nello script si usa `session _ start()` (di solito all'inizio)
La dimensione massima di un cookie è di 4KB	Non c'è limite alla dimensione massima di un file di sessione
Per cancellare un cookie si ricrea con un tempo di vita negativo	Per cancellare una variabile si usa `unset()`. Per distruggere una sessione si una `session _ destroy()`
Un cookie è eliminato dall'utente tramite le impostazioni del browser oppure quando termina la durata impostata	Un file di sessione è eliminato alla chiusura del browser, quando viene effettuato il logout (sotto al quale ci sarà `session _ destroy())` o trascrso il tempo impostato in `session.gc _ maxlifetime`

Approfondimento - Tecnologia 1

Versioni HTTP

Come abbiamo visto, HTTP poggia su TCP, quindi a livello Trasporto occorre che (Figura 1):

- il client effettui la richiesta connessione TCP (a tre vie);
- ci sia lo scambio di informazioni;
- la connessione TCP venga chiusa.



➜ **Fig. 1** Apertura connessione TCP, scambio messaggi HTTP, chiusura connessione TCP.

Con questo modello, ogni richiesta HTTP prevede l'apertura e la chiusura di una connessione TCP. Questo è poco efficiente. Infatti, se una pagina web contiene vari elementi, come per esempio delle immagini, le operazioni di apertura e chiusura connessione TCP sarebbero ripetute.
A partire dalla versione 1.0, HTTP ha avuto una evoluzione per migliorare in termini di efficienza e sicurezza.

Le versioni sono:

- HTTP/ 0.9 del 1991
- HTTP/ 1.0 del 1996
- HTTP/ 1.1 del 1997
- HTTP/ 2.0 del 2015
- HTTP/ 3.0 del 2018

Le versioni attualmente più utilizzate sono HTTP 1.1 e HTTP 1.2
La Tabella 1 riporta le principali caratteristiche delle diverse versioni di HTTP:

HTTP/ 1.1 presenta i seguenti vantaggi:

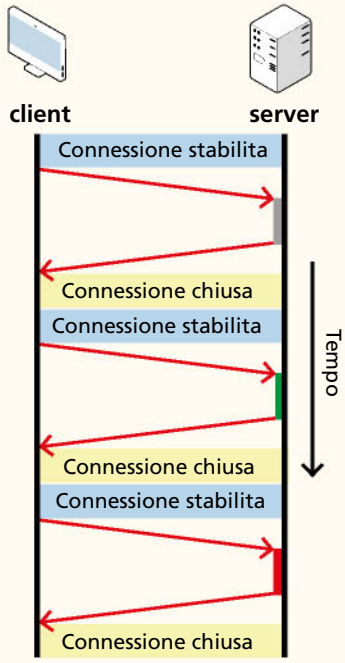
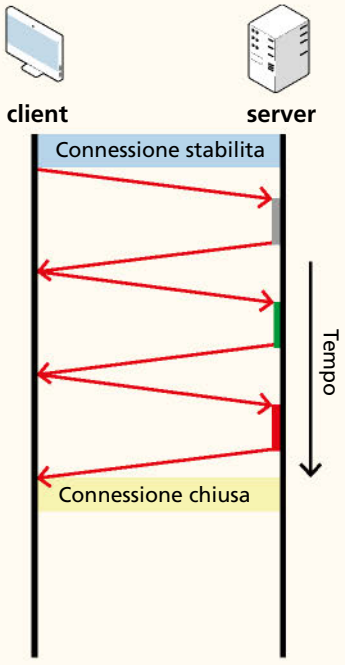
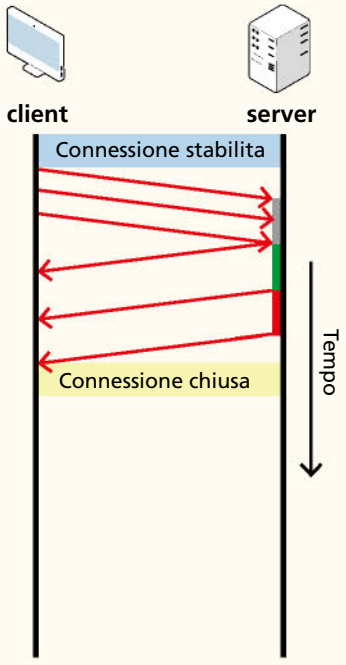
- Sono effettuate meno richieste di connessioni TCP con vantaggi sulle prestazioni (tempo CPU e banda per la trasmissione).
- La visualizzazione della pagina è più rapida.
- permettono di velocizzare la visualizzazione di un'intera pagina.
- la versione con pipeline aumenta ulteriormente l'efficienza.

HTTP/2, pur essendo compatibile con HTTP/1.1, introduce ulteriori miglioramenti, in particolare consente:

- Multiplexing: abilita il parallelismo consentendo di effettuare più richieste concorrenti su una stessa connessione TCP.
- Priorità: consente al client di chiedere al server di dare priorità alle risposte. Per esempio, i file CSS sono inviati prima in modo che le pagine siano mostrate subito in modo formattato.
- Compressione degli header: gli header vengono compressi per ridurre l'overhead (percentuale di intestazioni rispetto ai dati di payload).
- Cifratura: la maggior parte delle volte HTTP/2 è utilizzato con TLS (HTTPs).

HTTP/3, migliora ulteriormente le prestazioni ma attualmente è ancora poco diffuso.

Tab. 1 Versioni di HTTP.

HTTP/ 1.0	HTTP/ 1.1	
connessione non persistente	**connessione persistente**	
	Senza pipeline	Con pipeline
		
Connessione non persistente: per ogni richiesta HTTP, è aperta e chiusa una connessione TCP. Se una pagina web, per esempio, contiene 5 immagini sullo stesso server, devono essere inoltrate 6 richieste HTTP e per ciascuna è aperta e chiusa una connessione TCP, con notevole dispendio di tempo.	Connessione persistente senza pipeline: è aperta una connessione TCP, sono inoltrate le richieste HTTP e al termine la connessione TCP è chiusa. Il client HTTP invia una richiesta, il server invia la risposta e successivamente il client invia una nuova richiesta.	Connessione persistente con pipeline: è aperta una connessione TCP, sono inoltrate le richieste HTTP e al termine la connessione TCP è chiusa. Il client HTTP inoltra le richieste senza attendere le risposte del server.

Approfondimento - Tecnologia 2

API REST

In un'applicazione distribuita a più livelli (*distribuite multi-tier application*), c'è la necessità di far comunicare tra loro le applicazioni per scambiarsi dati utilizzando degli standard di comunicazione.
In particolare, in ambiente Web, le applicazioni rendono disponibili dei servizi (Web Services). Un singolo Web Service può essere utilizzato da diverse applicazioni aumentando l'efficienza e accorciando i tempi di sviluppo. Ogni microservizio è visto come un modulo software accessibile in internet, che può essere invocato tramite un'interfaccia e utilizzato da più applicazioni per "comporre" applicazioni più complesse.
Questa architettura deve favorire l'interoperabilità tra applicazioni e il **disaccoppiamento** tra il client che invia la richiesta di un servizio e il server che fornisce il servizio: il client non sa come funziona il server e viceversa, ma i due concordano un'interfaccia di comunicazione.
Ogni modulo svolge un compito, risolve un problema, incapsula un "servizio".

notabene
Il concetto di interoperabilità tra applicazioni distribuite è molto simile a quello di *information hiding*.

Esistono vari approcci di progettazione, ma uno dei più affermati è l'approccio **REST** (**RE***presentational* **S***tate* **T***ransfer*), che sfrutta pienamente le potenzialità del protocollo HTTP, da cui deriva, senza aggiungere alcun'altra sovrastruttura. REST è centrato più sul concetto di risorsa che di servizio.
Nell'implementazione dei servizi RESTful , il client invia al server una richiesta HTTP di una risorsa identificata da un URI utilizzando un "metodo". Il metodo è inteso come azione che il server deve eseguire su quella risorsa. Il server crea e rende disponibili gli endpoint HTTP (API), utili per la mappatura dei metodi HTTP con le operazioni CRUD, come mostrato nell'esempio nelle pagine successive.
Affinché un Web Service sia RESTful, devono essere soddisfatti i seguenti vincoli:

1. Identificazione delle risorse
2. Utilizzo esplicito dei metodi HTTP
3. Risorse autodescrittive
4. Collegamenti tra risorse
5. Comunicazione senza stato
6. Cacheable
7. Code on Demand

1. Identificazione delle risorse

Le risorse devono essere identificate univocamente da un URI. Per risorsa si intende un qualsiasi elemento oggetto della comunicazione tra le due applicazioni (service consumer e service provider).
Ogni informazione può essere una risorsa ed è identificata da un nome.
Esempi: un cliente, un libro, un articolo, un qualsiasi oggetto su cui è possibile effettuare operazioni. Per fare un parallelo con la programmazione a oggetti possiamo dire che una risorsa può essere assimilata a una istanza di una classe.

Di seguito esempi di URI:

- `http://www.miosito.com/libri/1`
- `http://www.miosito.com/ordini/2025/123`
- `http://www.miosito.com/ordini/2025`
- `http://www.miosito.com/libri?titolo=pinocchio`

2. Utilizzo esplicito dei metodi HTTP

È stabilita una mappatura uno a uno tra le tipiche operazioni CRUD (Create Read, Update, Delete) applicate a una risorsa e i metodi HTTP (Tabella 1).

← Tab. 1

metodo	Operazione CRUD	descrizione
POST	Create	Crea una nuova risorsa. Il metodo POST invia una risorsa da aggiungere ad una struttura già esistente. (append). Spesso il server risponde con: 201 Created. Nel response header Location è indicato l'URI della risorsa creata.
GET	Read	Utilizzato dal client per richiedere una risorsa. GET è una operazione di sola lettura.
PUT	Update	Aggiorna una risorsa o ne modifica lo stato.
DELETE	Delete	Elimina una risorsa.

notabene

Spesso si usa GET in modo improprio, per esempio per inviare una risorsa:

`http://www.miosito.com/crealibro?titolo=Pinocchio&pagine=200`

Questo approccio non è conforme ai principi REST. Il metodo GET deve essere usato per accedere alla rappresentazione di una risorsa e non per crearne una nuova. L'uso improprio di GET potrebbe creare problemi ed effetti indesiderati, in particolare se la richiesta è effettuata più volte.

3. Risorse autodescrittive

Le risorse sono concettualmente separate dalle loro rappresentazioni che sono codificate in un formato standard e comprensibile da client e da server. I formati più utilizzati sono JSON e xml.
Il client può richiedere uno specifico formato usando l'header *Accept*, o comunicare il formato della risorsa inviata tramite l'header *Content-Type*.
Il server invia il formato usato tramite il tipo MIME
Se il Web Service lo supporta, la stessa risorsa può essere richiesta in formati diversi, come ad esempio JSON o HTML.

notabene

La possibilità di rappresentazioni multiple ha il vantaggio che la risorsa può essere utilizzata da più applicazioni. Per esempio, se abbiamo un output sia HTML sia XML, possiamo usare la risorsa sia con un'applicazione sia con un browser, con la possibilità di progettare sia livelli intermedi di una applicazione multi-tier (web API) sia il livello di interfaccia utente (web UI, in genere il primo).

4. Collegamenti tra risorse

Le risorse sono collegate tramite link ipertestuali. Questo principio è anche noto come **HATEOAS**, dall'acronimo di **H***ypermedia* **A***s* **T***he* **E***ngine* **O***f* **A***pplication* **S***tate*. Tutte le informazioni relative a una risorsa devono essere contenute nella sua rappresentazione o devono essere accessibili tramite link contenuti nella sua rappresentazione. In particolare, la rappresentazione di un ordine in un linguaggio XML-based deve contenere gli eventuali collegamenti agli articoli e al cliente correlati.

Consideriamo ad esempio le risorse inerenti gli studenti:

```
<studente>
      <matricola>310122</matricola>
      <nome> Paola </nome>
      <cognome> Verdi </cognome>
      <classe rif = "http://www.miosito.com/classi/3A" />
      <verifiche>
<verifica rif = "http://www.miosito.com/prove/1"/>
<verifica rif = "http://www.miosito.com/prove/2"/>
      </verifiche>
</studente>
```

In questo modo il client può accedere alle risorse correlate seguendo i link contenuti nella rappresentazione della risorsa corrente.

5. Comunicazione senza stato

notabene

Questo meccanismo richiama la cardinalità 1:N e N:N del modello concettuale E/R usato per la progettazione di database relazionali.

Poiché HTTP è senza stato, anche un **Web Service RESTful**, è senza stato: ogni richiesta è indipendente dalle altre e deve contenere le informazioni utili per essere completamente servita, indipendentemente dalle precedenti. La gestione dell'applicazione è a carico del client.

6. Cacheable

Quando il server invia una risorsa al client, specifica, tramite header cache control e last value, se la risorsa deve essere mantenuta in una cache per essere riutilizzata in richieste successive.

7. Code on demand

Riguarda la possibilità che il server invii del codice che possa essere eseguito dal client.
È l'unico vincolo (requisito) opzionale.

Esempio

Si consideri la seguente collezione di risorse relative agli studenti rappresentate in formato json:

```
{
  "studenti": [
    {
     "matricola": "122345",
```

```
      "nome": "Marco",
      "cognome": "Rossi"
    },
    {
      "matricola": "310122",
      "nome": "Elena",
      "cognome": "Bianchi"
    }

  ]
}
```

Per la gestione di queste risorse il server crea e rende disponibili i seguenti endpoint HTTP (API), utili per la mappatura dei metodi HTTP con le operazioni CRUD:

`http://www.scuola.it/studenti`

- `GET /studenti`
- `GET /studenti/{id}`
- `POST /studenti`
- `PUT /studenti/{id}`
- `PATCH /studenti/{id}`
- `DELETE /studenti/{id}`

```
GET http://www.scuola.it/studenti/3120122 HTTP/1.1
```

richiede lo studente con matricola 310122.
Il server invia la risorsa nel body della richiesta.

```
POST http://www.scuola.it/studenti HTTP/1.1
Content-Type: application/json
{
      "matricola": "436788",
      "nome": "Maria",
      "cognome": "Rossi"
}
```

invia al server lo studente con matricola 436788 nel body della richiesta.

Approfondimento - Storia dell'informatica

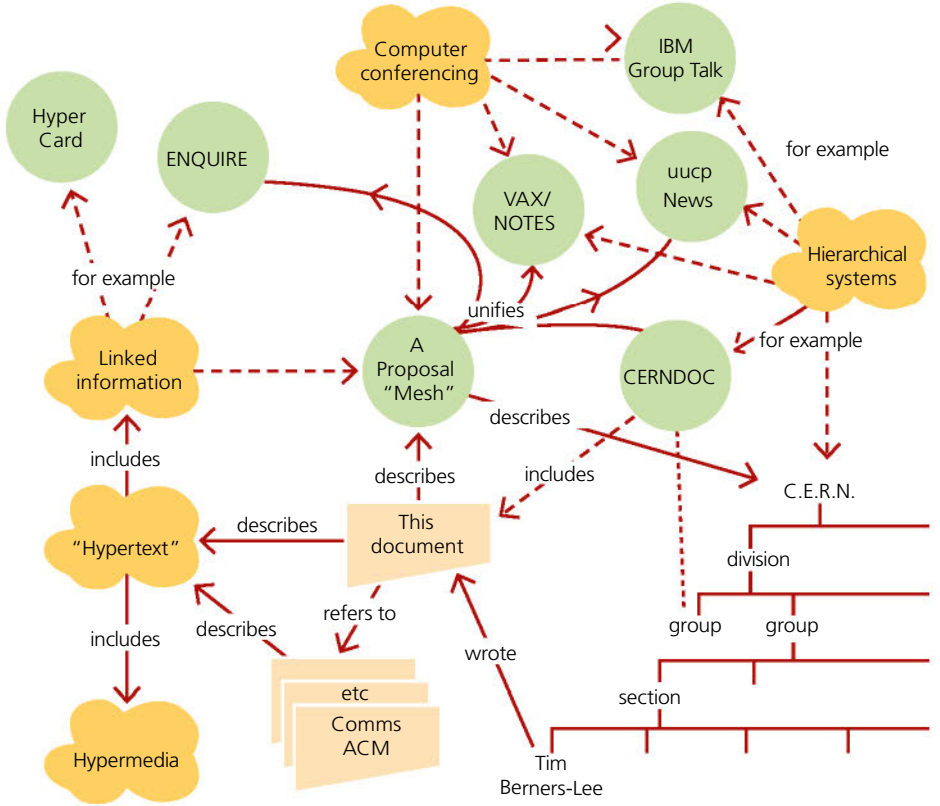


↑ **Fig. 1** «Il Web è unico perché è libero. Chiunque può creare un documento e metterlo gratuitamente online. Il W3C cerca di evitare che interessi di qualsiasi genere possano porre un freno a questa assoluta libertà» (dallo statuto del W3C `Whttp://www.w3.org`). Questa è la targa che, al CERN di Ginevra, ricorda l'ufficio dove nacque il Web.

La nascita del Web

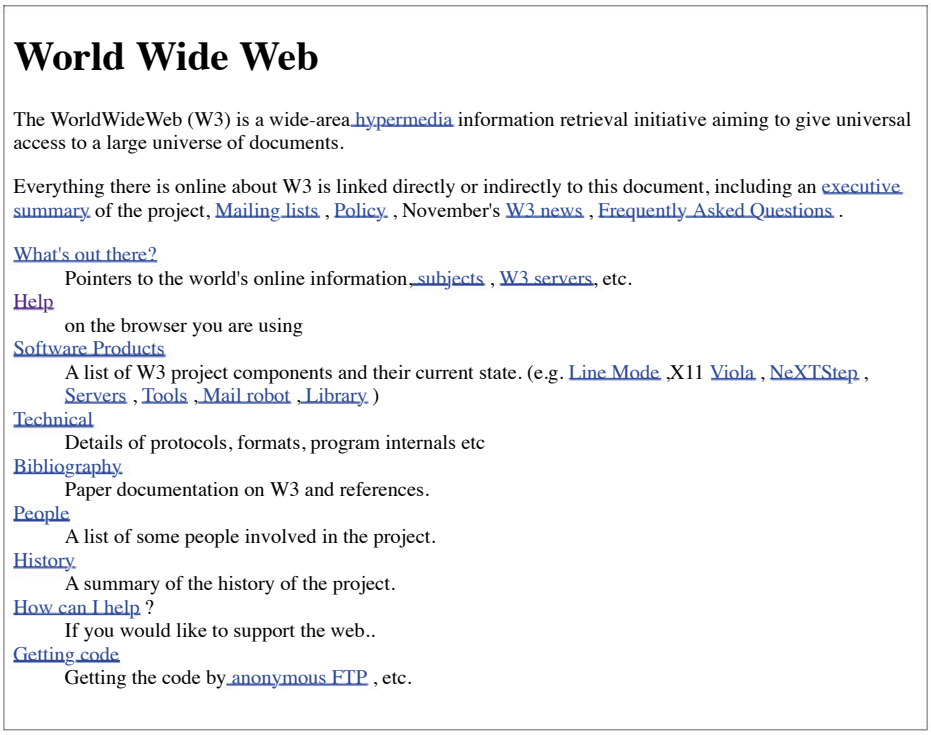
La nascita del World Wide Web è stato un momento rivoluzionario nella storia di Internet. Tutto ha avuto inizio nel 1989, quando Tim Berners-Lee, presso il CERN di Ginevra (**Figura 1**), ha l'idea di creare un «ampio database ipertestuale con link». Nella seconda metà degli anni Ottanta del secolo scorso, Internet era ancora limitata agli ambienti scientifici e a piccoli gruppi di appassionati. Mancavano strumenti di facile utilizzo che potessero permettere alla maggior parte delle persone di entrare in rete e scambiarsi informazioni. L'unico strumento sufficientemente versatile era la posta elettronica, che è giunta fino a noi con poche modifiche.

Nel 1990, le cose cambiano radicalmente. Tim Berners-Lee propone un progetto per utilizzare Internet allo scopo di condividere, in modo semplice e rapido, le informazioni con gli altri ricercatori sparsi sul pianeta (**Figura 2**). I testi si trasformano in "Ipertesti": è la nascita del World Wide Web.



↑ **Fig. 2** Lo schema (ridisegnato) che accompagnava il documento con cui nel 1989 Tom Berners-Lee propose al CERN il suo progetto per immagazzinare informazioni. Il documento recita così: «This proposal concerns the management of general information about accelerators and experiments at CERN. It discusses the problems of loss of information about complex evolving systems and derives a solution based on a distributed hypertext system».

Vengono creati nuovi standard come HTML (*HyperText Markup Language*) e il protocollo HTTP (*HyperText Transfer Protocol*). Nascono i primi browser, che consentono alle persone di "navigare" in Internet con facilità (**Figura 3**). Il Web diventa accessibile a un pubblico più ampio. Tim Berners-Lee afferma che il Web è un'invenzione sociale prima che tecnica. Lo progetta per permettere alle persone di collaborare e migliorare la loro esistenza.
Nel 1994, viene fondato il World Wide Web Consortium, una comunità internazionale che sviluppa gli standard Web e si impegna a preservare la libertà e l'indipendenza degli utenti della rete.



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

Fig. 3 La prima pagina Web, pubblicata al CERN, dove il 30 aprile 1993 venne rese pubblico il software World Wide Web.

Il concetto di ipertesto (un insieme di documenti messi in relazione tra loro per mezzo di parole chiave) è centrale nelle applicazioni web, anche se non è una sua caratteristica esclusiva. Già dal XVIII secolo, ai tempi dell'*Encyclopédie*, edita da d'Alembert e Diderot (**Figura 4**), c'è stata una prima rottura dell'ordine lineare, con una catalogazione alfabetica delle voci e un'organizzazione del sapere con "rinvii" che prefigurano gli attuali collegamenti ipertestuali e favoriscono i contatti tra le diverse discipline: un elemento può far parte di classi diverse a seconda del punto di osservazione. Con l'ipertesto, il lettore non è più costretto a seguire un percorso lineare predefinito, ma può scegliere cosa visitare, muovendosi tra argomenti diversi.

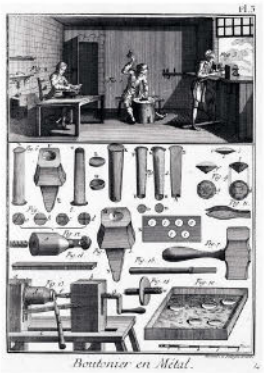


Fig. 4 L'*Encyclopédie* di d'Alembert e Diderot introduceva un concetto nuovo di navigazione del testo, con una catalogazione alfabetica delle voci.

Laboratorio

ATTIVITÀ 1
Esplorare una richiesta HTTP con Google Chrome

Scenario

Per accedere a un'applicazione Web utilizziamo un URL (*Uniform Resource Locator*) e il protocollo HTTPS. Ad esempio:

`https://www.esempio.com/search?q=mela+rossa&ie=UTF-8`

- L'URL contiene, oltre al dominio, uno script (`/search`) con i due parametri di query: "mela", "rossa".
- "**?**" indica i parametri di input nello script e il simbolo "**&**" delimita diversi parametri di input (il parametro `ie=UTF-8` indica la codifica dei caratteri utilizzata per la ricerca (`UTF-8` è la codifica Unicode, `ie` sta per Internet Explorer).

notabene

Il carattere / indica la root del server, cioè la directory principale del sito web in cui di solito si trova la pagina iniziale.

Consegna

Effettuare una richiesta con parametri al server web di Google, utilizzando un browser come Google Chrome, e analizzare con gli strumenti per sviluppatori le richieste/risposte del protocollo HTTP.

Svolgimento

Passo 1: richiesta al motore di ricerca
Si effettui una richiesta al motore di ricerca di Google inserendo la frase "mela rossa" nel campo di ricerca.

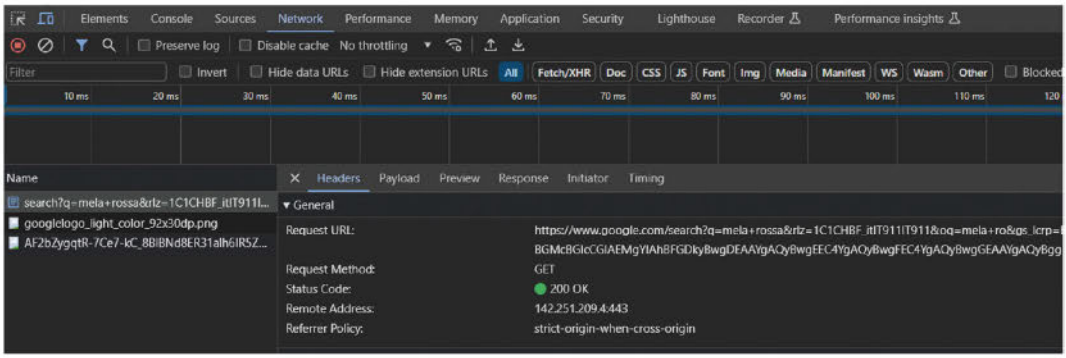


notabene

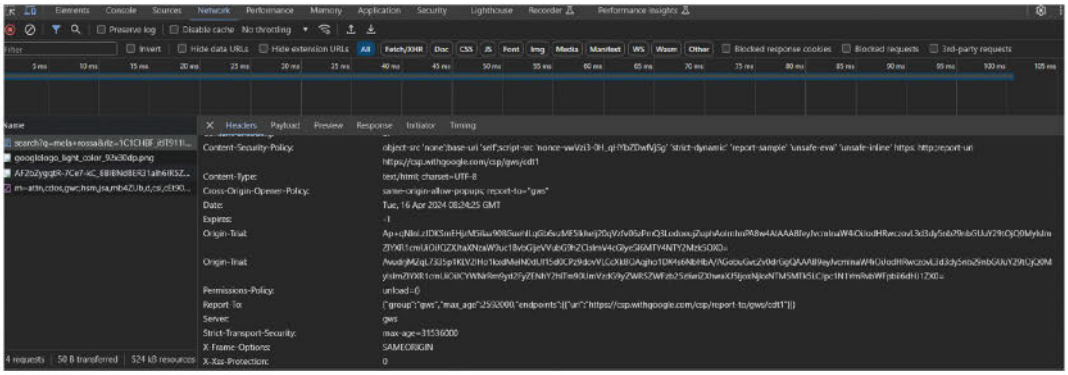
Occorre distinguere il motore di ricerca dalla barra degli indirizzi di un browser. In entrambi un utente fornisce un input inserendo una stringa in un campo di testo. Nella barra degli indirizzi di un browser occorre inserire un URI per accedere a una risorsa in Internet: tramite l'URI parte una richiesta HTTP e il browser visualizza la risposta. Nel motore di ricerca occorre inserire delle chiavi di ricerca per accedere a informazioni su quell'argomento. In questo caso verranno restituiti alcuni siti in cui trovare informazioni relative alla ricerca.

Passo 2: visualizzazione dei parametri di Richiesta/Risposta
Utilizzare nel browser il tasto F12 (strumenti per sviluppatori) e osservare:

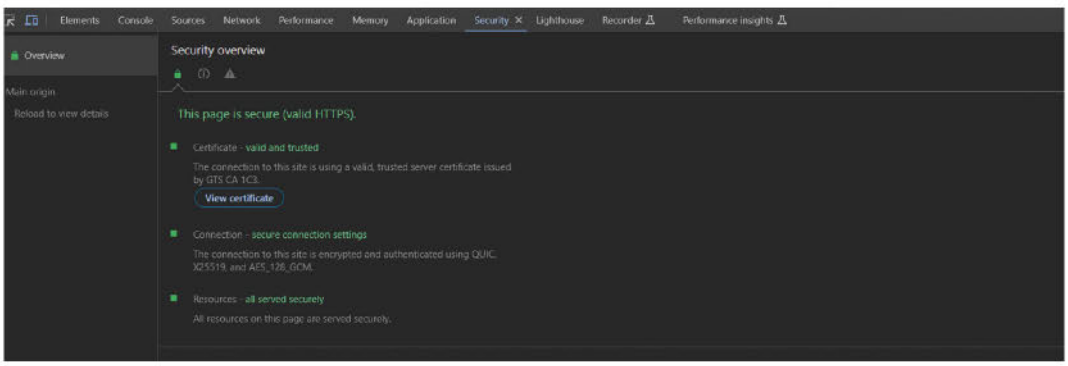
- metodo di chiamata: GET;
- passaggio dei parametri nella variabile `q=mela+rossa` verso l'applicazione Search in `www.google.it` attraverso il protocollo HTTPS;
- risposta: codice 200/OK.



Passo 3: analisi dettagliata di alcuni parametri presenti nell'intestazione



Passo 4: controllo della sicurezza (HTTPS = HTTP + TLS)



Laboratorio

ATTIVITÀ 2

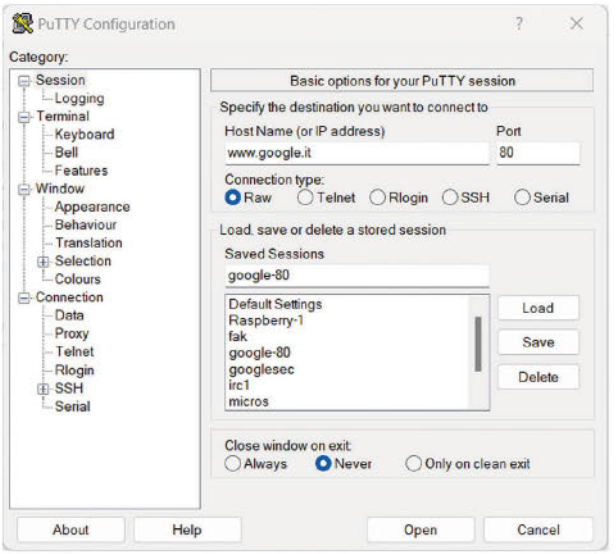
Collegarsi a google.it con Putty sulla porta 80

Scenario

Putty permette di collegarsi a Google utilizzando la riga di comando, per l'analisi dei comandi HTTP.

Consegna

Configurare Putty e collegarsi al server web di Google e ottenere la pagina principale, utilizzando la modalità Raw.



Svolgimento

Passo 1: configurazione di Putty

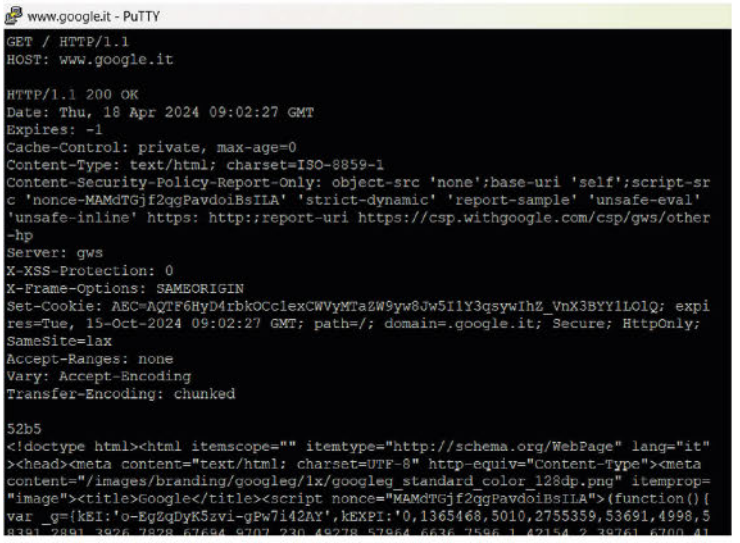
- inserire l'indirizzo IP;
- selezionare la porta 80;
- selezionare RAW come opzione;
- selezionare Never;
- cliccare su Open per avviare la connessione.

Passo 2: richiesta al server web di Google

Entrati nella finestra a riga di comando, inserire metodo (GET), / (root) Versione protocollo (HTTP/1.1), quindi, dopo essere andati a capo, inserire il nome dell'host e premere due volte il tasto INVIO.

Passo3: visualizza la pagina web ottenuta dal server

Copiare il codice HTML presente nel body della risposta in un file, salvarlo come file .html e visualizzarlo con un browser.



notabene

La connessione Raw (o connessione grezza) offre una comunicazione di rete senza alcun protocollo. I dati sono trasmessi senza alcuna formattazione. Questo tipo di connessione è utilizzato quasi esclusivamente per scopi di debugging, analisi o test, perché *non garantisce la sicurezza dei dati* che si potrebbe avere utilizzando il protocollo SSH (*Secure Shell*) che crittografa i dati.

ATTIVITÀ 3

Visualizzare il traffico HTTP con Wireshark

Scenario

Utilizzando il Web, si accede al sito della NASA di indirizzo internet `nasa.gov`

Consegna

Visualizzare il traffico HTTPS (richieste e risposte HTTPS) relativo al sito `nasa.gov` utilizzando Wireshark.

Svolgimento

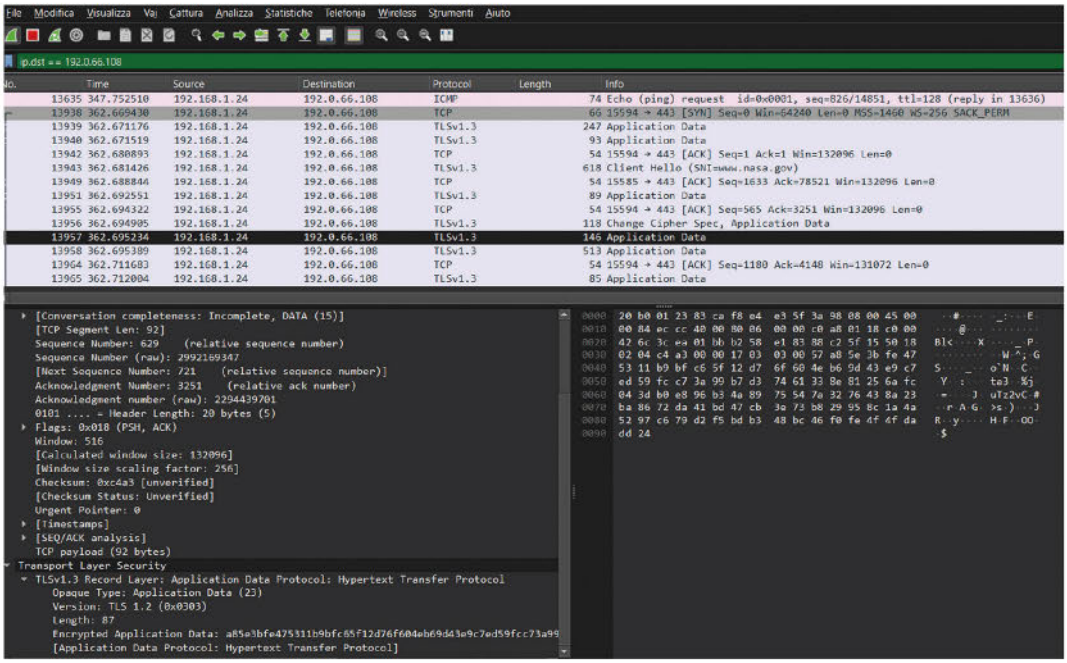
Passo 1: aprire Wireshark e impostare un filtro di visualizzazione con l'indirizzo IP associato al sito della Nasa:

- digitare il seguente filtro nella barra di ricerca di Wireshark:
  `ip.dst == 192.0.66.108`

Questo filtro mostrerà solo i pacchetti che hanno `nasa.gov` come indirizzo IP di destinazione.
Si noti come i dati inviati con il protocollo HTTP (*Application Data Protocol*) siano crittografati (*Encrypted Application data*). Anche in caso di intercettazione, non sono intelligibili.

notabene

L'utilizzo di HTTPS (*Hypertext Transfer Protocol Secure*) è fondamentale per garantire la sicurezza dei dati durante la comunicazione tra un Web browser e un server. I moderni browser Web segnalano esplicitamente i siti che non utilizzano HTTPS come non sicuri, mostrando un lucchetto nella barra degli indirizzi.



Laboratorio

ATTIVITÀ 4
Esplorare il protocollo QUIC con Wireshark

Scenario

Il protocollo QUIC (*Quick UDP Internet Connections*) è un protocollo sviluppato da Google inteso a migliorare le prestazioni delle connessioni Web. Tra le caratteristiche principali ricordiamo:

- utilizzo di UDP in sostituzione di TCP;
- implementazione di funzionalità utilizzate per garantire la gestione e la consegna dei dati e il controllo del flusso:
  - handshake iniziale per la negoziazione dei parametri crittografici e di trasporto;
  - trasmissione, in multiplexing, di diversi flussi di dati attraverso una singola connessione client-server;
  - assegnazione di numeri sequenziali univoci per gestire i pacchetti di dati;
  - correzione degli errori con il recupero dei dati persi o danneggiati durante la trasmissione;
  - gestione efficiente del sovraccarico di rete, con miglioramento delle prestazioni anche in condizioni di traffico intenso;
- utilizzo del protocollo sicuro TLS (versione 1.3) per la crittografia e l'autenticazione dei dati.

QUIC è, di fatto, il livello Trasporto che supporta HTTP/3 (una versione avanzata del protocollo HTTP).

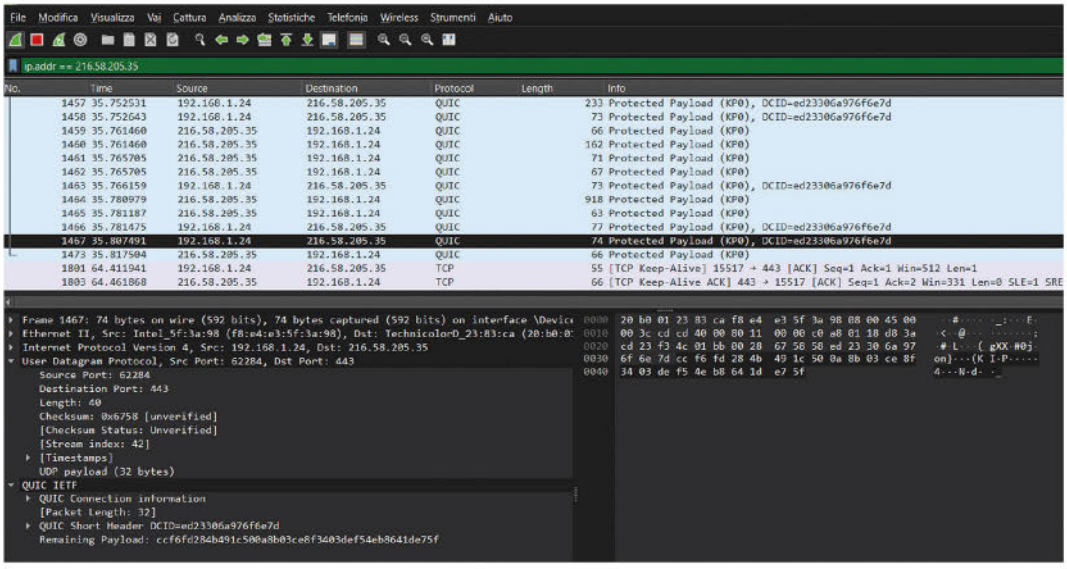
Consegna

Visualizzare il traffico QUIC relativo al sito **`google.it`**

Svolgimento

Passo 1: impostare il filtro di visualizzazione

```
ip.add r== indirizzo IP di google.it
```



ATTIVITÀ 5
Interagire con le API REST di JSONPlaceholder

Scenario

JSONPlaceholder è un servizio API REST gratuito che possiamo utilizzare come sandbox per testare localmente le nostre prove con API REST. JSONPlaceholder offre una serie di risorse pubbliche, tra cui:

- /posts
- /albums
- /todos
- /comments
- /photos
- /users

Per eseguire richieste HTTP su queste risorse e ottenere i dati desiderati, utilizziamo Postman, uno strumento che permette di eseguire in modo semplice ed efficiente richieste verso un server e analizzare le informazioni ricevute.

Consegna

Utilizzare Postman per interagire con le API di JSONPlaceholder per ottenere delle immagini.

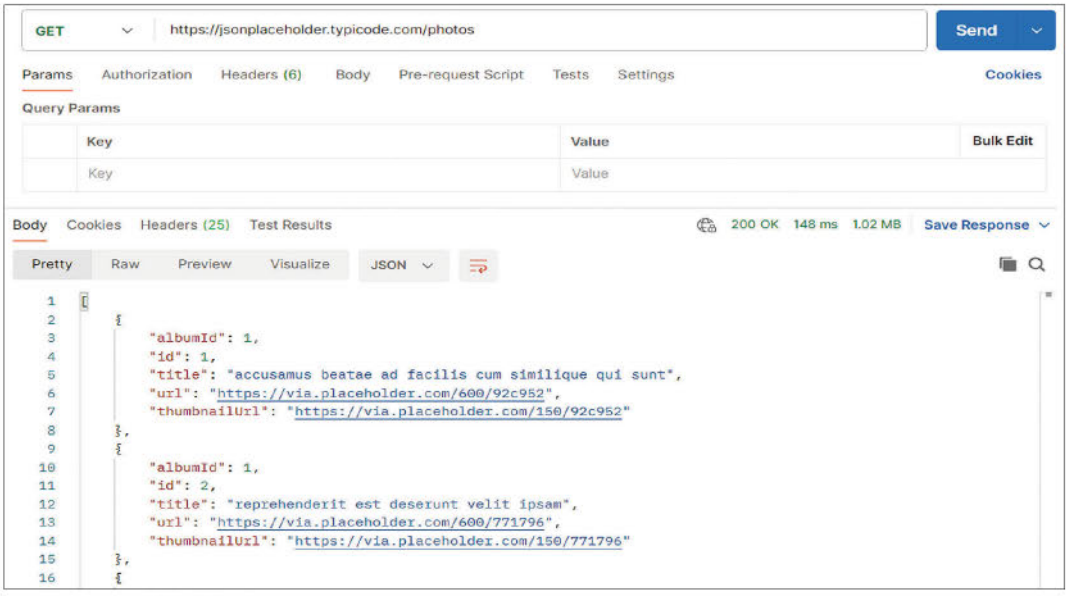
notabene

Postman si scarica da `www.postman.com` e si installa in locale sul proprio PC.

Svolgimento

Passo 1: ricerca delle foto in JSONPlaceholder con metodo GET

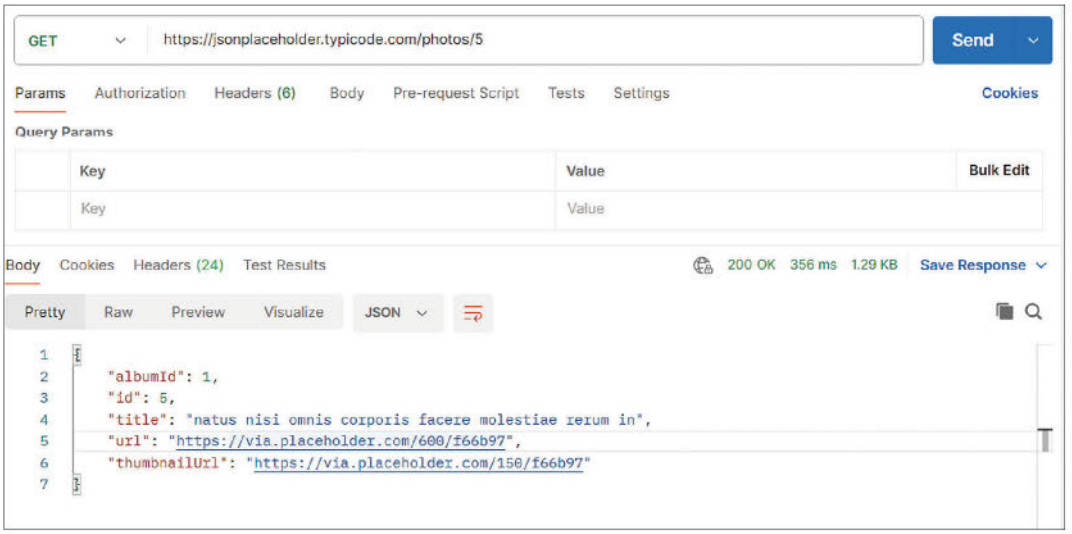
- Impostiamo, in Postman, (dopo averlo installato sul nostro dispositivo locale) il metodo HTTP su **GET**.
- Inseriamo l'URL per ottenere le foto da JSONPlaceholder: `https://jsonplaceholder.typicode.com/photos`.
- Eseguiamo la richiesta (Send) per ottenere l'elenco delle foto.



notabene

ReqBin è un altro ottimo strumento online, utilizzato per inviare richieste HTTP (POST, GET, PUT e HEAD) senza la necessità di installare alcuna applicazione in locale.

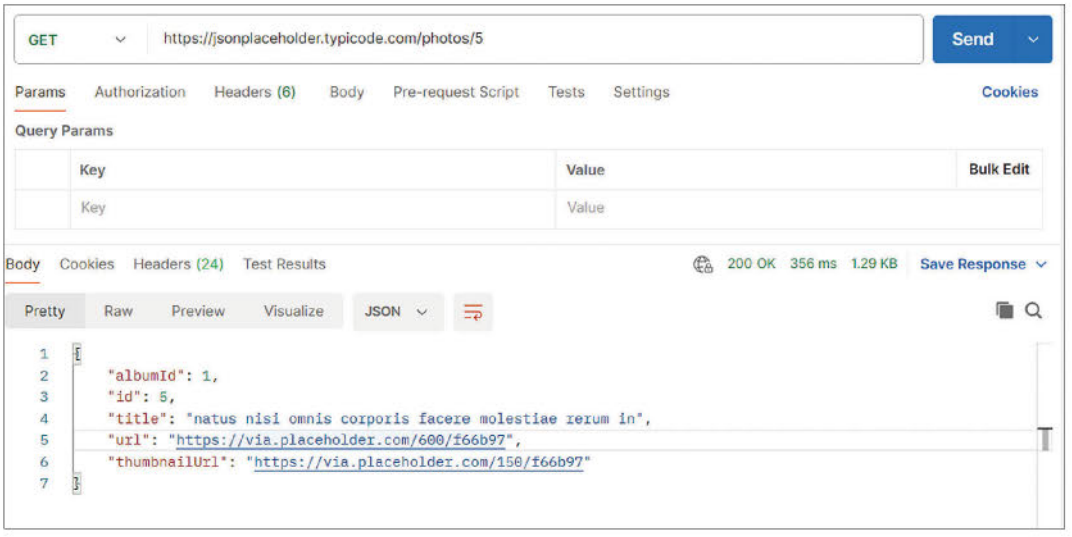
Passo 2: analisi della risposta
Verifichiamo che la risposta contenga l'elenco e i dettagli dell'immagine: ID, titolo, URL



notabene

La risposta di JSONPlaceholder è in formato JSON (*JavaScript Object Notation*), molto utile per rappresentare oggetti e strutture dati e, spesso, utilizzato per scambiare i dati tra un'applicazione Web e un server API.

Passo 3: ricerca dell'immagine con ID = 5



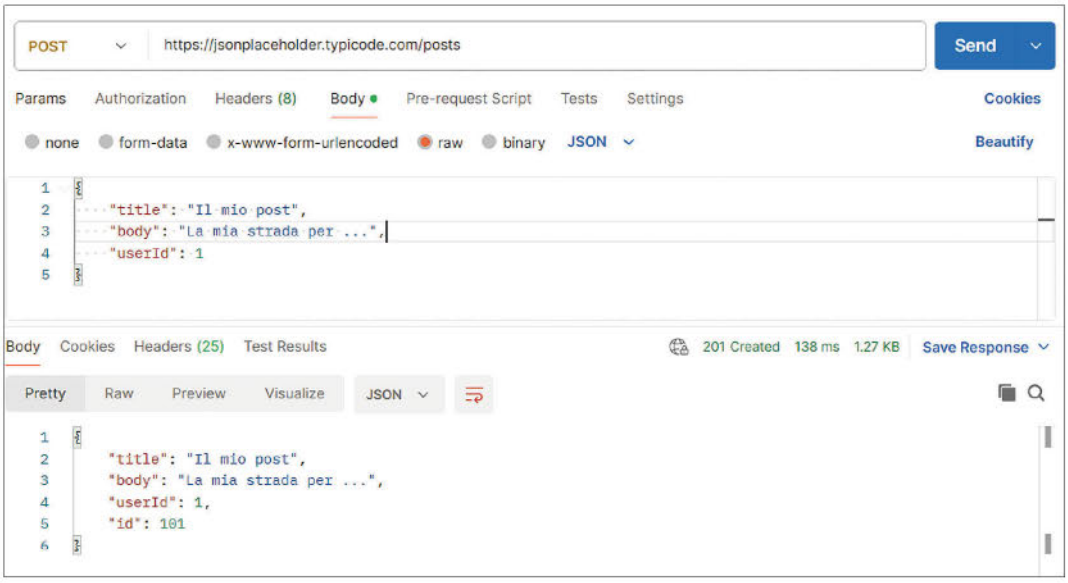
Passo 4: visualizzazione delll'immagine trovata
Visualizziamo su browser l'immagine `f66b97.png` (660 × 600 pixel) presente al link: `https://via.placeholder.com/600/f66b97`.

Passo 5: creazione e invio di un nuovo messaggio con il metodo POST

- Selezioniamo, in Postman, il metodo **POST**;
- Inseriamo l'URL `https://jsonplaceholder.typicode.com/posts` ;
- Nella sezione "Body", scegliamo il formato raw e impostiamo il tipo su JSON;
- Inseriamo il seguente messaggio JSON nel corpo della richiesta:

```
{
    "title": "Il mio post",
    "body": "La mia strada per ...",
    "userId": 1
}
```

- Inviamo il messaggio, premendo Send.



SINTESI

IL LIVELLO APPLICAZIONE IN INTERNET

È il livello più alto del modello TCP/IP e fornisce le interfacce e i protocolli necessari alle applicazioni degli utenti. Le applicazioni sono usate da utenti o da altre applicazioni, e sono suddivise in due o più parti residenti su nodi diversi di Internet. Lato mittente, un protocollo di livello applicazione genera un messaggio e lo passa al livello Trasporto. Lato ricevente, il livello Trasporto legge e toglie l'intestazione e passa il payload all'applicazione identificata dal numero di porta di destinazione.

HTTP E WEB

ARCHITETTURA CLIENT/SERVER

La maggior parte dei protocolli di livello applicazione di Internet sono basati su una architettura Client/Server in cui il client effettua una richiesta al server e il server invia una risposta al client.
Client e server indicano due ruoli assunti da due moduli software. Il client genera un messaggio utilizzando un determinato protocollo. Il server riceve il messaggio e, utilizzando lo stesso protocollo, lo interpreta per fornire una risposta al client.

PROTOCOLLO HTTP

Il protocollo HTTP (*Hypertext Transfer Protocol*) è fondamentale per il funzionamento del Web e di tutte le Web application. Caratteristiche:

- Client/Server.
- Il server lavora sulla porta 80.
- Usato per lo scambio di risorse in Internet.
- Si avvale dell'URI per l'identificazione di una risorsa.
- Il client utilizza i metodi per indicare al server le operazioni da eseguire sulle risorse.

IL WEB

Il funzionamento del Web è basato sul protocollo HTTP, in cui la risorsa richiesta dal client è un file HTML e la risorsa inviata dal server è il codice HTML della pagina richiesta.
Il funzionamento del Web è basato sul protocollo HTTP, in cui la risorsa richiesta dal client è un file HTML e la risorsa inviata dal server è il codice HTML della pagina richiesta.
L'URI assume la forma di URL (*Uniform Resource Locator*) ed è utilizzato per identificare il file richiesto.

- Il client può essere un qualsiasi browser.
- Il server coinvolto è un server HTTP.

API REST

Sono utilizzate per la comunicazione tra applicazioni di rete in ambiente web. Le applicazioni rendono disponibili dei servizi (*Web Services*). Ogni microservizio è visto come un modulo software accessibile in Internet, e può essere invocato tramite un'interfaccia (API) e utilizzato da più applicazioni per "comporre" applicazioni più complesse.
Affinché un Web Service sia RESTful, devono essere soddisfatti i seguenti vincoli:

1. Identificazione delle risorse.
2. Utilizzo esplicito dei metodi HTTP.
3. Risorse autodescrittive.
4. Collegamenti tra risorse.
5. Comunicazione senza stato.
6. Cacheable.
7. Code on Demand.

URI

Un URI (Uniform Resource Identifier) è una stringa che identifica univocamente una risorsa in Internet. È composta da tre parti principali:

`protocollo://indirizzo internet/risorsa`

Esempio:

`http://www.ricettario.it/torte/tortadimele.html`

RICHIESTA E RISPOSTA

La richiesta del client e la risposta del server sono due stringhe ASCII.

Richiesta:

```
<METODO>  <URI>
<VERSIONE>
HEADER:valore
…

BODY
```

Risposta:

```
<VERSIONE>  <CODICE>
<DESCRIZIONE CODICE>
HEADER:valore
…

BODY
```

HEADERS

Le intestazioni (headers) HTTP sono meta-informazioni che il client e il server si scambiano durante la comunicazione. Queste intestazioni forniscono dettagli aggiuntivi sulla richiesta o sulla risposta HTTP. Sono della forma:

`nome:valore`

METODI

Specificano le azioni che il client intende eseguire rispetto alla risorsa specificata tramite l'URI. I principali sono:

- GET: Il client richiede al server la risorsa identificata tramite l'URI.
- POST: Il client invia al server i dati presenti nel body della richiesta. Potrebbe essere una nuova risorsa o dei parametri.
- PATCH: Il client chiede l'aggiornamento della risorsa con la sostituzione di quella esistente. Nel body sono passati i dati da modificare.
- PUT: Il client chiede l'aggiornamento parziale di una risorsa. Nel body sono passati i dati da modificare.
- DELETE: Il client chiede l'aggiornamento parziale di una risorsa. Nel body sono passati i dati da modificare.

GET

Usata per la richiesta di una risorsa. I parametri (i dati che devono essere inviati al server) sono concatenati all'URI separati da "?"

- I parametri sono visibili nella barra degli indirizzi del browser, e quindi è possibile condividerli facilmente e salvarli come segnalibri.
- La stringa dei parametri ha una lunghezza limitata.
- Lato server i parametri sono letti dalla QUERYSTRING.

POST

Usata per l'invio di una risorsa.

- I parametri (la risorsa) sono inseriti nel body della richiesta.
- I parametri non sono visibili nella barra degli indirizzi del browser e quindi sono apparentemente più sicuri.
- La lunghezza della stringa dei parametri non ha limiti ed è specificata nell'header *Content_length*.

Verifica delle CONOSCENZE

Vero o Falso?

1 HTTP è un protocollo di livello Trasporto perché trasporta file. V F

2 HTTP trasmette file in formato ASCII. V F

3 HTTP è utilizzato per il trasferimento di file. V F

4 La QUERY_STRING è usata dal DBMS. V F

5 Un server web è una macchina in Internet. V F

6 Un server web tipicamente lavora sulla porta 25. V F

7 Un browser è un server usato per il protocollo HTTP. V F

8 Una pagina web dinamica è diversa per ogni richiesta del client. V F

9 HTTP utilizza il protocollo TCP. V F

10 Un'applicazione di livello tre è detta "three tier". V F

11 Il metodo GET utilizza la QUERY_STRING. V F

12 Il codice di ritorno 404 della risposta HTTP significa che tutto è andato a buon fine. V F

13 HTTPd è il demone HTTP. V F

14 HTTP non ha memoria. V F

15 La primitiva listen è eseguita da un demone. V F

16 gli header http contengono metainformazioni che client e server si trasmettono. V F

17 Il DBMS è incluso in una pagina Web. V F

18 La risposta HTTP inizia con un codice di ritorno. V F

19 Con il metodo POST i parametri sono passati nel body della richiesta. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

20 L'architettura a tre livelli di un'applicazione comprende:

a interfaccia utente, logica di funzionamento, accesso ai dati
b dati e funzioni
c hardware e software
d interfaccia utente e gestione delle periferiche

21 La prima riga della richiesta HTTP prevede:

a <metodo>spazio<versione HTTP>spazio<URL>
b <codice di ritorno>spazio<descrizione del codice>spazio<versione HTTP>
c <metodo>spazio<URL>spazio <versione HTTP> CRLF
d <protocollo> spazio<nome del server>spazio<nome della risorsa>

22 In un'architettura three tier:

a ci sono tre livelli di applicazione: utente, programmatore e sistemista
b ci sono tre livelli di hardware
c il server Web è il client rispetto al DBMS
d browser e server Web sono in esecuzione su macchine diverse

23 Dire che HTTP è senza stato significa che

a ogni richiesta è indipendente dalle altre
b HTTP non ha il codice di stato
c con HTTP non possono essere passati parametri da client a server
d HTTP non ha la porta di livello Trasporto

24 Nella sintassi HTTP la "riga bianca" è determinata:

a da due invii
b dai caratteri <carriage return> e <line feed>
c dall'assenza di caratteri
d dall'assenza di dati

Domande per la prova orale

25 Descrivi la sintassi del protocollo HTTP (richiesta e risposta) e fai un esempio in cui questo protocollo è utilizzato.

26 Esponi la differenza tra il metodo POST e il metodo GET.

27 Spiega che cosa si intende per "server web".

28 Descrivi i tre livelli di cui è costituita una generica applicazione informatica.

29 Qual è la differenza tra WWW e Internet?

30 Come funziona un sistema Client-Server?

Verifica delle ABILITÀ

Rispondi alle seguenti domande.

31 Che cos'è una pagina web? Esponi la differenza tra pagina web statica e pagina web dinamica, facendo degli esempi di ambito di utilizzo.



32 Considera il seguente codice HTML:

```
<A href="www.joeportal.au/cang/send.php?n=001&t=urgent" clicca qui la spedizione!</A>
```

- Scrivi un codice per un form che chiami lo stesso programma passando gli stessi parametri.
- Scrivi il programma chiamato leggendo i parametri in modo opportuno.

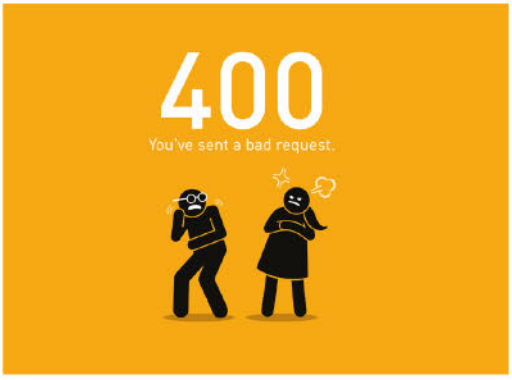
33 Considera la seguente riga:

```
http/1.1 404 NOT FOUND
```

Scrivi il relativo significato e il contesto in cui è utilizzata.

34 Trova gli errori nella seguente richiesta HTTP.

```
get SP /nonna/torta.html SP HTML/1.1 CR LF
CR LF
Accept : text/image
</BODY>
```



35 Descrivi un possibile endpoint creato da un server che gestisce libri, in esecuzione su biblioteca.it.

a. Scrivi il codice HTTP per richiedere il libro con id = 4.
b. Scrivi il codice HTTP per inviare un nuovo libro.
c. Scrivi il codice HTTP per richiedere il libro dal titolo «Pinocchio».

Esercizi in più

The HTTP protocol

Abstract

HTTP is an application-layer Internet protocol used for the realisation of the WWW. By means of a client, HTTP communicates with a server in order to make a request for a resource, typically a Web page. To do this, the client must send a request to the server, which is an ASCII text structured according to specific syntax. The server, an HTTP daemon, receives the request, interprets it and sends to the client a response that, if everything goes well, contains the requested page. The Web page can be either static or dynamic: a static page is an HTML file that resides on a server and is retrieved and sent to the client upon request; a dynamic page is generated dynamically via executable code (from either the client or the server). If it is server side, it is generated when required and typically varies according to parameters that the client sends to the server. A dynamic page is generally used when data must be accessed through a DBMS. In fact, a generic application is constituted by at least three conceptually different layers: the user interface, an operation logic (application engine) and access to data.

Questions

Answer all questions

1 What do we mean by "three tier architecture"?

2 Describe HTTP request syntax

3 Explain the difference between the GET method and the POST method

4 What are the advantages of using a dynamic Web page?

Choose the correct answer

5 The QueryString l:

- a is used for accessing data in a DBMS
- b is an environment variable
- c is a part of the HTTP request
- d is a part of the HTTP response

6 The CONTENT_LENGTH content

- a is used for the access to the interface with the user
- b is used in the HTTP response
- c is used with the POST method
- d is used with the GET method

7 An URI is:

- a a string that uniquely identifies a resource on the Internet
- b an HTTP method
- c a response from the HTTP server
- d an HTTP status code

8 The HTTP protocol

- a is an application layer protocol
- b is a network layer protocol
- c is used for the development of Web pages
- d is used to write dynamic pages

Crosswords

Across

2 Identifies a resource on the Internet

6 HTTP method used to send an Internet service resource for exchanging HTML files

8 Indicates that each HTTP request is independent from others

10 Sent from the client to the server

Down

1 Used with GET for parameter passing

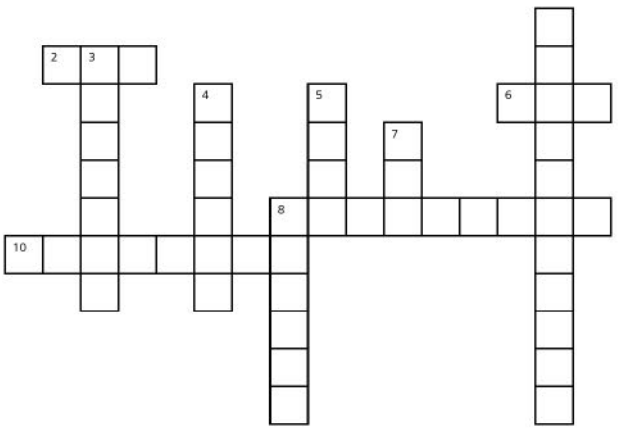
3 Sent from the server to the client

4 Sends a request to the server

5 HTTP method used to send a resource

7 HTTP method used to request a resource

8 Sends a response to the client

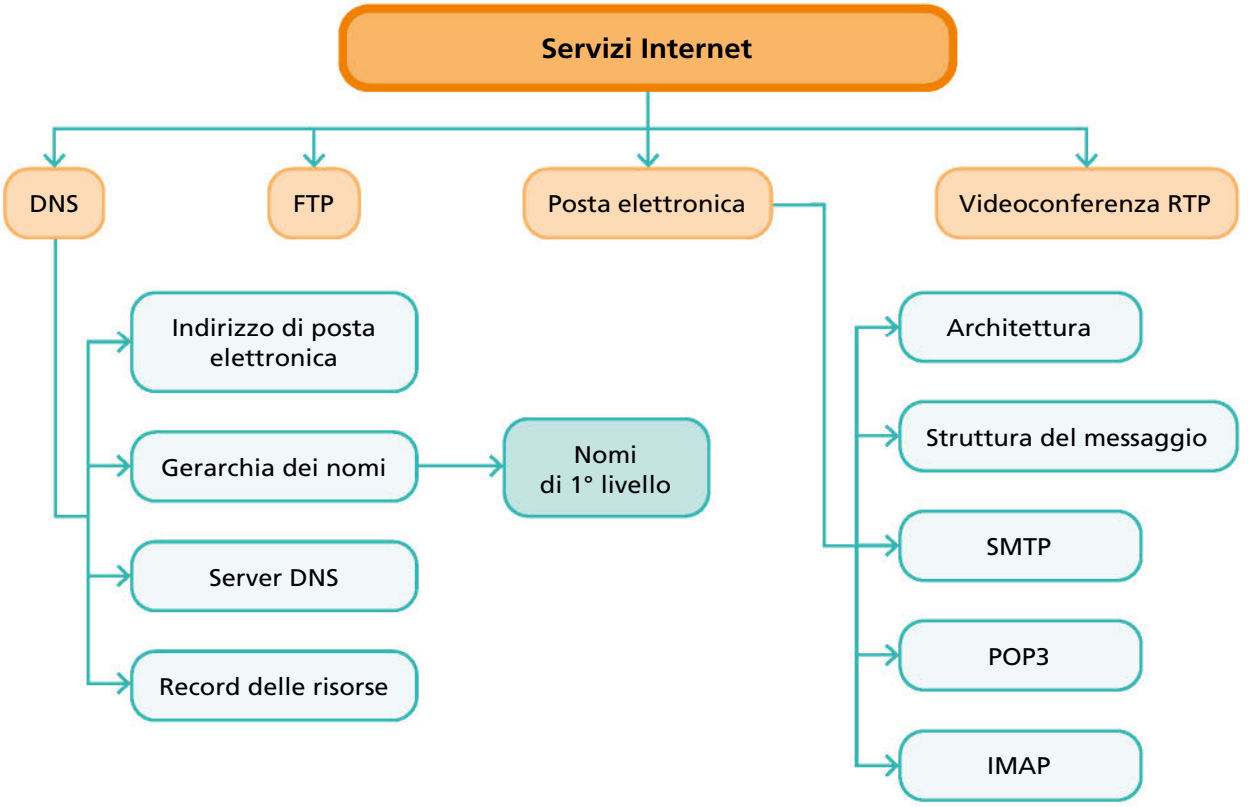




Unità

2

Servizi Internet



Visione d'insieme

- Standard Internet di livello Applicazione.
- Risoluzione dei nomi in Internet: il DNS (Domain Name System).
- La posta elettronica: protocolli SMTP, POP3, IMAP.

1 Introduzione

Navigando su Internet, spesso senza esserne consapevoli, facciamo affidamento su servizi "storici" che hanno preso vita agli inizi, e che rimangono fondamentali ancora oggi. La loro longevità è attribuibile alla capacità di evolversi in risposta alle mutevoli esigenze degli utenti. Prendiamo, ad esempio, i protocolli di posta elettronica come SMTP e POP, originariamente concepiti per utenti con accesso fisso, ai quali si è affiancato IMAP per soddisfare le necessità di utenti sempre più mobili, grazie all'avvento delle tecnologie wireless.
Un altro servizio essenziale, quasi invisibile ai normali utenti, è il Domain Name System (DNS). Questo sistema trasforma il nome di un sito web nel suo specifico indirizzo IP, o per dirla in termini tecnici, "risolve" i nomi. A prima vista, potrebbe sembrare un processo semplice: digitando il nome di un sito, i server DNS traducono il nome del dominio in un indirizzo IP, facilitando così la navigazione. Tuttavia, la realtà è più complessa. Con milioni di dispositivi connessi che richiedono aggiornamenti costanti, sarebbe impraticabile affidarsi a un database centralizzato per gestire tutte le richieste. Il DNS si avvale di un'architettura distribuita, composta da centinaia di server organizzati gerarchicamente, che assicura efficienza e affidabilità.
In questa Unità, ci dedicheremo all'analisi di questi servizi.

2 DNS

Il **Domain Name System** (**DNS**) è il servizio di livello Applicazione che associa al nome di un host in Internet il corrispondente *indirizzo IP* (Figura 1).
Ogni dispositivo collegato alla rete internet ha un indirizzo IP. Poiché questo è un numero che è difficile da ricordare, ai dispositivi è assegnato anche un nome più facilmente memorizzabile per gli utenti della rete.
Per esempio, è molto più facile ricordare il nome *www.wikipedia.it* piuttosto che l'indirizzo IP 108.157.194.27 (Figura 2). È come usare la rubrica del cellulare: non c'è bisogno di ricordarsi un numero di telefono, basta il nome del contatto!

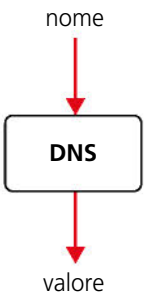


Fig. 1 Il *Domain Name System* è un sistema di risoluzione dei nomi: a fronte di un nome, restituisce un valore.

```
C:\>ping www.wikipedia.it

Esecuzione di Ping d2x2r9xi9rd3sc.cloudfront.net [108.157.194.27] con 32 byte di dati:
Risposta da 108.157.194.27: byte=32 durata=7ms TTL=246
Risposta da 108.157.194.27: byte=32 durata=7ms TTL=246
Risposta da 108.157.194.27: byte=32 durata=7ms TTL=246
Risposta da 108.157.194.27: byte=32 durata=6ms TTL=246

Statistiche Ping per 108.157.194.27:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 6ms, Massimo =  7ms, Medio =  6ms
```

Fig. 2 L'indirizzo IP di www.wikipedia.org rilevato da `Ping`.

Inizialmente, quando su Internet risiedevano solo poche centinaia di calcolatori, la risoluzione dei nomi era gestita manualmente tramite una tabella, chiamata *hosts.txt*, con la corrispondenza nome-indirizzo che veniva inviata per posta agli amministratori degli host. In questo modo la risoluzione della denominazione era realizzata con una procedura che cercava il nome del calcolatore nella copia locale della tabella e restituiva l'indirizzo corrispondente. Verso la metà degli anni Ottanta del secolo scorso si è affermato il servizio DNS, in grado di supportare il notevole aumento di sistemi collegati. Il sistema non è concentrato su un'unica macchina che contiene tutti i nomi e i rispettivi indirizzi, ma è organizzato in un grande database distribuito.

Pit Stop

1 A che cosa serve il DNS?

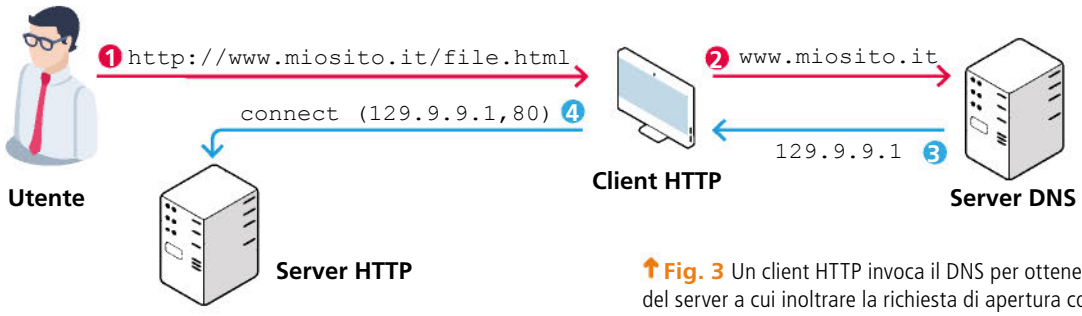


Fig. 3 Un client HTTP invoca il DNS per ottenere l'indirizzo IP del server a cui inoltrare la richiesta di apertura connessione TCP.

Consideriamo, per esempio, una richiesta HTTP con URL:

`http://www.miosito.it/file.html`

In questo caso, il client HTTP invoca il servizio DNS che, a fronte del nome `www.miosito.it`, restituisce il corrispondente indirizzo IP. A questo punto è stabilita una connessione TCP (**Figura 3**). Il DNS è invisibile all'utente ed è di supporto alle altre applicazioni (HTTP, posta elettronica, ...) per poter associare a un nome logico di un host il corrispondente indirizzo IP.

Il DNS è un protocollo client/server di livello applicazione (**Figura 4**) definito in RFC 1304, 1035 e successivi aggiornamenti. Lavora sulla porta 53 e utilizza UDP come protocollo di livello Trasporto.

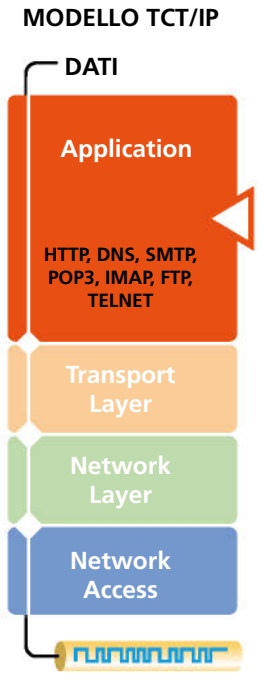


Fig. 4 DNS è un protocollo di livello applicazione.

Struttura gerarchica dei nomi

I nomi utilizzati in Internet identificano un host. Sono costituiti da più etichette (stringhe di caratteri), separate da un punto, facili da ricordare. Per esempio, www.unipd.it è formato da tre etichette: "www", "unipd" e "it".
I nomi sono organizzati in una gerarchia di dominî e sottodomini. La gerarchia è organizzata in livelli ed è rappresentata con una struttura ad albero nella quale la radice è il DNS Root, a ciascun nodo corrisponde un dominio e alle foglie corrispondono i calcolatori, ai quali viene associato un nome (**Figura 5**).

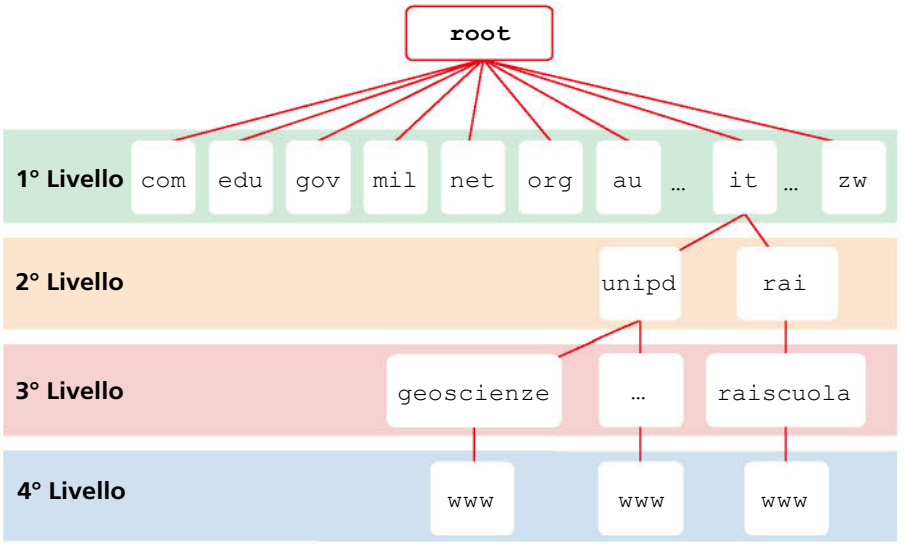


Fig. 5 Albero dei domini: dalla radice discendono i diversi domini. L'estremità di un ramo rappresenta l'host e identifica un terminale o un'entità di rete.

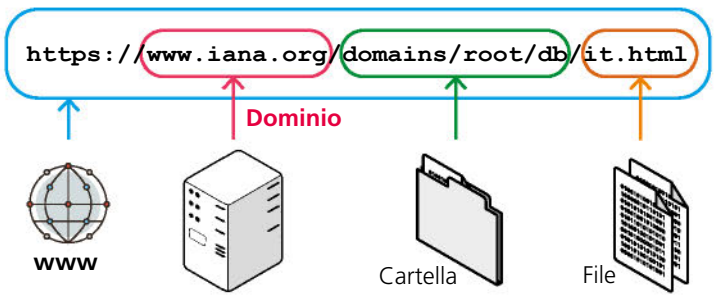
notabene

Un host usato come server web in genere viene chiamato "WWW", ma può avere anche un altro nome.

- **Primo livello**: è il **TLD** (***T**op **L**evel **D**omain*) ed è rappresentato dall'etichetta più a destra. Per questo livello il DNS stabilisce i valori possibili e il loro significato. Ogni TDL può contenere milioni di domini di secondo livello.
- **Secondo livello**: in genere individua un'organizzazione (Società, Università, Azienda, Ente, ...). Ogni dominio di secondo livello può contenere un indefinito numero di domini di terzo livello.
- **Livelli successivi**: specificano via via i sottodomini di terzo livello, quarto livello, fino a individuare uno **specifico host** (ultima etichetta a sinistra del nome).

Consideriamo, per esempio, il nome www.iana.org (Figura 6).
Partendo da destra troviamo:

- org: nome del dominio di primo livello;
- iana: nome del dominio di secondo livello;
- www: nome dell'host.



➜ **Fig. 6** Struttura completa di un indirizzo web: Protocollo: https. Dominio di primo livello (TLD): org. Dominio di secondo livello: iana. Server : www. Cartella: domains/root/db. File in cartella: it.html.

Dominio di primo livello

Come abbiamo visto, i domini di primo livello (TDL - *Top Level Domain*) corrispondono all'etichetta più a destra del nome. Sono divisi in due gruppi:

- **Nazionali**: ccTLD (*country code TLD*). Sono composti sempre da un codice di due caratteri che identifica una singola nazione (secondo lo standard ISO 3166). Per esempio .it (Italia), .fr (Francia). (Tabella 1).

notabene

Alcune organizzazioni utilizzano un nome di dominio internazionalizzato (IDNA – *Internationalizing Domain Names in Applications*) che contiene non solo caratteri ASCII ma anche caratteri Unicode approvati da ICANN. In questo modo si apre la possibilità di utilizzare caratteri alfabetici che non siano latini, come, ad esempio caratteri arabi, ebraici, cinesi, russi e hindi per i nomi dei domini di primo livello.

ccTLD	Nazione
it	Italia
uk	Regno Unito
fr	Francia
va	Città del Vaticano
tv	Tuvalu
us	Stati Uniti (raramente usato)
sm	San Marino
za	Sud Africa

➜ **Tab. 1** Esempio di domini di primo livello nazionali.

- **Generici**: gTLD (*generic* TLD). Sono usati per scopi generici. Per esempio .com, .gov (Tabella 2). Questi si suddividono in due due sottogruppi:
  – sponsorizzati: sTLD (*sponsored TLD*);
  – non sponsorizzati: uTLD (*unsponsored TLD*).

Alcune osservazioni e curiosità:

- i domini **.mil**, **.edu**, **.gov** esistono solo per gli Stati Uniti. Tutte le università americane sono sotto il dominio edu, gov è usato per enti governativi, mil per enti militari;
- le università inglesi appartengono al sottodominio **.ac** (accademico) del dominio **.uk** (United Kingdom);
- **.com** è usato da organizzazioni commerciali;
- **.net** è usato per organizzazioni di gestione della rete;
- **.org** è usato da enti privati (per esempio enti no-profit, associazioni non governative);
- **.gb** (Gran Bretagna) non include l'Irlanda del Nord;
- Altri TLD introdotti da ICANN: **.aero**, **.biz**, **.coop**, **.info**, **.museum**, **.name**, **.pro**;
- Il dominio **.tv** è il nome di primo livello nazionale di Tuvalu, ma risulta molto popolare, a causa dell'abbreviazione, tra le emittenti televisive di tutto il mondo. Tuvalu è una piccola nazione insulare di soli 26 chilometri quadrati, della Polinesia, nell'oceano Pacifico, a metà strada tra le Hawaii e l'Australia.

Gestione dei TLD

I TLD sono gestiti da **IANA** (***I**nternet **A**ssigned **N**umbers **A**uthority*) e da ICANN (***I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers*). IANA si occupa della gestione tecnica, come per esempio l'aggiunta o la rimozione dei nomi. ICANN ha un compito più generale e si occupa di sorvegliare il registro dei nomi e garantirne la corretta gestione.

I nomi sono liberamente scelti da chi desidera registrare un proprio dominio in Internet, ma devono essere preventivamente accettati e associati a un indirizzo IP da ICANN, che assegna gli indirizzi IP e gestisce i root server DNS dove sono registrati i domini, la cui lista è conservata e aggiornata IANA. ICANN ha ufficializzato la liberalizzazione di domini di primo livello che potranno essere scelti arbitrariamente. Ad esempio, si possono richiedere domini .app, .bank o .web; oppure si possono ottenere domini legati ai marchi, come .ferrari, .fiat o .gucci. Alcune aziende o organizzazioni hanno ottenuto l'autorizzazione da ICANN per gestire TLD personalizzati. Tra questi, quello del CERN di Ginevra: `https://home.cern/`.

notabene

Concretamente l'assegnazione degli indirizzi è fatta dai Registri Regionali di Internet (*Regional Internet Registry*):

- ARIN (*American Register for Internet Numbers*) (`www.arin.net`)
- RIPE (*Reseaux IP Europeans*) (`www.ripe.net`)
- APNIC (*Asia Pacific Network Information Center*) (`www.apnic.net`)
- AfriNIC (*African Network Information Centre*) (`www.afrinic.net`)
- LACNIC (*Latin America and Caribbean Network Information Centre*) (`www.lacnic.net`)

Tab. 2 Esempio di domini di primo livello generici.

gTLD			
sTLD		**uTLD**	
.aereo	per l'industria dei trasporti aerei	**.com**	per le organizzazioni commerciali
.asia	per la comunità dell'Asia	**.net**	per le infrastrutture di rete
.coop	per le cooperative	**.org**	per le organizzazioni
.museum	per i musei	**.info**	per i siti informativi
.jobs	per siti sull'impiego	**.biz**	per business
.edu	per siti di educazione scolastica superiore	**.name**	per le famiglie e i singoli
.gov	per siti governativi e le loro agenzie negli USA	**.pro**	per alcune professioni
.mil	per le forze armate USA	**.com**	per le organizzazioni commerciali
.int	per le organizzazioni internazionali		

Pit Stop

2 Chi gestisce i domini di primo livello?

In Italia, il registro deputato all'assegnazione dei nomi di primo livello con dominio .it è il NIC (`www.nic.it`), organo del Consiglio Nazionale delle Ricerche con sede a Pisa. Il registro è responsabile della gestione del name server ".it".
Il servizio WHOIS permette, tramite l'interrogazione di appositi database, di ottenere anche le informazioni del gestore a cui appartiene l'indirizzo.

Esempio 1

Utilizzo di WHOIS per avere informazioni su un nome internet

Nella barra degli indirizzi digitare `https://who.is/` oppure servirsi di `www.trovaip.it`, un sito che sfrutta WHOIS.
Cercare informazioni sull'indirizzo IP: `142.250.114.94`
Si ottiene il seguente risultato:

```
Indirizzo IP cercato: 142.250.114.94
Hostname: rr-in-f94.1e100.net
Posizione dell'IP 142.250.114.94:
Mountain View, (United States) (con la relativa mappa geografica)


Whois dell'indirizzo IP 142.250.114.94:
RESULTS FOUND: 2

-------------
Lookup results for 142.250.114.94 from whois.lacnic.net server:

NetRange:       142.250.0.0 - 142.251.255.255
CIDR:           142.250.0.0/15
NetName:        GOOGLE
NetHandle:      NET-142-250-0-0-1
Parent:         NET142 (NET-142-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS15169
Organization:   Google LLC (GOGL)
RegDate:        2012-05-24
Updated:        2012-05-24
Ref:            https://rdap.arin.net/registry/ip/142.250.0.0
OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints
                are located in the following links.
Comment:
Comment:        To report abuse and illegal activity:
                https://www.google.com/contact/
Comment:
```

```
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL
OrgTechHandle: ZG39-ARIN
OrgTechName: Google LLC
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com
OrgTechRef: https://rdap.arin.net/registry/entity/ZG39-ARIN
OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-650-253-0000
OrgAbuseEmail: network-abuse@google.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE5250-ARIN
```

Cercare informazioni sul dominio: `www.google.it`
Si ottiene il seguente risultato:

```
Informazioni su google.it:

Indirizzo IP 1: 142.250.114.94
Hostname: rr-in-f94.1e100.net
Nameserver 1: ns4.google.com
Nameserver 2: ns1.google.com
Nameserver 3: ns2.google.com
Nameserver 4: ns3.google.com
Rete: GOOGLE
Provider: Early registration addresses
```

Come funziona il DNS

Le zone DNS

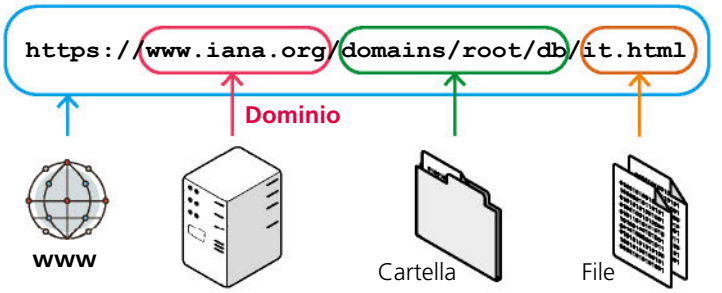
Tecnicamente il DNS è composto da una rete di name server. Il collegamento tra name server e nomi di dominio è fatto tramite le zone DNS. Una **zona DNS** è una parte dell'albero della gerarchia dei nomi, gestita da una specifica organizzazione, un'unità amministrativa. Non va confusa con il dominio o con un name server specifico. Una zona DNS gestisce almeno un dominio e i suoi eventuali sottodomini che possono essere a loro volta delle zone autonome.
Per esempio, i domini di primo livello costituiscono una zona gestita da ICANN. Le informazioni DNS di una zona sono memorizzate in un **DNS zone file**, un file di testo archiviato nel file system di un server. La struttura del file, definita in RFC 1035, è organizzata in righe.

Server DNS

DNS è un'applicazione client/server: i client DNS inviano le richieste a un server DNS (distributore di nomi). In generale il DNS è un sistema in cui, a fronte di un nome, il server DNS restituisce un valore. A volte il valore costituisce l'informazione finale, cioè l'indirizzo IP cercato, altre volte invece è un puntatore (indirizzo IP) a un altro server cui il client deve inviare un'altra richiesta. Si può pensare al DNS come a una gerarchia di distributori di nomi più che a una gerarchia di domini (Figura 7). Ogni unità amministrativa decide se usare uno o più server relativamente a un dominio.

notabene

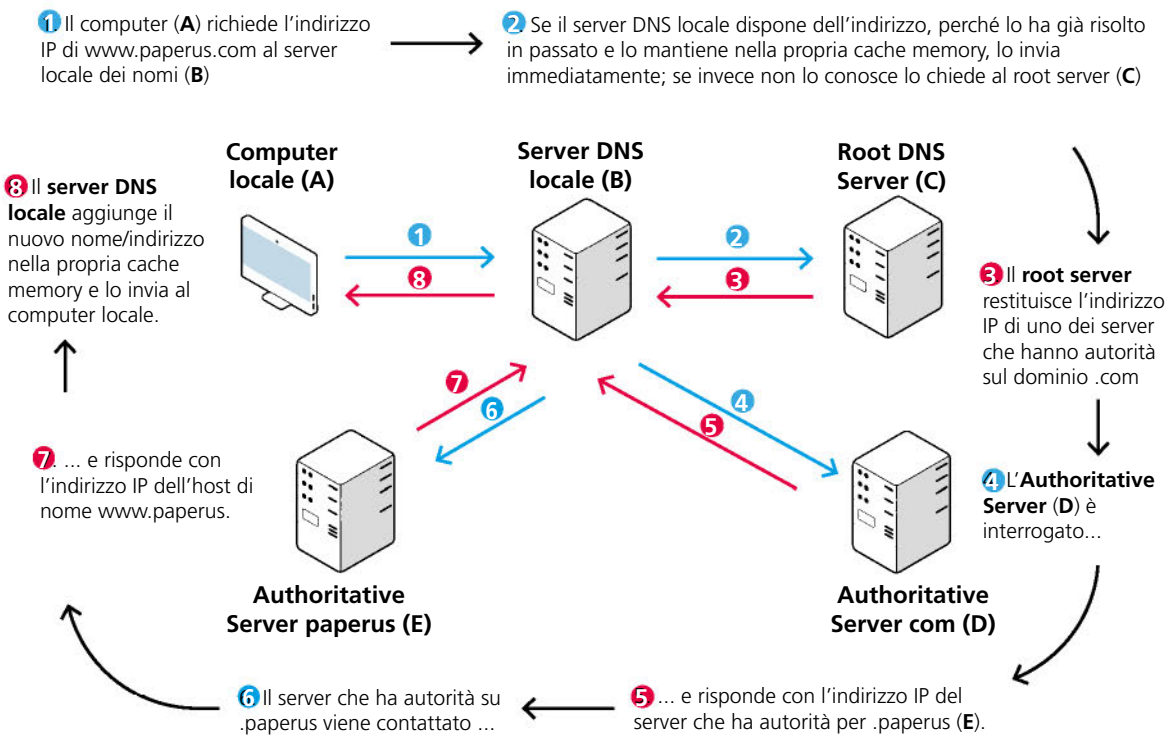
Le informazioni contenute in ogni zona sono organizzate in due o più server DNS (distributori di nomi), in modo tale che le informazioni siano disponibili anche in caso di guasto di uno dei due.



➜ **Fig. 7** Gerarchia dei distributori di nomi.

I server dei nomi sono organizzati nel seguente modo (**Figura 8**):

- **Server dei nomi locali** (*Local Name Server*). Ogni organizzazione (università, azienda privata,...) ha un server dei nomi locale. La richiesta di risoluzione di un nome è inviata al server dei nomi locali il cui indirizzo IP è inserito a mano nell'host. In genere questo server è nella rete locale dell'host. Il server dei nomi locali ha l'indirizzo del root server.
- **Server dei nomi radice** (*Root Name Server*). Quando il server dei nomi locali non può soddisfare immediatamente la richiesta di un host, assume il ruolo di client DNS e invia la richiesta al Root Name Server. Si possono verificare due casi:
  - Il root server ha le informazioni relative al nome richiesto, le invia al server dei nomi locale che invia la risposta all'host che ha fatto richiesta.
  - Il root server non ha le informazioni richieste, ma conosce l'indirizzo IP di un server dei nomi assoluto a cui chiedere.



➜ **Fig. 8** Esempio di risoluzione dei nomi iterativa.

- **Server dei nomi assoluto** (*Authoritative Name Server*). È un server che ha le informazioni sulla corrispondenza tra nome dell'host e il suo indirizzo IP. In genere per ogni host ci sono almeno due server name assoluti per far fronte a eventuali malfunzionamenti.

La risoluzione del nome può essere:

- **ricorsiva**: in cui ogni name server manda una richiesta ad un altro name server che manderà una richiesta ad un successivo server;
- **iterativa**: in cui è il local name server a gestire gli altri server coinvolti.

Ogni host ha una propria cache in cui memorizza i nomi risolti più recentemente. Quando l'host necessita della risoluzione di un nome, prima di tutto controlla se l'IP corrispondente è già nella sua cache. In questo caso il problema è risolto, senza la necessità di dover interrogare i vari server DNS.
Per il sistema operativo Windows, il comando per visualizzare i nomi/IP presenti nella cache di un host è `ipconfig /displaydns` (**Figura 9**), il comando per svuotare la cache è `ipconfig /flushdns` (**Figura 10**).

```
C:\Users>ipconfig /displaydns

Configurazione IP di Windows

    www.googleapis.com
    ----------------------------------------
    Nome record . . . . . : www.googleapis.com
    Tipo record . . . . . : 1
    Durata (TTL). . . . . : 94
    Lunghezza dati. . . . : 4
    Sezione . . . . . . . : Risposta
    Record A (Host) . . . : 142.251.209.42
```

Fig. 9 Comando per visualizzare la cache su un host.

```
C:\Users>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Users>ipconfig /displaydns

Configurazione IP di Windows
```

Fig. 10 Comando per svuotare la cache su un host.

Record delle risorse
Le informazioni mantenute nei server name sono organizzate in record chiamati **record delle risorse** o record DNS. Un record delle risorse è costituito dai seguenti campi:

`<Name, Value, Type, Class, TTL>`

dove:

- **Name** è il nome fornito dal client al server DNS;
- **Value** è il valore restituito dal server DNS al client;
- **Type** specifica come il Value deve essere interpretato (**Tabella 3**);
- **Class** indica la classe di appartenenza del record delle risorse (IN significa che la classe è Internet). È opzionale;
- **TTL** (*Time To Live*) indica per quanto tempo, in secondi, il record è valido. Quando TTL scade, il server deve eliminare il record dalla sua cache. È opzionale.

Type = A	Indirizzo IPv4 del dispositivo
Type = MX	(*Mail eXchange record*) fornisce il nome del dominio del server di posta (mail server)
Type = NS	(*authoritative Name Server*) fornisce il nome del dominio per un calcolatore che sa come risolvere i nomi all'interno del dominio specificato
Type = CNAME	fornisce il nome canonico di un calcolatore; è utilizzato per definire nomi alternativi
Type = AAAA	indirizzo IPv6 del dispositivo
Type = PTR	permette un *reverse lookup* (risoluzione inversa). Collega un indirizzo IP con il relativo nome di dominio. Esiste un record PTR per ogni indirizzo IP utilizzato nei record A o AAAA
Type = SOA	(*Start of Authority*) fornisce informazioni sulla zona del server DNS. È utile quando è effettuato un trasferimento di zona in cui i file di zona sono copiati su altri server per evitare disservizi
Record TXT	contiene testo leggibile da persone o applicazioni. Si può utilizzare per trasmettere informazioni, per esempio per verificare il titolare di un dominio e aumentare il livello di sicurezza

Tab. 3 Alcuni valori possibili del campo Type del record di risorsa. Il campo Type è obbligatorio e descrive il tipo di record risorsa, mentre i campi TTL e class sono campi opzionali.

In pratica:

- il distributore dei nomi radice (*root server*) contiene una coppia, record NS e record A, relativi a ogni server di secondo livello;
- questi due record, insieme, costituiscono un puntatore che va dal distributore di nomi radice a ciascun server di secondo livello;
- nello stesso modo, ogni dominio di secondo livello contiene coppie di record NS e A, che puntano a distributori di terzo livello, oppure a soli record A che restituiscono l'indirizzo IP;
- l'ultimo livello della gerarchia è un distributore che contiene solo record A, che non punta ad alcun altro server e restituisce direttamente gli indirizzi IP. Nel database di questo livello potrebbero esserci anche record MX (per indicare un server di posta elettronica) o record CNAME per poter assegnare un altro nome al server. Infatti i server hanno un unico indirizzo IP, ma possono avere più nomi (alias) associati allo stesso IP. In generale, a ogni interrogazione il record NS restituisce il nome del server a cui puntare; questo nome è usato come input del record A per ottenere l'IP relativo.

L'esempio seguente mostra la sequenza dei passi da quando un utente clicca su un link fino a quando la pagina richiesta viene mostrata al browser, passando la richiesta al server DNS.

Esempio 2

Una connessione di rete completa

Il trasferimento di una pagina web da server a client con HTTP 1.1 consiste in una serie di passi. Vediamoli.

1. L'utente clicca sul collegamento ipertestuale: `http://www.paperus.org/nonna/applepie.htm` per richiedere la pagina `applepie.htm` che contiene alcune immagini.
2. Il browser ricava il nome del server (`www.paperus.org`) dall'URL e lo fornisce al DNS per ottenerne l'indirizzo IP.
3. Il DNS risponde con l'indirizzo IP: `200.244.244.1`.

4. Il browser richiede una connessione TCP sulla porta 80, al server di indirizzo `200.244.244.1`.
5. Il server accetta la richiesta di connessione.
6. Il browser invia la richiesta HTTP per l'acquisizione del file `applepie.htm` che risiede nella cartella "nonna" con il nome del path (percorso).
7. Il server risponde con la pagina HTML richiesta.
8. Il client riceve il file HTML e lo interpreta e, per ogni immagine di cui trova il riferimento, effettua una nuova richiesta al server ripercorrendo i passi dal numero 5 al 7. (Nel caso le immagini non risiedano nello stesso archivio in cui risiede la pagina HTML, sarà necessario ricorrere ancora al DNS.)
9. Viene rilasciata la connessione TCP.

Messaggi di richiesta e risposta

Il protocollo DNS ha due tipi di messaggi:

- richiesta (*query*) di un client a un server per ottenere informazioni sulle risorse;
- risposta (*response*) di un server a un client che contiene nomi, indirizzi e informazioni aggiuntive.

Entrambi i messaggi, sia di richiesta sia di risposta, hanno lo stesso formato, che comprende un'intestazione e le relative sezioni di richiesta o di risposta (**Figura 11**, **Figura 12**).

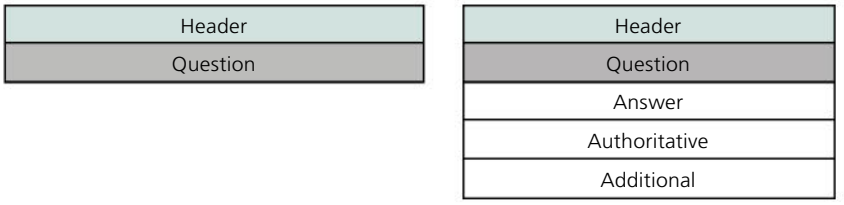


Fig. 11 Entrambi i messaggi di query e di risposta hanno lo stesso formato. La sezione Question è comune a Richieste e Risposte.

- *Header* (intestazione) è di 12 byte e contiene campi e flag che identificano il tipo di messaggio;
- *Question* contiene il nome da risolvere;
- *Answer* include uno o più record con le risposte dal server al client (resolver);
- *Authoritative* fornisce informazioni (nome di dominio) su uno o più server autorevoli per la richiesta-risposta;
- *Additional* fornisce informazioni aggiuntive.

DNS dinamico

In genere il servizio DNS associa un indirizzo IP a un nome di un host.
In questo modo è possibile, per esempio, accedere a un sito web tramite un URL. In questi casi l'indirizzo IP dell'host è statico e quindi, una volta assegnato, non viene più modificato.
Se volessimo, invece, accedere a un dispositivo di una rete locale dall'esterno, per esempio la nostra rete domestica, le cose sarebbero diverse. Pensiamo alla domotica e alla possibilità di controllare antifurto, riscaldamento, telecamera e altri dispositivi da remoto. Spesso la connessione domestica a Internet ha un indirizzo IP dinamico che cambia periodicamente. Gli ISP utilizzano indirizzi IP dinamici perché sono più economici e permettono di recuperare gli indirizzi IP non utilizzati.

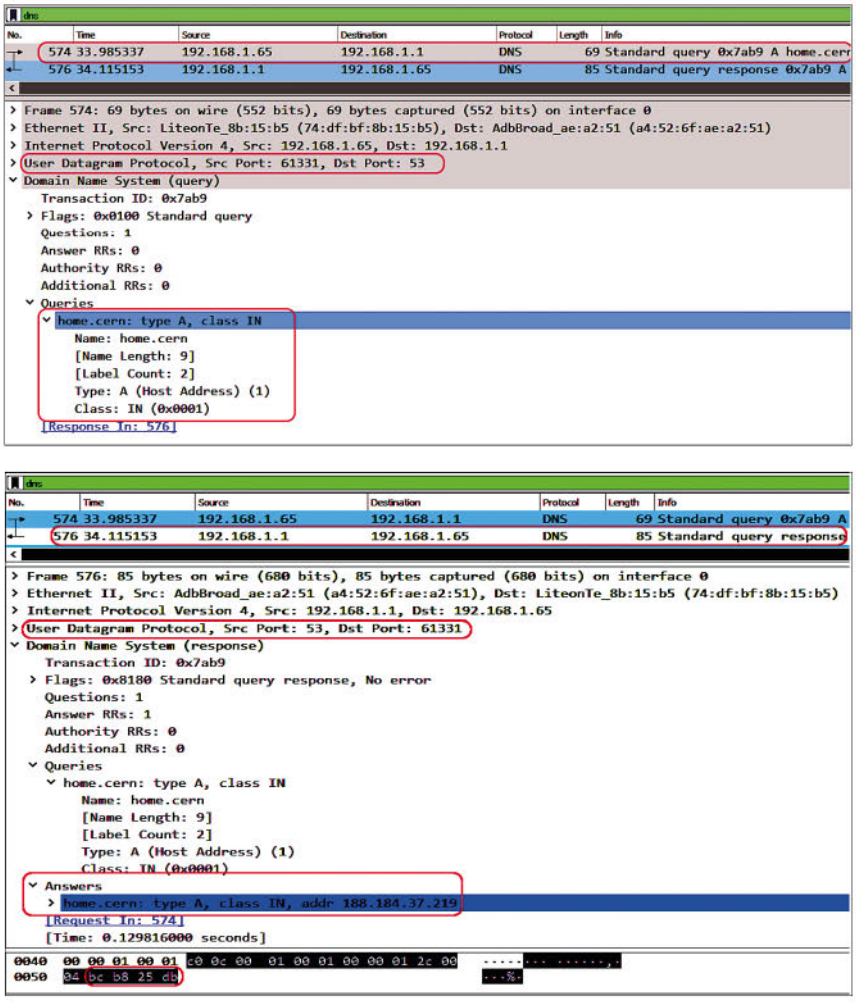


Fig. 12 a. La richiesta DNS della home page di `www.cern.org`. **b.** La risposta del DNS alla richiesta della home page di `www.cern.org` con nome (`home.cern`), tipo A (1), classe IN (1) e indirizzo IP `188.184.37.219` (bc b8 25 db espresso in esadecimale).

notabene

Ci sono ISP che forniscono DDNS, alcuni gratuiti e altri a pagamento. A volte il servizio DDNS è implementato direttamente sul router per uso privato.

È come se cambiassimo continuamente il numero di telefono: se dobbiamo effettuare telefonate non ci sono problemi, ma se dobbiamo riceverne, diventa necessario comunicare continuamente il nuovo numero agli altri.
Per poter associare il nome fisso di un host a un indirizzo IP dinamico, occorre usare il **servizio DNS dinamico** (**DDNS**).
Per utilizzare il DNS dinamico occorre:

- scegliere opportunamente un provider di servizi DDNS in grado di mantenere l'aggiornamento dei dati del DNS con il nome dell'host desiderato;
- installare un client sul dispositivo con IP dinamico. Il client DDNS rileva il cambiamento di IP e lo comunica al server DDNS che aggiornerà il record DNS.

Il DDNS è utile, per esempio, nei seguenti casi:

- accesso remoto. I dipendenti di un'azienda possono accedere a risorse interne all'azienda da remoto utilizzando un nome di dominio fisso. È utile per le organizzazioni con lavoratori remoti, filiali o dipendenti in movimento;
- servizi di hosting. È possibile utilizzare indirizzi IP dinamici, anziché quelli statici, più costosi per servizi in hosting quali siti web, server FTP, ...;
- monitoraggio remoto. È possibile gestire sistemi di monitoraggio da remoto in tempo reale, come telecamere di sorveglianza.

Galleria
DNS con Wireshark

notabene

Nell'Unità 10, relativa all'IoT, vedremo come utilizzare il DDNS combinato con il port forwarding per accedere da remoto a servizi IoT interni a una rete.

La parola a ... Ray Tomlinson



All'inizio degli anni Settanta del secolo scorso, Ray Tomlinson, un ingegnere elettronico e programmatore americano che lavorava alla rete ARPANET, studiò il sistema per inviare facilmente messaggi da un computer a un altro. Nacquero la posta elettronica e il protocollo SMTP. Tomlinson associò al servizio di posta anche il simbolo @, ora utilizzato da quasi 4 miliardi di account di posta elettronica nel mondo. Ray ha descritto la sua invenzione dicendo: «Vedo l'e-mail utilizzata, in larga misura, esattamente nel modo in cui l'avevo immaginata. In particolare, non è strettamente uno strumento di lavoro o qualcosa di puramente personale. Ognuno la usa in modi diversi, ma la usano nel modo che ritengono funzioni per loro».

3 La posta elettronica

La posta elettronica è uno dei primi servizi internet, già esistente fin dagli anni Settanta, ed è un metodo di comunicazione testuale, per inviare dei messaggi in formato digitale tramite la rete Internet. È attualmente ancora molto utilizzata, soprattutto in ambito aziendale.
Rispetto alla versione iniziale, sono state aggiunte delle migliorie per adattarla alle esigenze legate allo sviluppo tecnologico: mobile, sicurezza, utilizzo del Web,....

Architettura del sistema di posta elettronica

La posta elettronica è un mezzo di comunicazione **asincrono** in cui la comunicazione può avvenire anche se il mittente e il destinatario del messaggio non sono contemporaneamente connessi alla rete Internet.
Il funzionamento del sistema di posta è diviso in due parti (Figura 13):

1. invio del messaggio:
   - **submission**: il messaggio (mail) è inviato dal mittente a un **server di posta** che è sempre in esecuzione (**server di posta in uscita**). In genere questo server è reso disponibile da un fornitore di servizi. Qui il messaggio è memorizzato nella casella di posta del mittente (Mail Box);
   - **relay**: successivamente il messaggio è trasferito al server del destinatario (**server di posta in arrivo**) e qui memorizzato nella casella di posta del destinatario.
2. **Lettura del messaggio**: Il destinatario legge dalla sua casella di posta i messaggi che gli sono arrivati.

notabene

Altri sistemi di comunicazione in rete, come la chat o la videoconferenza, sono invece sistemi sincroni perché mittente e destinatario interagiscono tra loro durante la conversazione.

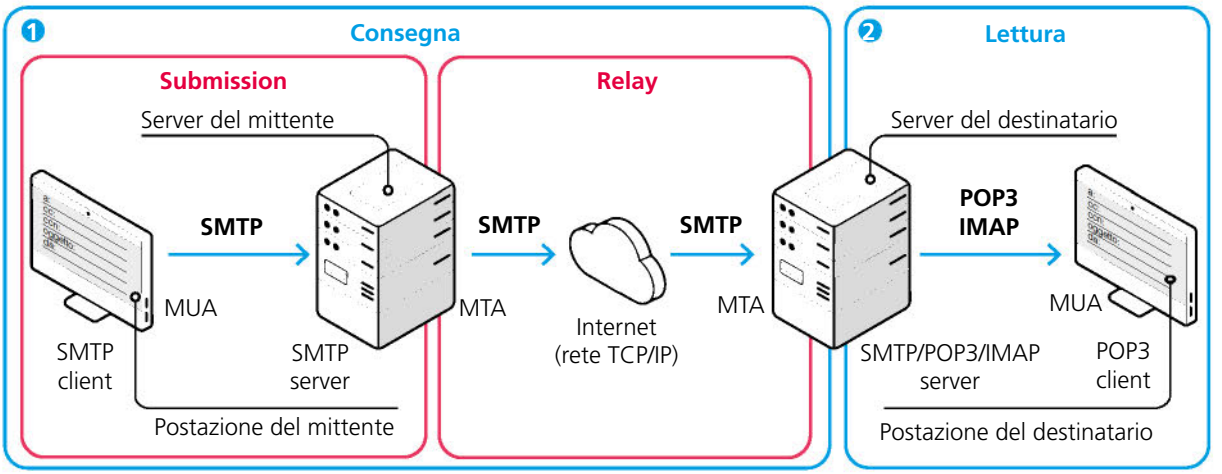


Fig. 13 Architettura del sistema di posta elettronica. La consegna è fatta con SMTP, le lettura con POP3 oppure IMAP.

notabene

Prima di essere consegnata al server del destinatario la mail potrebbe passare da più server.

Occorre specificare che:

- l'invio del messaggio (submission e relay) è fatto tramite protocollo SMTP;
- la lettura del messaggio è fatta con protocollo POP3 oppure con protocollo IMAP;
- i programmi usati per gestire i messaggi dal mittente e dal destinatario (creare, cancellare, modificare, ...) sono chiamati **Mail User Agent** (**MUA**);
- i programmi usati per trasferire i messaggi tra i server sono chiamati **Mail Transfer Agent** (**MTA**).

Pit Stop

3 Come è strutturato un sistema di posta elettronica?

Client di posta

Un **client di posta** è usato da un utente per la gestione delle mail. Può essere:

- un programma che salva tutte le e-mail in arrivo sul computer. In questo caso l'utente può gestire la posta anche senza la connessione a Internet;
- Webmail, un programma eseguito via Web utilizzando un servizio di un provider. Previa registrazione al servizio, l'utente che dispone di una connessione internet, può consultare e gestire le mail da qualunque dispositivo e da qualunque luogo.

Per la scelta di un client di posta elettronica occorre considerare alcune caratteristiche tra le quali:

- **sicurezza**. Un client di posta deve fornire garanzia di sicurezza utilizzando sistemi di crittografia e autenticazione per proteggere le informazioni, e una costante manutenzione e aggiornamento delle contromisure relative alle nuove minacce e vulnerabilità;
- **funzionalità**. Un client deve avere le funzionalità di cui l'utente necessita. Per esempio la gestione di più account, la gestione di una rubrica, la possibilità di invio posticipato, la sincronizzazione con un calendario, la gestione della posta indesiderata (spam), l'archiviazione organizzata, la possibilità di utilizzo su più piattaforme e dispositivi;
- **interfaccia**. Un client deve essere semplice da usare;
- **assistenza e continuità del servizio**. Il servizio non deve avere interruzioni, né perdite di messaggi, e deve garantire l'assistenza tecnica.

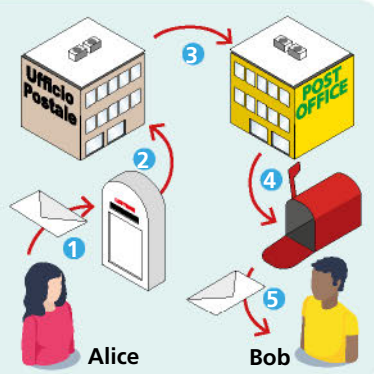
Esempi di client di posta sono: Mozilla Thunderbird multipiattaforma, Microsoft Outlook per Windows, Mail per macOS, iOS e watchOS, Outlook per Windows.

Esempi di servizi di posta sono: Gmail, Libero Mail, Tiscali Mail, iCloud Mail...

Comprendi con l'analogia

La posta elettronica come la posta ordinaria

La posta elettronica, che opera attraverso Internet, è molto simile alla posta ordinaria. Come nella posta ordinaria l'autore del messaggio scrive il testo e lo inserisce in una busta con l'indirizzo del destinatario. Lo "imbuca" nella cassetta per le lettere (che nel caso specifico corrisponde a inviarlo al proprio server di posta con cui si è stipulato un contratto). Il servizio postale penserà a inoltrare la lettera fino a inserirla nella mail-box del destinatario che prenderà la lettera e la metterà in un cassetto della scrivania, oppure la terrà in tasca per leggerla quando vuole.



Struttura di un messaggio

Una e-mail è formata da tre parti (Figura 14):

1. **Busta** (envelope)
2. **Intestazione** (header)
3. **corpo del messaggio** (body)

La **busta** è un testo ASCII che contiene l'indirizzo del mittente e l'indirizzo del destinatario utili agli agenti di trasferimento (sui server) per recapitare il messaggio. L'**intestazione** è testo ASCII e contiene i campi obbligatori *indirizzo mittente* e *indirizzo destinatario*, e altre informazioni facoltative, utili agli agenti utente, per permettere al destinatario di rispondere, archiviare, eliminare il messaggio. L'intestazione è costituita da più campi, ognuno su una riga diversa, della forma `<nome campo>: valore`.

notabene

L'agente utente costruisce il messaggio e lo passa all'agente di trasferimento, che usa i campi d'intestazione per costruire la busta.

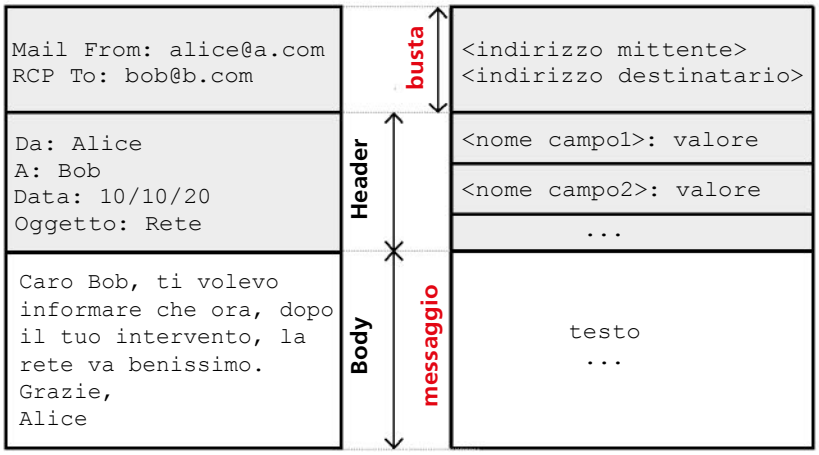


Fig. 14 Formato di una e-mail: busta – intestazione – corpo.

La Tabella 4 riassume alcuni campi facoltativi presenti nell'intestazione.

Tab. 4 Campi facoltativi dell'intestazione.

Campi facoltativi	Descrizione
Subject: (*Oggetto:*)	Contiene una breve descrizione dell'argomento in discussione nel messaggio
Date: (*Data:*)	Data e ora della scrittura del messaggio
Cc:	Carbon copy o Copia carbone. Indirizzo dei destinatari secondari
Bcc: (*Ccn:*)	Blind carbon copy o Copia carbone nascosta. Destinatari secondari non visibili al destinatario
Reply-to: (*Rispondi a:*)	Indirizzi a cui inviare la risposta
Return-path:	È utilizzato per identificare un percorso di ritorno al mittente: è aggiunto dall'agente di trasferimento
Altri campi possono essere aggiunti da programmi di controllo dei messaggi. Per esempio, il campo Received viene aggiunto da ciascun server SMTP che fa transitare il messaggio, indicando l'indirizzo IP e altre informazioni di servizio utili a tracciarne il percorso. È inoltre possibile definire delle intestazioni personalizzate nella forma `X-nomecampo:valore`. Queste intestazioni vengono utilizzate per informare il programma ricevente o il lettore stesso in merito a particolari situazioni:	
X-Priority: 1,	Per indicare un'alta priorità del messaggio
X-Mailer: *client manual…*	Per indicare che l'invio del messaggio è avvenuto manualmente, per esempio tramite Telnet

notabene

Il formato dell'intestazione è definito in RFC 822, quindi le intestazioni sono chiamate «intestazioni RFC 822» o semplicemente «intestazioni 822».

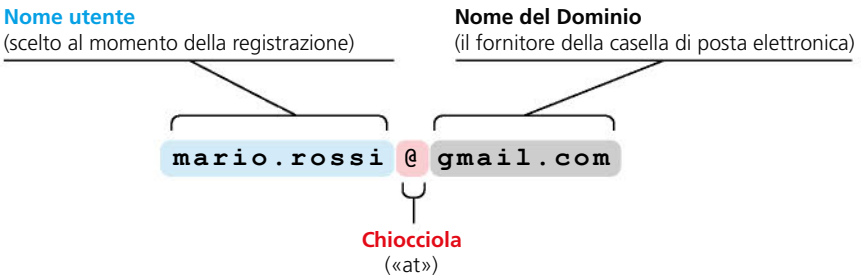
Il **corpo** contiene il messaggio vero e proprio destinato al lettore. Originariamente era codificato in ASCII a 7 bit, ma poi è stato esteso per supportare allegati multimediali, definiti tramite lo standard MIME (*Multipurpose Internet Mail Extensions*), di cui parleremo più avanti.

Indirizzo di posta elettronica

Ogni utente può avere una o più mailbox, alle quali accede autenticandosi con username e password. A ogni mailbox è associato un indirizzo univoco, che è una stringa formata da tre parti:

1. **nome utente**. Identifica la posizione finale della mailbox. Può includere una combinazione di lettere, numeri e alcuni segni di punteggiatura. È il nome con cui l'utente si è registrato al servizio di posta;
2. **@** (simbolo "chiocciola", che significa "presso", in inglese "at");
3. **nome server**. Identifica il calcolatore su cui risiede la mailbox. È un nome di dominio oppure un indirizzo IP. Se si usa il nome di dominio, il protocollo SMTP deve usare il DNS per la risoluzione del nome.

Esempi:



Pit Stop

4 Come è fatto un indirizzo di posta elettronica?

Riepiloghiamo le operazioni che sono effettuate per inviare un messaggio di posta elettronica:

- la e-mail è inviata da un client di posta al server di posta del mittente;
- Il server mittente usando **SMTP** legge nell'envelope della e-mail l'indirizzo del destinatario, e invoca il **DNS** fino a trovare il server **MX** associato al dominio del destinatario, al quale è consegnata la mail nella casella del destinatario;
- Il destinatario può scaricare la e-mail sul proprio dispositivo quando lo desidera utilizzando **POP3**, oppure può lasciarla nella sua casella e accedervi da qualsiasi dispositivo via Web utilizzando **IMAP**.

notabene

Il simbolo «@», noto anche come «a commerciale» o «chiocciola», risale all'antichità, ed è l'unione delle lettere «a» e «d», a formare la preposizione latina *ad*, cioè «verso», nel senso di moto a luogo.

Per continuare l'analogia con il sistema postale tradizionale, immaginiamo che Alice scriva un messaggio a Bob (**Figura 15**).

- Il messaggio di posta che Alice spedisce a Bob è inviato con il protocollo SMTP (*Simple Mail Transfer Protocol*) al server del proprio provider (1).
- Il server locale individua l'indirizzo del server remoto di Bob servendosi del servizio DNS (2 e 3).
- Il messaggio è inoltrato al server su cui risiede la casella postale di Bob (4) e qui memorizzato.
- Dalla propria postazione personale Bob si connette, tramite il protocollo POP3 (Post Office Protocol) o IMAP (Internet Mail Access Control), alla propria casella di posta e scarica il messaggio sul proprio computer (5).

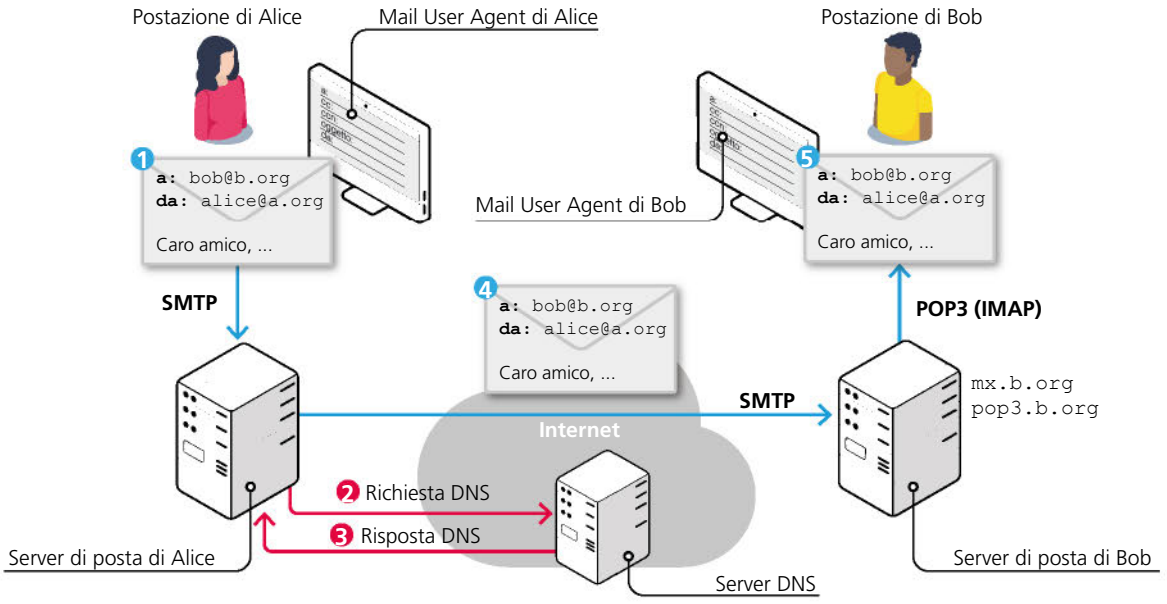


Fig. 15 Il percorso del messaggio di posta elettronica dal computer di Alice a quello di Bob, passando per i server di posta e sfruttando i protocolli SMTP e POP3.

MIME (Multipurpose Internet Mail Extensions)

Il formato ASCII inizialmente usato per i messaggi di posta elettronica, si è rivelato ben presto inadeguato e insufficiente per:

- rappresentare una gran varietà di caratteri come le lettere accentate o appartenenti ad alfabeti non latini;
- includere tipi di informazioni non testuali come audio o immagini o file eventualmente compressi.

Per questo motivo è stato proposto lo standard MIME (RFC 1521, RFC 1341 e RFC 822), utilizzato sia per la posta elettronica, sia per HTTP.
L'idea alla base di MIME è quella di continuare a utilizzare la codifica base originaria in ASCII, senza quindi aggiornare i protocolli, ma modificando i programmi di invio e ricezione del messaggio.
In particolare, sono state definite nuove intestazioni:

- "MIME versione", che indica che il messaggio è in formato MIME. Ad esempio: "MIME-Version: 1.0".
- "Content-Type", che specifica la natura del corpo del messaggio.
- RFC 2045, che definisce sette tipi di Content-Type, ciascuno con dei sottotipi. Il valore di questo campo è espresso nella forma "tipo/sottotipo". Ecco alcuni esempi:
  - "Content-Type:text/html";
  - "Content-Type:text/xml";
  - "Content-Type:text/plain".
- "Content Transfer Encoding", che identifica la codifica dei dati. Ciò permette al destinatario la conversione dei dati da ASCII a 7 bit standard al formato previsto in Content-Type.
- "Content Description", una stringa ASCII che identifica il tipo di messaggio (per esempio: «questo messaggio contiene la foto di mia zia»).
- "Content ID", il codice identificativo del contenuto.

notabene

`"Content-Type"` è usato anche come metainformazione nel protocollo HTTP, come abbiamo visto nell'Unità precedente (per esempio `"Content-Type:text/html"`). È infatti stato definito in RFC 2584 quando il Web è diventato popolare.

Vediamo ora due esempi di messaggi di posta elettronica che mostrano, rispettivamente, l'insieme dei campi di cui è composto il messaggio e la codifica di un'immagine trasmessa in allegato.

Esempio 3

Messaggio originale di solo testo («Ciao») con relativo codice, mostrato nella finestra di posta in arrivo di Gmail.

```
Subject: Saluti
From: lanpa <lanpa@gmail.com>
To: lanpa <lanpa@gmail.com>
Content-Type: multipart/alternative; boundary="000000000000a4535e061a9e44b4"

--000000000000a4535e061a9e44b4
Content-Type: text/plain; charset="UTF-8"

Ciao

--000000000000a4535e061a9e44b4
Content-Type: text/html; charset="UTF-8"

<div dir="ltr">Ciao</div>

--000000000000a4535e061a9e44b4--
```

Esempio 4

La figura mostra uno stralcio del codice sorgente di un messaggio con testo scritto in ASCII e un'immagine in formato .jpg ("NATUR0521.jpg") in allegato (*attachment*). Si noti come opera il destinatario, che usa la *Content Transfer Encoding base 64* per codificare il file in formato JPG. Il *Content Type* indica l'azione da compiere per la decompressione del formato JPG.

```
From: pippo@pluto.it
To: pluto@pippo.it
Subject: prova multipart
MIME version: 1.0
Content Transfer Encoding: base 64
Content type:multipart/mixed; Boundary= _NextPart_000_0018_01C5A56C.863505C0
This is a multi-part message in MIME format.
------=_NextPart_000_0018_01C5A56C.863505C0
Content-Type: multipart/alternative;
    boundary="----=_NextPart_001_0019_01C5A56C.863505C0"
------=_NextPart_001_0019_01C5A56C.863505C0
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printablea
ciao , eccoti l'immagine.
.............
------=_NextPart_000_0018_01C5A56C.863505C0
Content-Type: image/jpeg;
    name="NATUR0521.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="NATUR0521.jpg"
/9j/4AAQSkZJRgABAQAAAQABAAD/5QApQUxQSEFfSU5GTwDCAgAAaAAAAAAMAAAAAAAAAHAEAADgC
Ozs7Ozs7Ozs7Ozs7Ozs7.....................................................
```

Protocollo SMTP (Simple Mail Transfer Protocol)

Il protocollo SMTP, pubblicato nel 1981 (RFC 788), poi aggiornato con RFC 821 nel 1982 e ulteriormente modificato nel 1995 con RFC 1869 (Extended SMTP, ESMTP) e nel 2008 con RFC 5321, attualmente in uso, è utilizzato per la consegna del messaggio (Figura 16). È un protocollo client/server che lavora sulla porta 25 e utilizza TCP come protocollo di livello trasporto. Quando la connessione viene stabilita, il client invia il messaggio al server, che lo inserisce nella casella di posta del mittente e poi lo inoltra al server del destinatario.

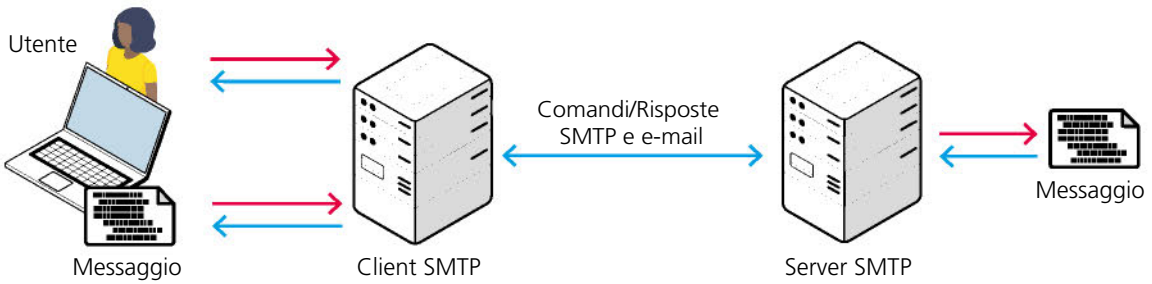


Fig. 16 funzionamento di smtp: il messaggio è inviato dal client di posta al server del mittente e da qui trasferito sul server del destinatario.

La comunicazione tra client e server si articola in tre fasi:

1. **apertura della connessione**: è aperta una connessione TCP, e successivamente il client inizia l'invio dell'e-mail attivando l'handshake (comando `HELO` oppure `EHLO`);
2. **trasferimento dei dati dell'e-mail**: il client invia al server l'header (mittente, destinatario, eventuali altri dati opzionali) e il body dell'e-mail utilizzando una serie di comandi. Il server esegue il Mail Transfer Agent, in base al dominio specificato nell'indirizzo del destinatario;
3. **chiusura della connessione**: il client comunica al server la fine dell'invio dei dati del body e il server chiude la connessione.

Client e Server utilizzano comandi (stringhe di testo):

- il client invia dei comandi, in genere di 4 caratteri;
- il server risponde inviando dei codici di stato di 3 cifre seguiti da una frase opzionale che descrive il codice di stato;
- Le righe di comando e risposta terminano con i caratteri CR-LF (a capo).

Esempi di comandi SMTP, eseguiti dal client, sono: `HELO`, `MAIL FROM`, `RCPT TO`, `DATA`, `QUIT`.

In Figura 17 è riportato il diagramma che mostra il funzionamento di una connessione SMTP con i comandi che, servendosi del livello trasporto, implementano le primitive per aprire e chiudere la connessione e inviare i messaggi di posta. Notiamo subito che, appena stabilita la connessione TCP, il server invia il codice 220 al client per indicare che è pronto a ricevere la posta.

- Appena stabilita la connessione TCP, il **server** invia il codice 220 al client per indicare che è pronto a ricevere la posta.
- Il **client** risponde, aprendo la comunicazione, con il comando `HELO` insieme al nome (o all'indirizzo IP) della macchina su cui si trova.
- Il **server** risponde con l'identità della propria macchina.

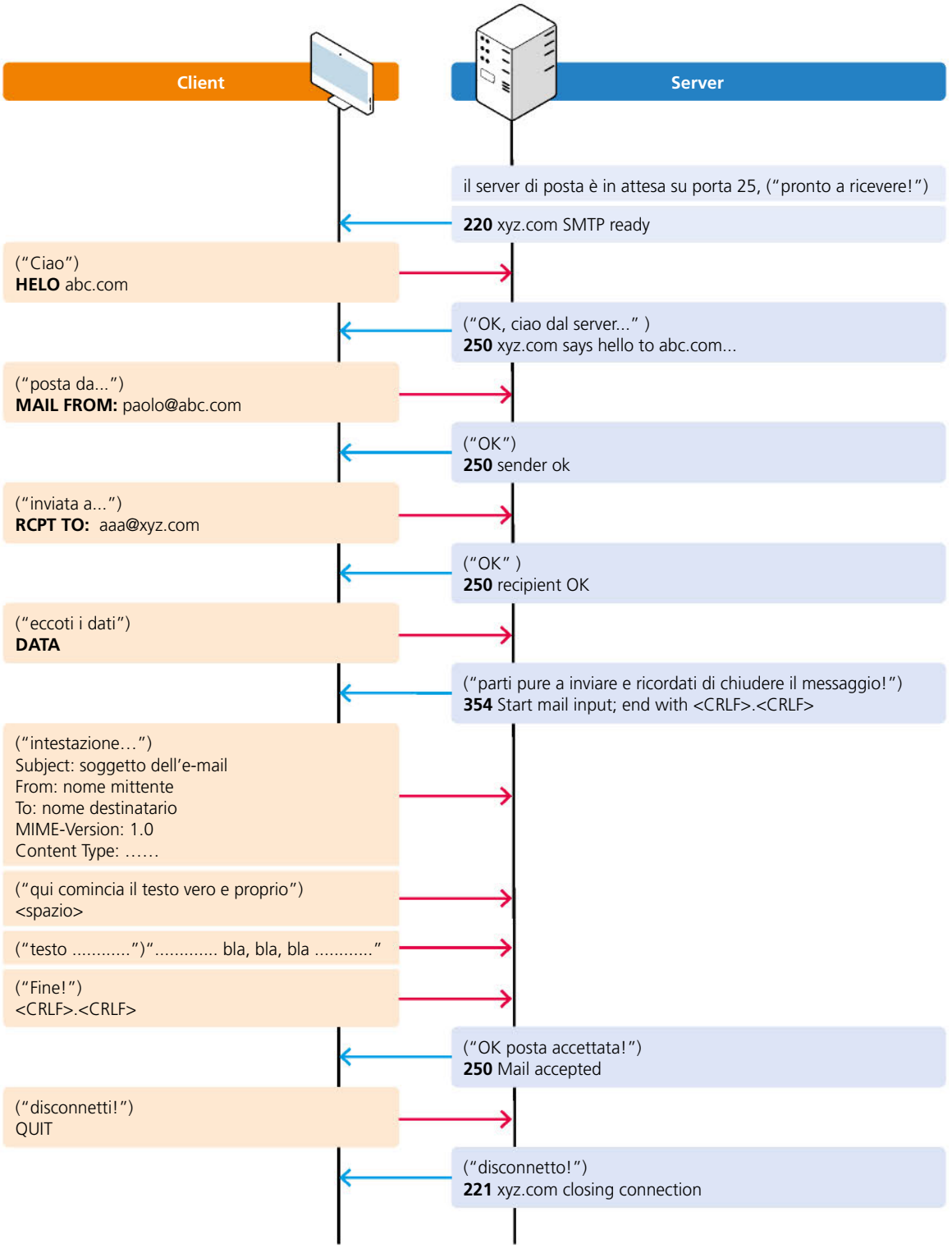


Fig. 17 Una connessione tra client e server basata su SMTP: sono indicati in grassetto i comandi inviati dal client al server con i relativi codici di risposta, tra parentesi il commento al comando.

- Il **client** inizia a inviare l'intestazione della posta con il comando `MAIL-FROM`.
- Il **server** replica con il codice 250, confermando la ricezione.
- Il **client** continua inviando un comando `RCPT TO`.
- Il **server** conferma con il codice 250 (Qualunque altra riga d'intestazione è inviata nello stesso modo).
- Il **client** invia il comando `DATA` per segnalare l'inizio del body.
- Il **server** risponde con il codice 354.
- Il **client** spedisce il body (contenuto della mail) come una sequenza di righe terminate da un punto (".").
- Il **server** conferma la ricezione restituendo il codice 250.
- Il **client** invia il comando QUIT per comunicare la fine dell'invio del messaggio.
- Il **server** ritorna il codice 221, a cui segue l'interruzione della connessione TCP.

Pit Stop

5 Che cos' è il protocollo SMTP?

6 Come funziona il protocollo SMTP?

La Tabella 5 mostra alcuni messaggi di errore che possono verificarsi durante l'invio della posta.

Messaggio	Descrizione
`MAILBOX FULL`	La casella di posta a cui l'utente invia il messaggio ha raggiunto il limite massimo di capienza consentito e non è più in grado di ricevere ulteriori messaggi
`BAD DESTINATION MAILBOX ADDRESS USER UNKNOWN`	L'indirizzo di posta non esiste
`ROUTING SERVER FAILURE`	Il dominio non esiste
`DELIVERY TIME EXPIRED`	L'indirizzo di destinazione non riceve il messaggio nonostante ripetuti tentativi
`MESSAGE TOO BIG`	Il messaggio inviato è troppo grande per essere accettato dal server di destinazione

← Tab. 5 messaggi di errore durante l'invio della posta.

Protocollo SMTP con autenticazione

In origine il protocollo SMTP non prevedeva alcuna autenticazione da parte del mittente, e ciò consentiva di inviare e-mail con indirizzi falsi, facilitando lo spam e il phishing. Per cercare di limitare queste operazioni fraudolente è stata sviluppata un'estensione di SMTP (SMTP Service Extension for Authentication, RFC 4954) in cui la fase di connessione al server di posta è preceduta da un'autenticazione dell'utente.

- Il **client** inizia la conversazione con il comando **`EHLO`** con cui richiede al server di posta la lista dei comandi che ampliano quelli nativi di SMTP.
- Il **server** conferma inviando il codice 250.
- Il **client** invia il comando **`AUTH LOGIN`** seguito da **username** e **password** della casella di posta del mittente. Queste informazioni devono essere codificate in Base64 per essere accettate (ad esempio, la parola "PASSWORD" è codificata come stringa "UEFTU1dPUkQ=".
- Se l'autenticazione va a buon fine il server conferma inviando il codice 235.

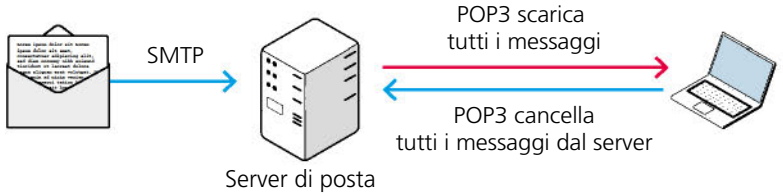
La **Tabella 6** sintetizza i comandi SMTP inviati dal client.

Comando	Descrizione	Parametri	Note
HELO	*Hello*	nome mittente	Inviato dal mittente al server SMTP per aprire una sessione di posta.
EHLO	*Extended Hello*	nome mittente	Inviato dal mittente a un server SMTP che prevede le "Estensioni SMTP". Il server risponde inviando le estensioni supportate (ad esempio HELP, AUTH, LOGIN...).
MAIL	*Inizia l'e-mail*	parametro obbligatorio: "FROM:" specifica l'e-mail del destinatario	Comunica l'indirizzo mittente.
RCPT	*Destinatario*	parametro obbligatorio: "TO:" specifica l'e-mail del destinatario	Specifica un destinatario del messaggio di posta.
DATA	*Contenuto del messaggio*	Nessuno	Il mittente è pronto a inviare il testo del messaggio al server. Il server SMTP risponde con un messaggio 354. Il mittente trasmette una linea alla volta terminando con un "." su una sola linea.
RSET	*Reset*	Nessuno	Annulla i comandi dati.
VRFY	*Verify*	e-mail da verificare	Si richiede al server di confermare l'esistenza dell'utente specificato.
HELP	*Help*	Comando SMTP	Manuale dei comandi.
NOOP	*No Operation*	Nessuno	Non svolge alcuna azione ma verifica se esiste la connessione con il server.
QUIT	*Quit*	Nessuno	Termina la sessione SMTP.

↑ **Tab. 6** Principali comandi SMTP inviati da client.

Protocollo POP3 (Post Office Protocol v3)

Il protocollo POP3 (*Post Office Protocol versione* 3), descritto in RFC: 1734, 1939, 1957, 2449, è utilizzato dal client di posta del destinatario per accedere alla sua casella di posta e leggere le mail. (**Figura 18**). Quando un client POP3 (utente destinatario) si connette al server, recupera tutti i messaggi dalla casella di posta, li scarica sul dispositivo utente locale e li elimina dalla casella di posta sul server. In questo modo è possibile accedere ai messaggi anche senza connessione internet. È da evidenziare però che, i client POP3 consentono di mantenere su server copia dei messaggi di posta, se espressamente richiesto.



➜ **Fig. 18** Funzionamento di POP3.

POP3 è un protocollo client/server che utilizza TCP e lavora sulla porta 110. I comandi inviati dal client sono stringhe di 4 caratteri. Il server risponde con codici di tre cifre.

La comunicazione tra client e server si articola in tre fasi:

- apertura della connessione;
- trasferimento del messaggio;
- chiusura della connessione.

Il trasferimento di messaggi comprende:

- **autenticazione**: l'utente deve comunicare nome e password per poter accedere alla propria mail-box;
- **transazione**: il client scarica i messaggi presenti sul server di posta, e, una volta scaricati, può contrassegnarli e informare il server che dovranno essere rimossi;
- **aggiornamento**: il server elimina i messaggi precedentemente contrassegnati e la connessione viene terminata.

La Tabella 7 sintetizza i comandi POP3 inviati dal client.

Comando	Descrizione	Parametri	
USER	*Username*	*Casella postale* (ad esempio: nome.cognome@serverpop.xx)	Viene usato per la fase di autenticazione dal client. Identifica l'utente
PASS	*Password*	Password	Viene usato per la fase di autenticazione dal client. Invia in chiaro la password dell'utente
LIST	*List*	Senza parametri indica la dimensione di ogni messaggio, altrimenti quella del solo messaggio indicato	È eseguito dal client per chiedere di elencare il contenuto della casella di posta (verrà visualizzato un messaggio per riga specificando la lunghezza di ogni messaggio in byte). Termina con un punto "."
STAT	*State*	-	Restituisce il numero di messaggi presenti nella casella di posta e lo spazio occupato
RETR	*Retry*	-	Recupera e visualizza il messaggio indicato
DELE	*Delete*	-	Contrassegna il messaggio per la sua eliminazione
NOOP	*No Operation*	-	Non svolge alcuna azione, ma verifica se esiste la connessione con il server. Restituisce un messaggio +OK se il server risponde
QUIT	*Quit*	-	Termina la sessione POP3. Segue la fase di aggiornamento e la disconnessione dal server
NOOP	*No Operation*	-	Non svolge alcuna azione, ma verifica se esiste la connessione con il server
QUIT	*Quit*	-	Termina la sessione POP3

← **Tab. 7** Principali comandi POP3 inviati dal client al server.

Pit Stop

7 Che cos'è e a che cosa serve il protocollo POP3?

8 Come funziona il protocollo POP3?

Esempio 5

Il comando `LIST` è utilizzato per verificare la lista dei messaggi presenti nella casella di posta.
L'esecuzione di `LIST` restituisce il numero dei messaggi e la loro dimensione in byte. Successivamente si procede alla marcatura per la cancellazione dei messaggi con il comando `DELE` seguito dal numero del messaggio e, infine, con il comando `QUIT` si abbandona la sessione dando luogo alla cancellazione dei file precedentemente marcati. Nell'esempio che segue sono elencati tre messaggi, rispettivamente di 890, 1900 e 400 byte, che poi vengono recuperati e cancellati.

```
LIST
1 890
2 1900
3 400

RETR1
DELE1;
RETR2
DELE2
QUIT
```

Protocollo IMAP (Internet Message Access Protocol)

Il protocollo IMAP (Internet Message Access Protocol) (RFC 3501) è utilizzato dal client di posta del destinatario per accedere alla sua casella di posta e leggere le e-mail. È stato ideato da Mark Crispin nel 1986 come alternativa a POP3 per superarne i limiti. Diversamente da POP3, IMAP consente di gestire le e-mail senza scaricarle localmente e senza doverle eliminare dal server (**Figura 19**). Gli utenti possono visualizzare sul loro client le copie dei messaggi, mentre i messaggi originali rimangono sul server fino alla loro cancellazione manuale. In genere IMAP è utilizzato da webmail client che consentono, tramite browser, di leggere solo l'intestazione o parti del messaggio, senza necessariamente fare il download dei file, e di organizzare e archiviare i messaggi di posta elettronica mantenendo la sincronizzazione tra client e server.

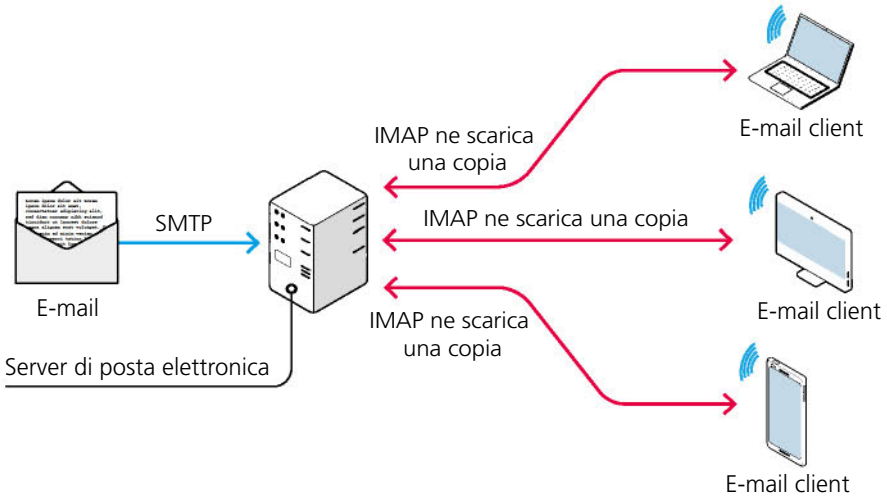


Fig. 19 Funzionamento di imap.

È un protocollo client /server che utilizza TCP e la vora sulla porta 143.
I comandi del client riguardano:

- l'accesso autorizzato alla casella di posta;
- la verifica della presenza di nuovi messaggi;
- la gestione e la rimozione dei messaggi o parti di essi.

Esempi di comandi IMAP del client sono: `SELECT`, `SEARCH`, `FETCH`, `EXPUNGE`.
Nella sezione di Laboratorio presenteremo una tipica sessione che utilizza Telnet o un terminale a riga di comando per la visualizzazione di una e-mail con IMAP.

4 Il protocollo FTP (File Transfer Protocol)

File Transfer Protocol (FTP) è un protocollo di livello applicativo usato da un client per accedere al file system di un server remoto e avere la possibilità di fare su di esso le operazioni che, in genere, si fanno sul proprio dispositivo locale. È molto utile per trasferire i file da un dispositivo locale a un server remoto, ad esempio quando si vuole pubblicare un sito internet in hosting. È un protocollo client-server che utilizza TCP e due porte: la porta 21 per l'invio dei comandi del protocollo e un'altra porta per il trasferimento dei dati (file).
FTP è uno dei primi protocolli storici di Internet. Sviluppato nel 1971 presso il MIT (Massachusetts Institute of Technology) di Cambridge, è stato definito nella RFC 114, ma ha subito vari cambiamenti negli anni fino ad arrivare alla RFC 959.
Come per gli altri protocolli di livello applicazione, anche per FTP esiste la versione sicura SFTP (*SSH File Transfer Protocol*) e FTPS (FTP *Secure*). SFTP utilizza SSH e fornisce una connessione crittogafata su cui trasferire i dati in modo sicuro. FTPS utilizza SSL/TLS per crittografare i dati trasmessi tramite FTP.

Pit Stop

9 Che cos'è il protocollo FTP?

Accesso FTP

Il protocollo FTP permette al server FTP di accettare le richieste che gli arrivano da un client.
Gli utenti possono autenticarsi utilizzando username e password, oppure, se il server lo permette, accedere in modo anonimo digitando "anonymous" alla richiesta del login, senza immettere alcuna password.
L'accesso anonimo pone dei limiti alle operazioni consentite: è possibile, per esempio, fare il download dei file ma non modificarne il contenuto. Con l'autenticazione in chiaro la connessione non è sicura. Per proteggere le credenziali di accesso la connessione può utilizzare protocolli sicuri come SSL (FTPS – FTP Secure) oppure FTP può essere sostituito da SSH File Transfer Protocol (SFTP).
È possibile utilizzare un client FTP sia da riga di comando, sia utilizzando l'interfaccia grafica di una applicazione client FTP (per esempio FileZilla), sia utilizzando un browser (si veda la sezione di Laboratorio).

Funzionamento del protocollo FTP

Una sessione FTP si articola in quattro fasi:

- il client effettua una richiesta a un server FTP;
- il server effettua l'autenticazione del client;
- il client effettua il trasferimento dei dati;
- la connessione viene chiusa.

Pit Stop

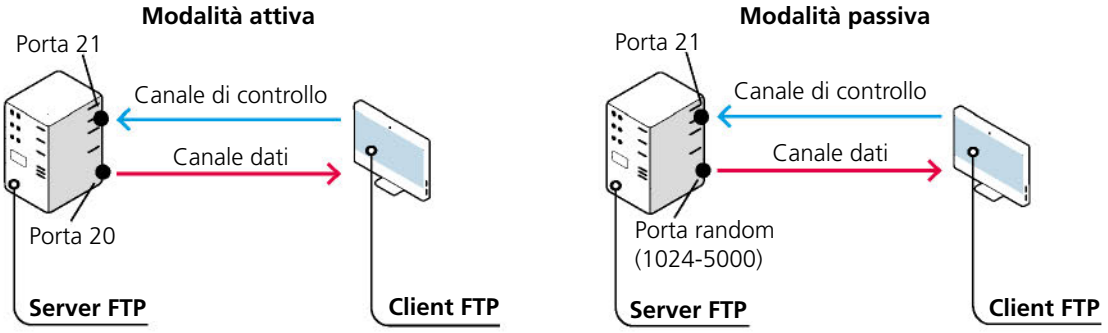
10 Cos'è una connessione FTP attiva?

11 Cos'è una connessione FTP passiva?

Il protocollo FTP può utilizzare due diverse modalità per il collegamento client-server (Figura 20):

- modalità **Attiva** (o Standard): il client comunica al server la porta lato client a cui connettersi. Il client invia al server FTP il comando `PORT` che specifica il numero della porta che il client utilizzerà per il trasferimento dei dati. Il server instaura una nuova connessione per il transito dei dati, tra la porta del client e la sua porta 20 (Figura 20a);
- modalità **Passiva** (Figura 20b): il server sceglie la porta lato client a cui connettersi. il client invia al server FTP il comando `PASV`. Il server sceglie arbitrariamente una porta, compresa tra 1024 e 5000, e la comunica al client FTP che apre una nuova connessione per il passaggio dei dati (Figura 21).

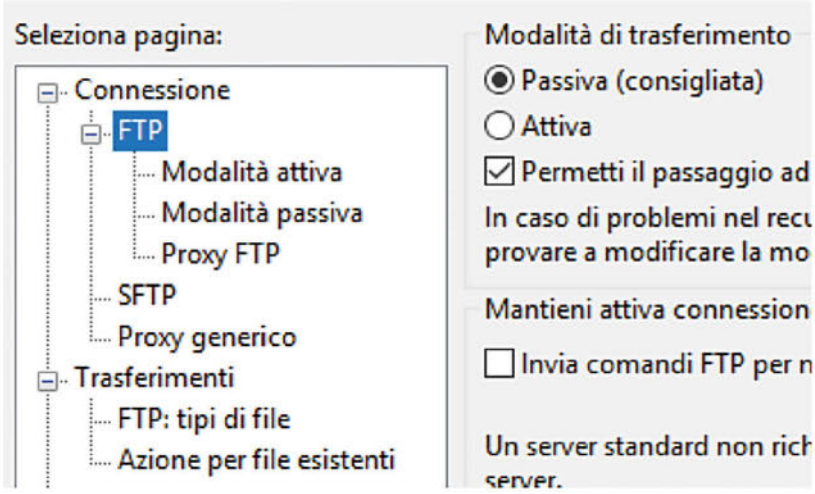
In entrambi i casi il client utilizza la porta 21 per inviare i comandi al server.



a Avvio della connessione dati da server (porta 20)

b Avvio della connessione dati da client

↑ **Fig. 20** Il protocollo FTP supporta due modalità. **a.** La modalità Standard (o Attiva) utilizza su server la porta 21 per i comandi. L'avvio della connessione dati è fatto da server utilizzando la porta 20. **b.** Anche la modalità Passiva utilizza la porta 21 per il canale di controllo, ma l'avvio della connessione dati è effettuato da client su una porta del server scelta arbitrariamente da quest'ultimo.



↑ **Fig. 21** Impostazione predefinita di FileZilla in modalità **Passiva**.

Comandi del protocollo FTP

Il server è un interprete di comandi ricevuti dal client: li legge, effettua l'analisi sintattica, li esegue e risponde con un codice di conferma. La Tabella 8 riporta i più comuni comandi del client FTP, quasi tutti derivati dal sistema Unix.

Funzione di	Comandi da parte del client	Descrizione
Apertura	`open`	Apertura connessione al sito (vengono richieste login e password per l'identificazione dell'utente)
Chiusura	`quit`	Termina la sessione
Trasferimento e gestione dei file	`get`	Preleva il file indicato e lo salva nella cartella corrente del client (download)
	`w`	Copia il file indicato sull'host remoto (upload)
	`delete`	Rimuove un file dalla cartella corrente
Navigazione nel file system	`pwd`	Mostra il nome della cartella in cui ci si trova sull'host remoto
	`ls, dir`	Mostra i file contenuti nella cartella
	`cd`	Si posiziona nella cartella indicata sul client
	`mkdir`	Crea una nuova cartella
Aiuto	`help`, oppure "`?`"	Mostra l'elenco dei comandi disponibili

← Tab. 8 Elenco dei più comuni comandi FTP.

I codici di risposta del server sono costituiti da numeri di tre cifre in cui ogni cifra, a partire da quella più significativa, identifica il tipo e il dettaglio. La Tabella 9 mostra il significato della prima cifra del codice.

– **1**yz:	risposta preliminare positiva: il comando è stato accettato, seguirà ulteriore risposta prima del comando successivo
– **2**yz:	comando eseguito con successo, ad esempio: 200, 226 ecc.
– **3**yz:	risposta intermedia positiva: comando eseguito correttamente, ma in attesa di ulteriori informazioni successive
– **4**yz:	comando non eseguito correttamente
– **5**yz:	comando che il server non ha potuto eseguire

← Tab. 9 Codifica della prima cifra del codice di risposta.

notabene

Il Trivial File Transfer Protocol (TFTP) è un protocollo di trasferimento file di livello applicativo molto semplice, spesso utilizzato in reti locali per operazioni come il salvataggio della configurazione di dispositivi di rete quali router e switch. Supporta operazioni di base come lettura e scrittura di file, ma non gestisce e-mail e non supporta la navigazione tra le directory. Non include meccanismi di autenticazione o cifratura, ciò che lo rende inadatto per l'uso su Internet in ambienti non protetti. La porta standard utilizzata per le richieste iniziali è la 69, mentre il trasferimento dati avviene su porte casuali selezionate dal server.

Pit Stop

12 Quali sono i principali comandi FTP?

Pit Stop

13 Che cos'è il protocollo RTP?

5 RTP: il protocolli delle videoconferenze

Un effetto collaterale positivo della pandemia di coronavirus è stata l'accelerazione dello sviluppo delle tecnologie legate alla sicurezza e alla comunicazione a distanza, tra cui la videoconferenza. In pochi giorni, milioni di studenti, professori, impiegati e dirigenti hanno dovuto improvvisarsi esperti nell'uso di webcam, microfoni, pixel e banda passante.
In effetti il funzionamento di una videoconferenza, al di là della semplicità d'utilizzo, è abbastanza complesso perché prevede una serie di passi per il trattamento dei dati che devono essere fatti in tempo reale e che vanno dalla cattura dell'audio e del video con microfoni e webcam, alla compressione dei dati per ridurre la larghezza di banda necessaria alla loro trasmissione, l'invio dei dati attraverso Internet agli altri partecipanti, la decompressione dei dati ricevuti, fino alla loro riproduzione in tempo reale.
In questo contesto, ci focalizziamo sui protocolli che supportano la videoconferenza, in particolare su RTP e il suo omologo sicuro SRTP che sono utilizzati in applicazioni come Google Meet, Microsoft Teams e Cisco Webex.

notabene

Se in una videoconferenza vengono utilizzati sia i media audio che quelli video, sono trasmessi come sessioni RTP separate e i pacchetti vengono trasmessi utilizzando due diverse porte UDP.

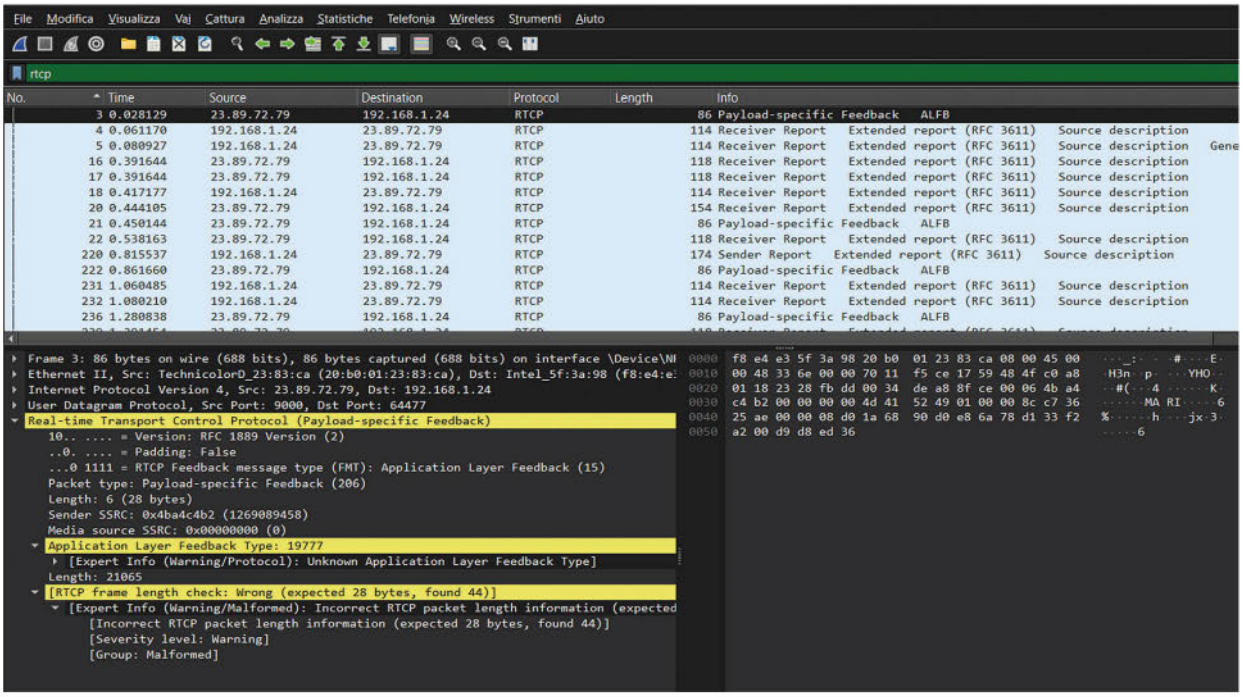
Campo	Lunghezza in bit	Descrizione
V - Versione	2	Indica la versione del protocollo.
P - Padding	1	Indica se, alla fine del pacchetto, sono presenti uno o più ottetti di riempimento.
X - Extension	1	Indica la presenza di un header esteso.
CC - CSRC Count	4	Contiene il numero di identificatori CSRC.
M - Marker	1	Usato dal livello applicativo per segnalare eventi significativi.
PT - Payload Type	7	Identifica il formato del payload per i diversi tipi di dati audio e video trasportati.
Sequence Number	16	Il numero di sequenza è incrementato di uno per ciascun pacchetto di dati inviato e può essere utilizzato dall'applicazione del destinatario per rilevare la perdita di pacchetti e per ripristinare la sequenza dei pacchetti. Il valore inziale è casuale per motivi di sicurezza.
Timestamp	32	Timestamp riflette l'istante di campionamento del primo ottetto. È utilizzato per permettere al ricevente di sincronizzarsi.
SSRC Synchronization Source Identifier	32	Identifica univocamente la sorgente del flusso audio e video.
CSRC contributing source identifier	32 (da 0 a 15 elementi)	Enumerano le fonti dei dati presenti nel payload. Il numero di identificatori CSRC è dato dal valore del campo CC.
Payload	variabile	Dopo il preambolo sono inseriti i dati veri e propri, ossia il carico utile (payload), che contiene i flussi audio o video.

0 1 2 3 4 5 6 7 8 9 0 0 1 2 3 4 5 6 7 8 9 0 0 1 2 3 4 5 6 7 8 9 0 1	
V P X CC M PT	Sequence Number
Timestamp	
Synchronization Source (SSRC) Identifier	
Contributing Source (CSRC) Identifiers ...	

← **Fig. 22** Il formato del protocollo RTP.

Le caratteristiche principali di RTP (*Real-time Transport Protocol*) comprendono il trasporto in tempo reale, su Internet, dei dati audio e video e l'utilizzo del protocollo UDP che privilegia la velocità nella consegna dei dati.
Il formato del protocollo RTP, descritto nell'RFC 3550, include un header seguito da un payload (**Figura 22**).

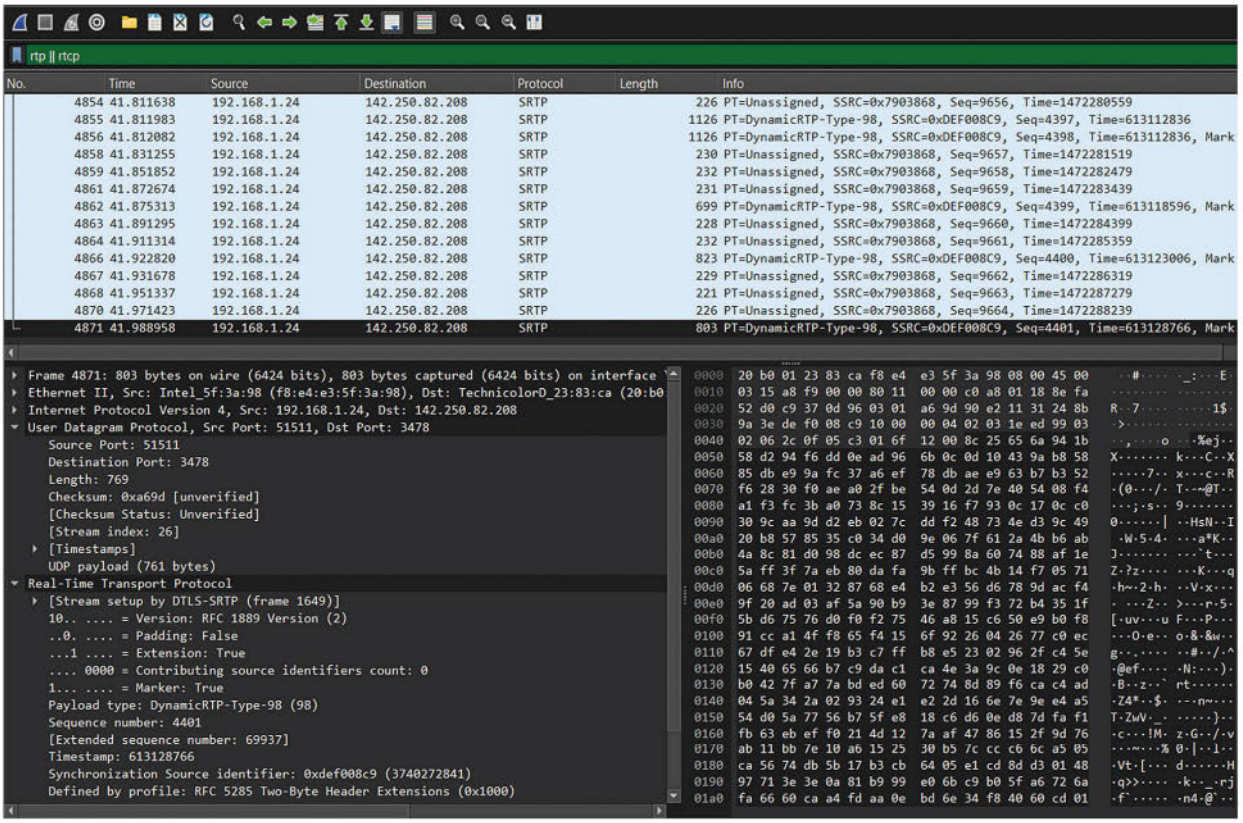
Il protocollo RTP è affiancato dal protocollo RTCP (*Real-Time Control Protocol*), che ne arricchisce le funzionalità con meccanismi di controllo e monitoraggio RTCP lavora insieme a RTP per migliorare la trasmissione in tempo reale. RTCP monitora e controlla la Qualità del Servizio (QoS), raccogliendo dati su perdite di pacchetti e ritardi.
Inoltre, identifica i partecipanti e regola la trasmissione dei dati, prevenendo la congestione della rete. L'header di RTCP è simile a quello di RTP per garantire coerenza e compatibilità tra i due protocolli, rendendo più facile la loro coesistenza sui sistemi. (**Figura 23**).



↑ **Fig. 22** La cattura di un messaggio RTP e RTCP con wireshark.

SRTP (*Secure Real-time Transport Protocol*) rappresenta l'evoluzione protetta di RTP, come definito nell'RFC 3711. Questo protocollo rafforza la sicurezza dei dati trasmessi attraverso l'implementazione di funzionalità di crittografia e autenticazione. In particolare, SRTP incorpora la crittografia AES (*Advanced Encryption Standard*), per la cifratura dei dati, garantendo così la riservatezza e l'integrità dei dati. In aggiunta, il protocollo assicura l'autenticazione dei messaggi, confermando l'identità del mittente (**Figura 23**).

Fig. 23



Approfondimento - Tecnologia 1

DNS e sicurezza

Il DNS è utilizzato quotidianamente quando navighiamo in Internet, quando usiamo la posta elettronica e in tutte le attività online che richiedono la risoluzione dei nomi di dominio in indirizzi IP. Occorre essere consapevoli di eventuali problemi di sicurezza informatica legati all'uso del DNS. Di seguito ne presentiamo alcuni.

Privacy. Se il server DNS è di proprietà di un fornitore di servizi e non si utilizza una VPN che, come vedremo, consente di mascherare il proprio indirizzo IP, l'ISP potrebbe essere a conoscenza della nostra attività in rete e della cronologia di navigazione.

Affidabilità. È necessario affidarsi ad un provider che garantisca l'affidabilità del servizio DNS per evitare che si verifichino errori nella risoluzione dei nomi o rallentamenti.

Filtraggio dei contenuti. È opportuno affidarsi a un provider in grado di bloccare siti inappropriati.

Per quanto riguarda l'attività di hacking, numerosi sono gli attacchi informatici che possono essere attuati verso server DNS e cache DNS vulnerabili:

- **DNS cache poisoning** e **DNS spoofing**: le ultime richieste vengono memorizzate in una cache al fine di velocizzare le richieste future. Questo attacco riempie la cache con indirizzi IP falsi, inducendo i server a connettersi a indirizzi IP dannosi e conducendo gli utenti a siti web falsi e fraudolenti. È necessario controllare sempre l'URL nel browser.
- Dirottamento e reindirizzamento DNS. Può avvenire in vari modi:
  - **server DNS dirottato**. Sono modificate le impostazioni del server DNS per reindirizzare le richieste DNS verso server dannosi;
  - **dirottamento di un router DNS**. Sono modificate le impostazioni DNS di un router e quindi di tutti i dispositivi da esso gestiti;
  - **dirottamento del DNS locale**. Sono modificate le impostazioni del DNS locale, sul dispositivo dell'utente, installando un malware sul dispositivo dell'utente.

Una delle soluzioni usate per proteggere le informazioni scambiate con il DNS è utilizzare il protocollo **DNSSEC** (***D**omain **N**ame **S**ystem **S**ecurity **E**xtensions*). Questo protocollo si basa sulla crittografia a chiave pubblica, certificati e firme digitali e consente di:

- verificare dell'**integrità** di ogni record;
- autenticare il server DNS e quindi assicurarsi che le informazioni provengano da un server DNS autorevole;
- assicurarsi che il server DNS sia considerato attendibile dal dominio superiore nella gerarchia DNS (**chain of trust**, o catena della fiducia).

notabene

Nelle prossime Unità saranno spiegati i significati di integrità, crittografia, protocolli sicuri e chain of trust).

Approfondimento - Tecnologia 2

Sicurezza e utilizzo delle porte

Le Unità che seguono approfondiscono i concetti e le tecniche relative alla sicurezza, ma già in questo contesto possiamo vedere gli effetti devastanti che possono essere causati da un uso improprio del servizio di posta elettronica.
Il servizio di posta elettronica è uno di quelli più presi di mira da malintenzionati, che lo utilizzano per aprire delle backdoor e introdursi nei sistemi di sicurezza. Non basta quindi premunirsi di sistemi per proteggersi da virus, spam e phishing: occorre avere la certezza che i provider garantiscano la tutela del nostro account e la continuità del servizio.
Alcuni suggerimenti per tutelarci:

- utilizzare almeno due account, in modo da poter accedere sempre ai propri dati anche se uno dei due dovesse risultare inaccessibile;
- non usare l'indirizzo aziendale per la registrazione a servizi privati;
- prestare attenzione quando si fornisce il consenso all'utilizzo dei dati. Quello a fini di marketing inonderà la nostra casella di posta di pubblicità;
- utilizzare password diverse per servizi diversi e modificare spesso la password;
- non pubblicare l'indirizzo di posta su social media;
- prestare attenzione ai servizi gratuiti che non garantiscono l'assistenza, invadono di pubblicità e non forniscono servizi aggiuntivi;
- affidarsi a un provider che utilizza sistemi di sicurezza quali la crittografia, protocolli sicuri per criptare i messaggi che viaggiano in rete e l'autenticazione a due fattori.

L'esempio che segue mostra come sia estremamente facile far apparire al destinatario un indirizzo e-mail falso: è sufficiente inserire nel comando `MAIL FROM` un indirizzo di fantasia (`hacker@xxx.it`).

```
Client ->   telnet smtp.xxx.it 25
Server <-   Connected to mail.xxx.it
Server <-   220 SMTP smtp.xxx.it
Client ->   HELO default
Server <-   250 smtp.xxx.it Hello, pleased to meet you
Client ->   MAIL FROM: hacker@xxx.it
Server <-   250 hacker@xxx.it... Sender ok
Client ->   RCPT TO: vito.vittima@yyy.it
Server <-   250 vito.vittima@yyy.it... Recipient ok
Client ->   DATA.....
Server <-   250 TAA18303 Message accepted for delivery
Client ->   QUIT
```

Il ricevente, `vito.vittima@yyy.it`, potrebbe rispondere a `hacker@xxx.it` e insospettirsi vedendo che l'indirizzo non è raggiungibile. Per questo motivo viene spesso creata una falsa e-mail del tipo `assi-stenza-tecnica@xxx.it`, a cui è possibile rispondere. Questa tecnica viene frequentemente utilizzata per richiedere nome utente e password a una persona completamente ignara di quello che succede.

Ad esempio:

```
From: assistenza-tecnica@xxx.it
To: vito.vittima@yyy.it
Oggetto: Attenzione!
Data: 12.12.2015
Gentile cliente, la informiamo che a causa di un guasto
in centrale i dati sul nostro server sono andati perduti.
Le chiediamo di ripristinare immediatamente le sue cre-
denziali per potere riattivare il servizio.
Per favore inserisca al seguente indirizzo www.colcavolo.
com i suoi dati comprensivi di Username e Password oppure
risponda direttamente a questa e-mail.
Scusandoci per l'inconveniente, la salutiamo cordialmen-
te.
Assistenza Tecnica
ISP-XXX.i
```

L'invio sicuro di e-mail richiede l'utilizzo di protocolli sicuri che utilizzano algoritmi di crittografia. Per questo motivo il sistema di posta elettronica utilizza varie porte. Di seguito le più utilizzate:

Porta	Utilizzo
25	È la porta SMTP standard per il trasferimento dei messaggi tra i server di posta. Non è cifrata. Spesso è bloccata dai fornitori di servizi in cloud perché affetta da molto spam.
587	Utilizzata per la fase di submission (consegna della posta al server del mittente). È criptata con il protocollo TLS (*Transport Layer Security*).
465	Nel 1975 IANA ha assegnato questa porta per SMTP. Inizialmente usata per la fase di submission con SSL, è attualmente fuori uso, ma ancora supportata da molti server. Sostituita da 587.
2525	Utilizzata spesso al posto della porta 587 quando questa è bloccata. Utilizza TLS. Non è riconosciuta da IETF o IANA.

Esempio

Caratteristiche di due particolari servizi di posta elettronica

Gmail
Indirizzo del server SMTP: `smtp-mail.outlook.com`
Porte: 587 consigliata per l'invio sicuro di e-mail crittografate con il protocollo Transport Layer Security (TLS). Le porte 465 e 25 sono ancora supportate ma sconsigliate.

Outlook
Indirizzo del server SMTP: `smtp.gmail.com`
Porte: 587 consigliata per l'invio sicuro di e-mail crittografate con il protocollo Transport Layer Security (TLS).

Netiquette per la posta elettronica

L'insieme di regole e linee guida da seguire in rete per apparire credibili e rispettosi tenendo un comportamento appropriato sono complessivamente chiamate "netiquette", una parola composta dai termini inglesi "net" (rete) ed "etiquette" (etichetta, galateo, ovvero buona educazione). Alcune delle "regole d'oro" sono le seguenti:

1. Usare sempre il campo "oggetto", che deve essere un sommario della e-mail;
2. Limitarsi a un solo argomento per e-mail e aggiungere allegati solo se necessari (pensiamo alla ricezione di allegati su dispositivi mobili);
3. Essere brevi (non è un romanzo!);
4. Usare toni educati e pacati e limitare l'uso di emoticon solo ad ambienti informali;
5. Tenere un linguaggio appropriato, mai volgare o irrispettoso o che possa mettere a disagio il destinatario
6. Fare attenzione agli errori (è fastidioso ricevere e-mail piene di errori che denotano fretta e poco rispetto per il destinatario)
7. Mettere in CC solo chi è effettivamente interessato
8. Rileggere sempre ciò che viene scritto e cancellare il superfluo, in modo da essere sintetici.
9. Scegliere un buon indirizzo: semplice e facile da ricordare, soprattutto per gli usi professionali. Un buon indirizzo aumenta l'affidabilità, l'organizzazione, promuovendo l'azienda. È come presentare a un cliente un biglietto da visita elegante e ben strutturato.
10. L'ultimo elemento di un messaggio di posta è la firma. Questa deve essere fatta con criterio: deve contenere le informazioni di contatto, il ruolo del mittente nell'azienda, telefono, e-mail, sito web e collegamenti ai social media.

Approfondimento - Tecnologia 3

Emoticon, smile ed emoji

La posta elettronica, come altri servizi di Internet, viene utilizzata anche per sostituire telefonate o colloqui personali. Il fatto che in questi contesti informali la posta elettronica non preveda, al contrario della comunicazione orale, forme di comunicazione non verbale (come lo sguardo, i gesti, il tono della voce che accompagnano la conversazione e contribuiscono a determinarne il significato) può prestarsi a errori di interpretazione e malintesi. Per questa ragione, per comunicare stati d'animo o sentimenti, chi scrive una e-mail o un "instant message" ricorre spesso a una riproduzione stilizzata delle espressioni facciali, semplicemente componendo i caratteri di testo in modo fantasioso e creativo (**Tabella 1**). La nascita delle prime emoticon sembra risalire alla fine degli anni Settanta del secolo scorso, ma è con l'avvento degli SMS che esse hanno avuto un successo planetario, tanto è vero che oggi su ogni dispositivo mobile sono presenti rappresentazioni grafiche di emoticon (emoji) con volti sorridenti (smile), emozioni, animali, cibi e oggetti di ogni genere. La standardizzazione degli emoticon è prevista dello standard Unicode che fornisce i caratteri grafici per personaggi ed emozioni, in modo da unificare nel mondo l'interpretazione delle icone (**Figura 1**).

:-) :-D	sono felice, molto felice
:D :) :))	mi fai ridere
:-X	bacioni
:'(	mi fai piangere
=:-)	mi fai drizzare i capelli
[]&:*	abbracci e baci
8-#	morto
:*)	ubriaco
8;-)	ho la testa che mi gira
:-Q	fumatore
(:-$	sono a letto con la febbre
@:-)	conturbante
[:]	robot
:-) :-(:-I	giudizio: positivo, negativo, così così
8-)	occhialuto
+O:-)	il Papa
:-X	bocca cucita

Tab. 1



Fig. 1 Un esempio di emoticon Unicode standard (Intervallo di valori esadecimali: 1F600-1F632).

Laboratorio

ATTIVITÀ 1
DNS: visualizzare i record DNS presenti nella cache del proprio computer

Scenario

Ogni host ha una memoria temporanea in cui memorizza i record DNS già risolti. In questo modo, se necessario, si può evitare di inoltrare le richieste ai vari server DNS, poiché l'IP cercato sarà disponibile immediatamente.

Consegna

Visualizzare i record DNS presenti nella cache del proprio computer su sistema operativo Windows.

Svolgimento

Aprire il prompt dei comandi e digitare il comando `ipconfig /displaydns`.
Di seguito mostriamo, a titolo di esempio, l'esecuzione del comando e alcuni record delle risorse presenti:

```
C:\Users>ipconfig /displaydns

Configurazione IP di Windows

    clients3.google.com
    ----------------------------------------
    Nome record . . . . . : clients3.google.com
    Tipo record . . . . . : 5
    Durata (TTL). . . . . : 108
    Lunghezza dati. . . . : 8
    Sezione . . . . . : Risposta
    Record CNAME  . . . . : clients.l.google.com


    Nome record . . . . . : clients.l.google.com
    Tipo record . . . . . : 1
    Durata (TTL). . . . . : 108
    Lunghezza dati. . . . : 4
    Sezione . . . . . : Risposta
    Record A (Host) . . . : 142.250.180.174


    www.gmail.com
    ----------------------------------------
    Nome record . . . . . : www.gmail.com
    Tipo record . . . . . : 1
    Durata (TTL). . . . . : 152
    Lunghezza dati. . . . : 4
    Sezione . . . . . : Risposta
    Record A (Host) . . . : 216.58.204.133
```

Utilizzare il comando `ipconfig /flushdns` per svuotare la memoria cache, come di seguito:

```
C:\Users>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.
```

ATTIVITÀ 2
DNS: utilizzo del comando nslookup

Scenario

In genere il DNS è usato da applicazioni client per risolvere un nome, per esempio da un client HTTP o da un client per la posta elettronica. A volte però è utile o necessario poter inviare delle richieste direttamente al server DNS (o a più server DNS) e ottenere l'indirizzo IP di un host o per monitorare il funzionamento del sistema. Il comando `nslookup` svolge questa funzione.

`Nslookup` funziona in due modalità:

- **modalità interattiva**, usata per avere informazioni sui server interrogati per risolvere un nome;
- **modalità non interattiva**, usata per avere l'indirizzo IP (o nome) di un singolo host nel server locale.

Consegna

Usare il comando `nslookup` da riga di comando per effettuare una richiesta DNS e ottenere l'indirizzo IP associato a un nome o viceversa.

notabene

Il nome «nslookup» deriva da *name server look up* (controllo dei name server).

Svolgimento

```
C:\Users>nslookup
Server predefinito:  one.one.one.one
Address:  1.1.1.1

> www.google.com
Server:  one.one.one.one
Address:  1.1.1.1
```

Risposta da un server non autorevole:

```
Nome:    www.google.com.homenet.telecomitalia.it
Address:  127.0.0.1
```

notabene

Un "server non autorevole" indica che la risposta proviene da un server DNS che ha ottenuto l'informazione da una fonte non ufficiale).

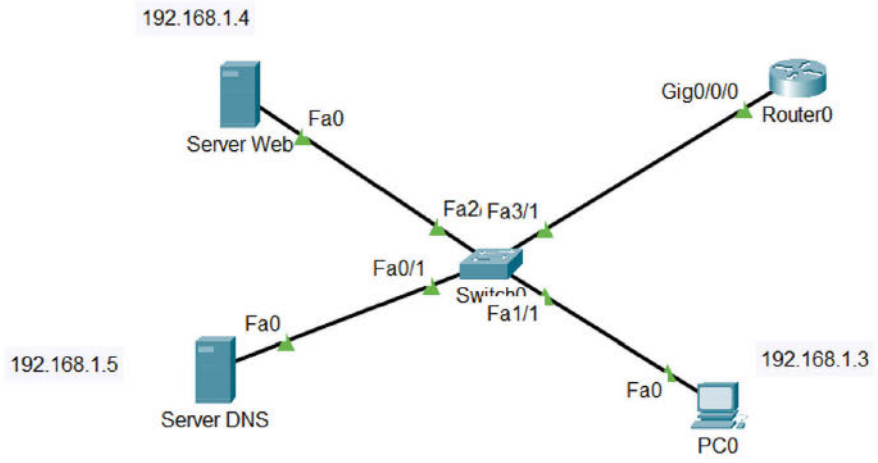
ATTIVITÀ 3
DNS: risoluzione del nome di host tramite DNS

Scenario

Si consideri la rete mostrata in figura, con indirizzo di rete 192.168.1.0/24.

Sia:

- `192.168.1.4` (di nome `www.pinco.it`) l'host su cui è in esecuzione il server HTTP (porta 80);
- `192.168.1.5` l'host su cui è in esecuzione il server DNS (porta 53);
- `192.168.1.3` l'host da cui utilizzare un client HTTP (browser) per chiedere una pagina web al server web.



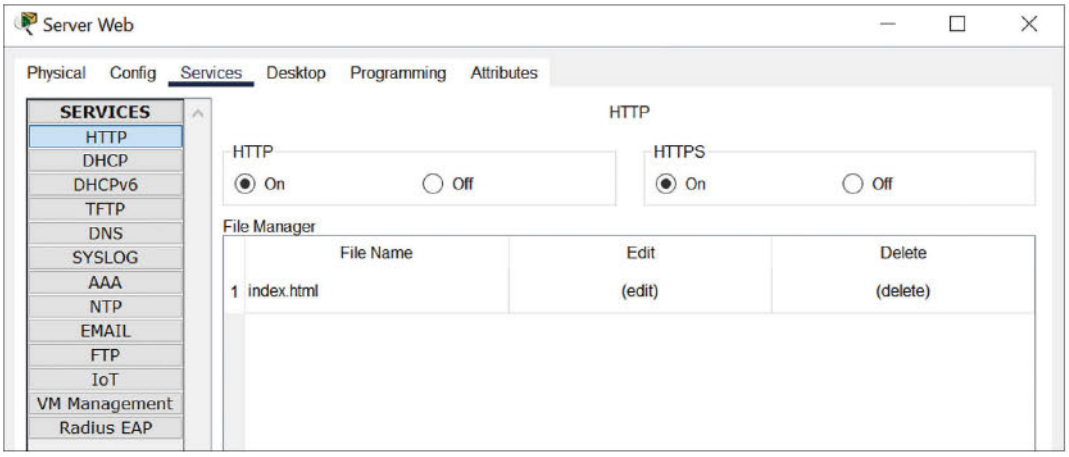
Consegna

Utilizzare il servizio DNS per risolvere il nome di un host (`www.pinco.it`) presente nell'URL usato per la richiesta di una pagina web.

Svolgimento

Dopo aver assegnato la configurazione di rete ai dispositivi (Indirizzo IP, Subnetmask e default gateway), seguire i passi descritti di seguito.

Passo 1: configurare l'host `192.168.1.4` come server web, come in figura



- Se si desidera personalizzare il contenuto delle pagine web, in particolare il file `index.html`:

File Name: index.html

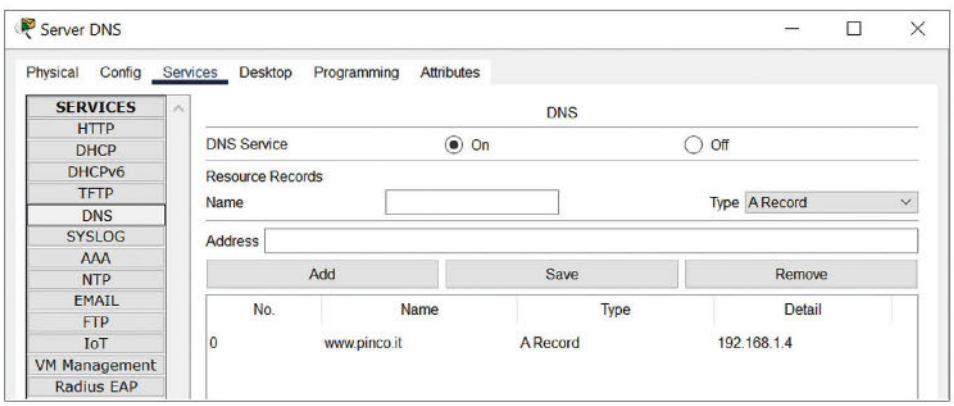
```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>PROVA DI LABORATORIO
<p>Molto bene!!!
<br>Il DNS funzionaaaa!!!!

</html>
```

Passo 2: configurare l'host 192.168.1.5 come server DNS
Aggiungere il record DNS con:

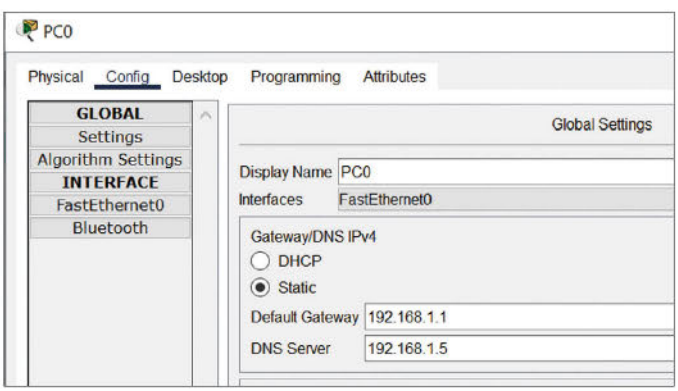
- `Name: www.pinco.it`
- `Value: 192.168.1.4`
- `Type: A`

In questo modo un client DNS richiedente che fornisca il nome `www.pinco.it` avrà come risposta l'IP corrispondente.



Passo 3

- Nella configurazione di rete di PC0, assegnare al server DNS l'indirizzo `192.168.1.5`.



- Aprire il browser da PC0 e digitare nella barra degli indirizzi l'URL `http://www.pinco.it` per far partire la richiesta http. Il nome del file di default è `index.html` (come se ci fosse `http://www.pico.it/index.html`).
- Cliccare su GO.

Se tutto va bene, sarà visualizzato il file `index.html` restituito al client HTTP dal server HTTP in esecuzione su `192.168.1.4`.

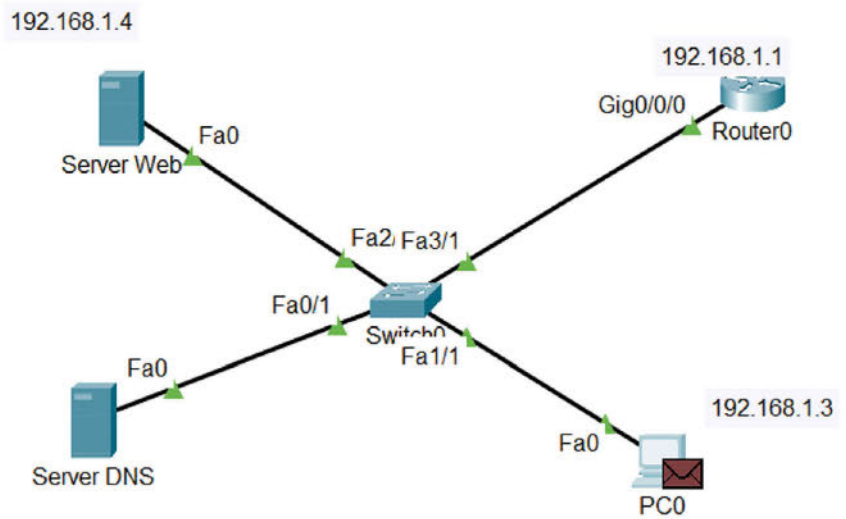


Analizziamo ora nel dettaglio ciò che è successo, avvalendoci della modalità *Simulation* di Packet Tracer.

Passo 4: il client HTTP manda una richiesta al server DNS

Consideriamo l'URL utilizzato dal client HTTP: `http://www.pinco.it/index.html`.

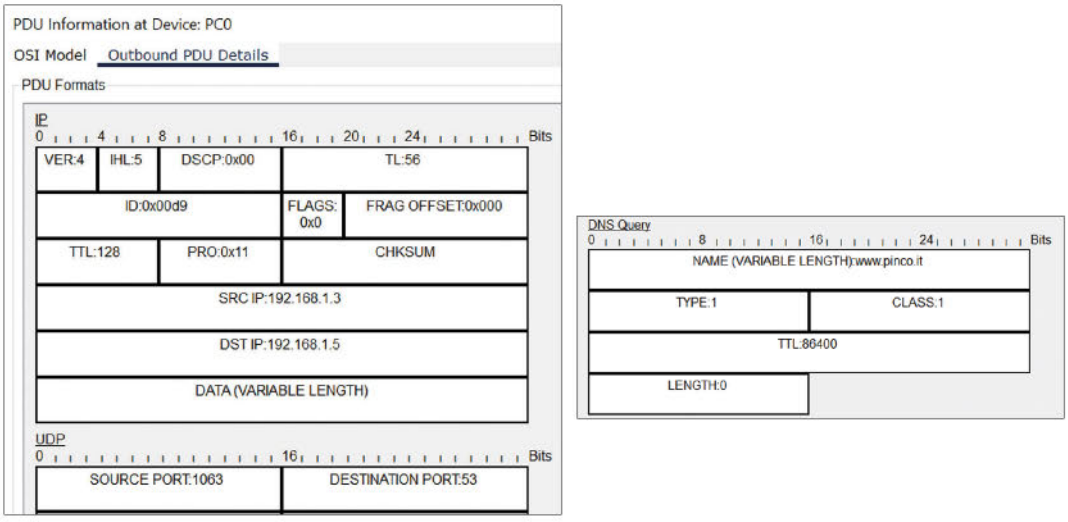
- HTTP è il protocollo utilizzato che significa che la richiesta è indirizzata a un server web sulla porta 80;
- `index.html` è il file HTML richiesto dal client al server HTTP;
- `www.pinco.it` è il nome dell'host, che però deve essere risolto tramite il DNS.



- Da PC0 parte una richiesta HTTP.
- Per poter stabilire una connessione TCP con il server HTTP, al client HTTP serve l'indirizzo IP del server HTTP.
- Il client HTTP estrae dall'URL l'indirizzo dell'host (`www.pinco.it`) e, tramite client DNS, invia una richiesta al DNS (`192.168.1.5`) per la risoluzione del nome e avere l'IP.

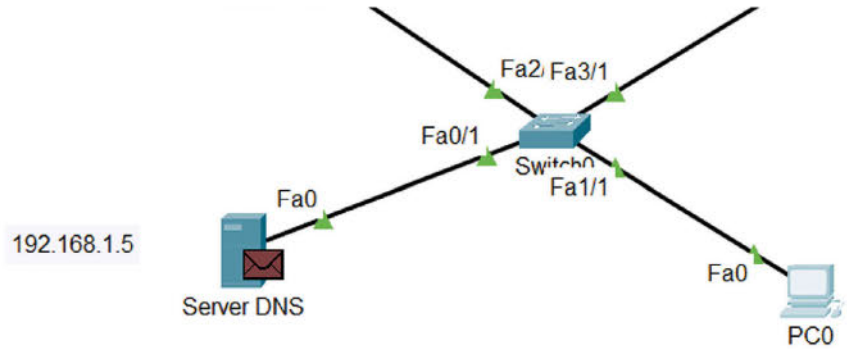
Qui sotto osserviamo il PDU in uscita da PC0:

- nel pacchetto l'indirizzo IP del mittente è quello di PC=, l'indirizzo IP del destinatario è `192.168.1.5` (server DNS);
- nel segmento la porta del destinatario è 53 (porta del DNS);
- nel payload (messaggio di livello applicazione) è presente la richiesta DNS con il nome da risolvere (`www.pinco.it`).



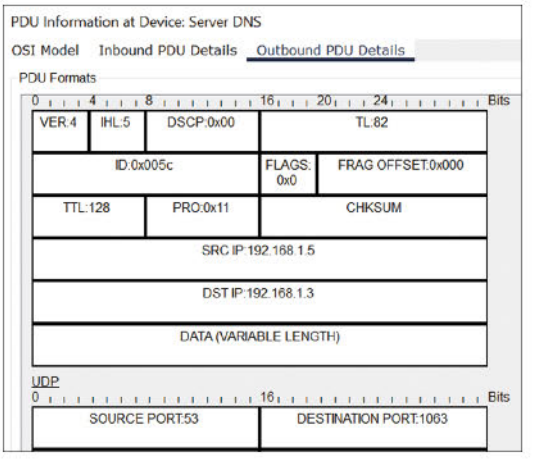
Passo 5: il server DNS manda la risposta al client HTTP

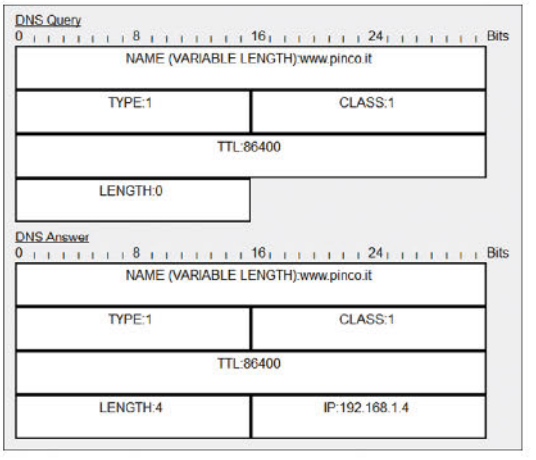
La richiesta arriva al server DNS che, consultando il record delle risorse, invia al client HTTP il nome dell'host richiesto.



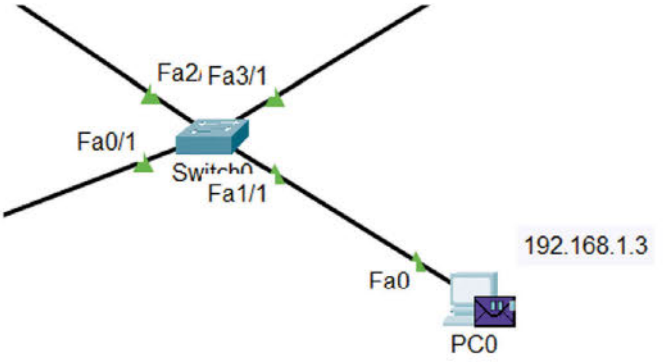
Qui sotto osserviamo il PDU in uscita dal server DNS:

- nel pacchetto l'indirizzo IP del mittente è quello del server web, l'indirizzo IP del destinatario è quello del client HTTP (da cui ha ricevuto la richiesta);
- nel segmento la porta mittente è 53, la porta destinazione 1063 (quella che era mittente nella richiesta);
- nel payload (messaggio di livello applicazione) è presente la richiesta DNS (che gli era pervenuta) e la risposta DNS con l'indirizzo IP associato al nome.



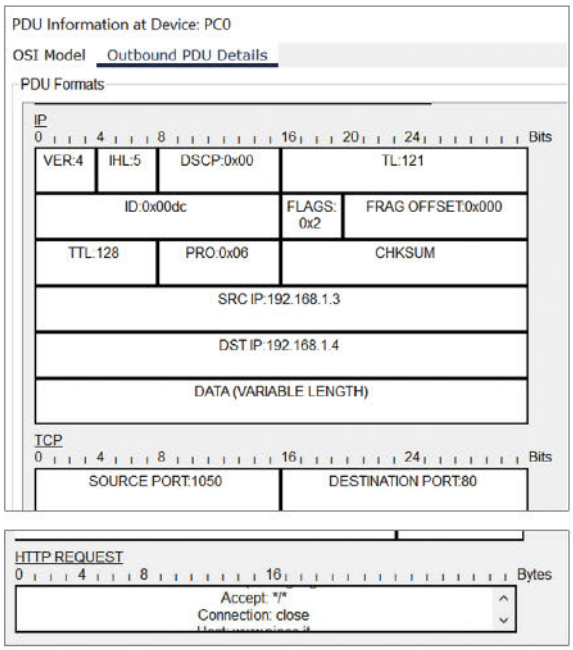


Passo 6: il client HTTP manda una richiesta al server HTTP



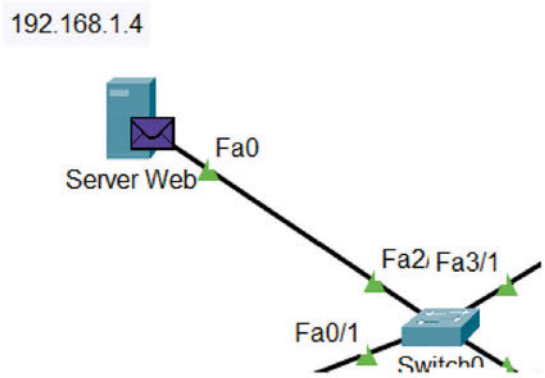
Il client HTTP (su PC0) riceve la risposta dal server DNS, e con l'indirizzo IP ricevuto invia al server HTTP la richiesta del file `index.html`.

Qui sotto osserviamo il PDU in uscita dal PC0:



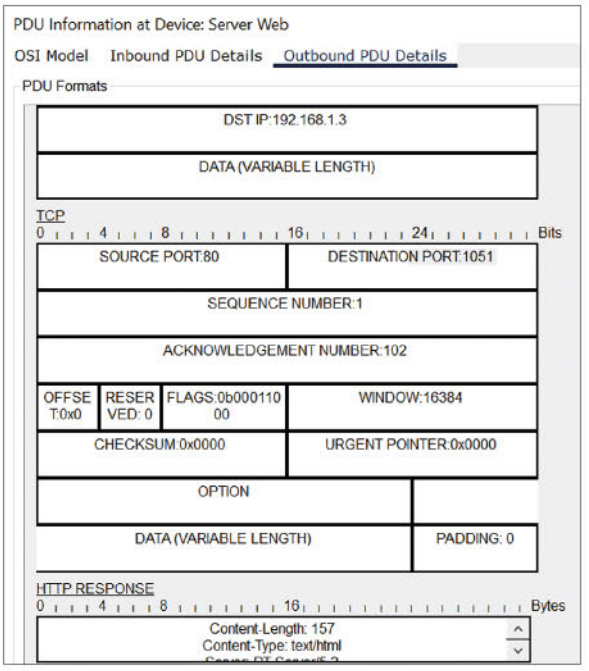
- nel pacchetto l'indirizzo IP del mittente è quello del client HTTP, l'indirizzo IP del destinatario è quello del server HTTP (indirizzo ricevuto da DNS);
- nel segmento la porta destinazione è 80 (server HTTP).
- Il payload contiene la richiesta HTTP.

Passo 7: il server HTTP invia la risposta al client HTTP



Il server HTTP riceve la richiesta dal client HTTP e invia la risposta con la pagina web (file `index.html`) richiesta.
Successivamente il client HTTP riceverà la risposta e il browser visualizzerà la pagina web.

Qui a fianco osserviamo il PDU in uscita dal server WEB.



Nel pacchetto l'indirizzo IP del mittente è quello del server HTTP, l'indirizzo IP del destinatario è quello del client HTTP;

- Nel segmento la porta destinazione 80 (serve HTTP);
- Il payload contiene la risposta HTTP.

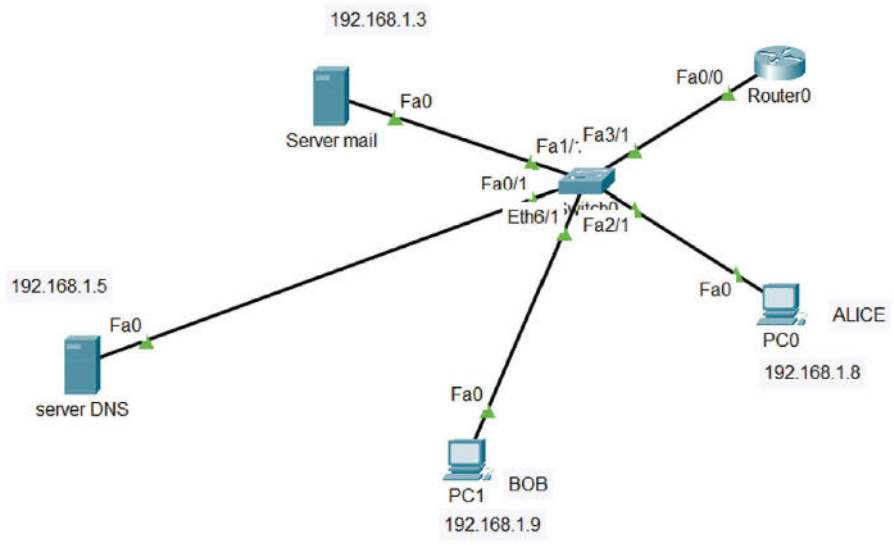
ATTIVITÀ 4

Posta elettronica: invio di un messaggio con STMP e lettura di un messaggio con POP3 utilizzando Packet Tracer

Scenario

Si consideri la rete mostrata in figura, con indirizzo di rete 192.168.1.0/24.
Sia:

- `192.168.1.8` il client da cui Alice invia e riceve le mail;
- `192.168.1.9` il client da cui Bob invia e riceve le mail;
- `192.168.1.3` il server di posta con le mail box di Alice e Bob;
- `192.168.1.5` l'host su cui è in esecuzione il server DNS (porta 53).



Consegna

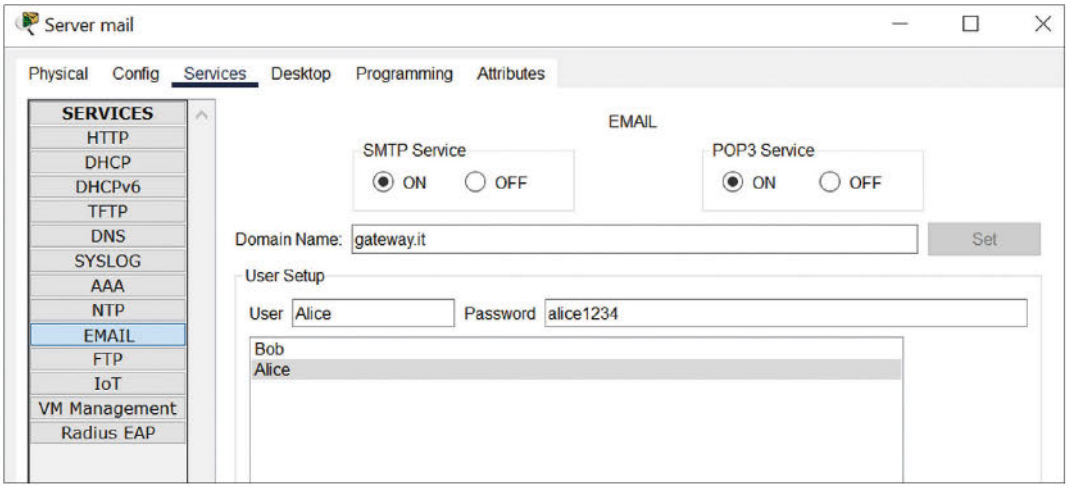
Configurare i client di posta e il server di posta affinché Alice e Bob possano inviare e ricevere mail.

Svolgimento

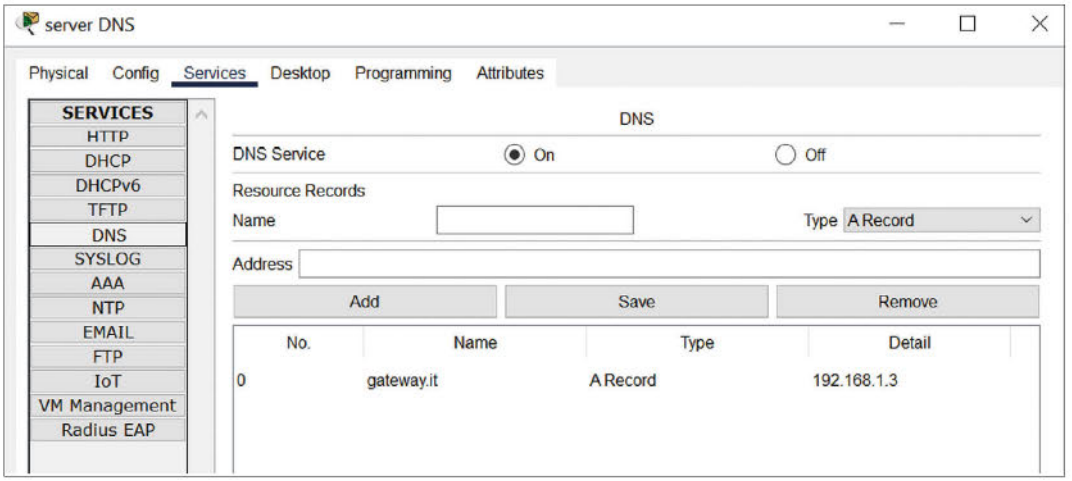
Dopo aver assegnato la configurazione di rete ai dispositivi (Indirizzo IP, Subnetmask e default gateway), seguire i passi descritti di seguito.

Passo 1: configurazione dei server

- Configurare il server `192.168.1.3` come server e-mail e nome di dominio `gateway.it`;
- Creare due utenti, Alice e Bob, con user (nome utente) e password. Questi dati serviranno poi per accedere alla mail box;
- Abilitare il servizio SMTP e POP3.



- Configurare il server 192.168.1.5 come server DNS come nell'attività precedente, inserendo il record che associa al nome di `dominio gateway.it`, l'indirizzo IP `192.168.1.3`.

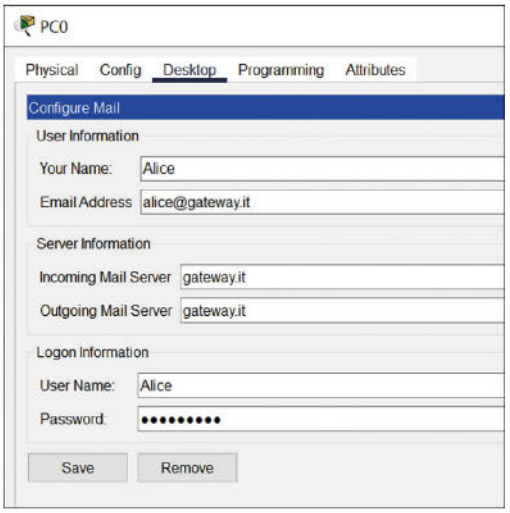


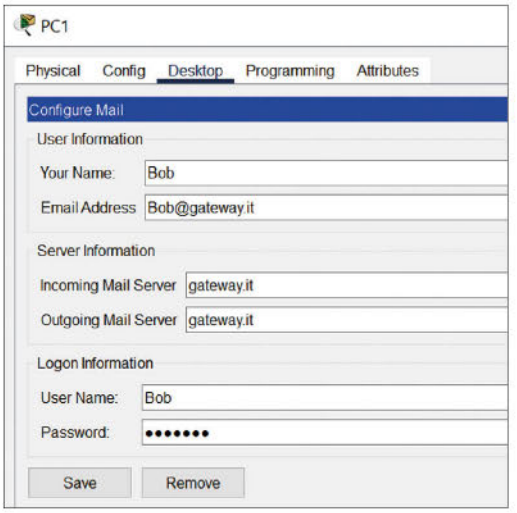
Passo 2: configurazione dei client

Aprire il PC0 di Alice e accedere da desktop alla funzione e-mail.

Selezionare il menu *Configure Mail* e inserire i dati di configurazione come descritto in figura, tenendo presente che nome utente e password sono quelli che Alice dovrà utilizzare per accedere alla sua casella di posta sul server.

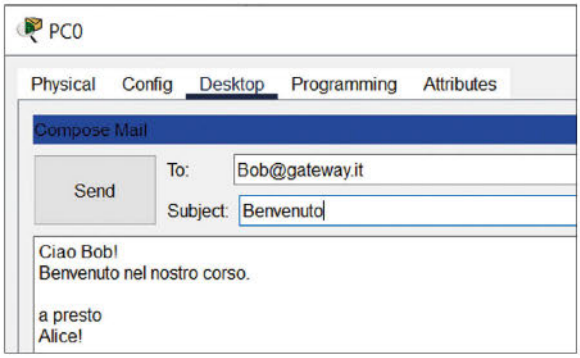
Ripetere tutto sul PC1 di Bob.



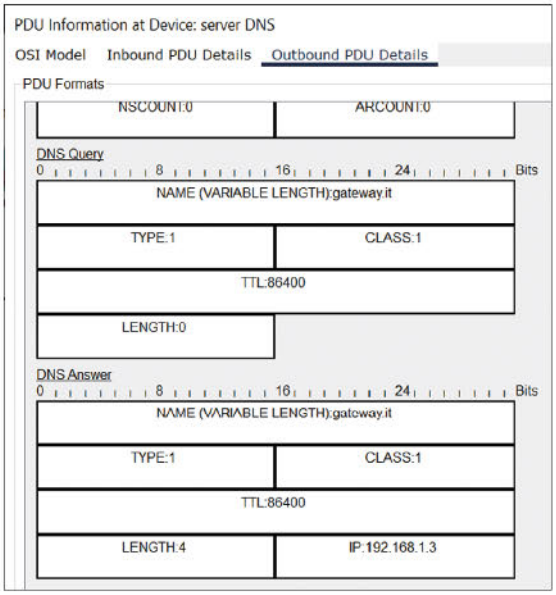


Passo 3: Alice invia un messaggio di posta a Bob

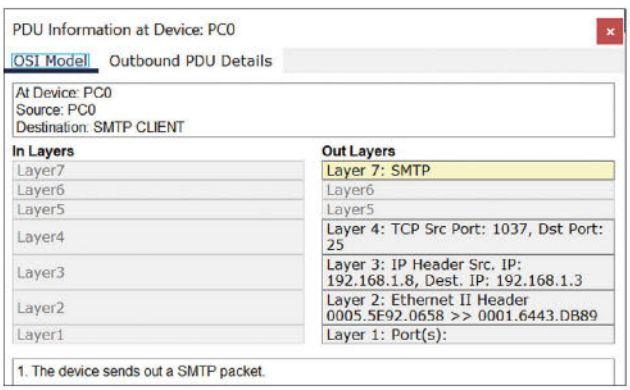
Dal PC0 di Alice accedere dal desktop alla funzione e-mail e scegliere *Compose* per scrivere una nuova e-mail. Inviare con *SEND*.



Passiamo ora in modalità *Simulation* di Packet Tracer per osservare i PDU nei vari passaggi. Poiché l'e-mail deve essere consegnata a Bob@gateway.it, deve essere inviata una richiesta al server DNS per la risoluzione del nome di dominio. Il server DNS risponde come in figura:

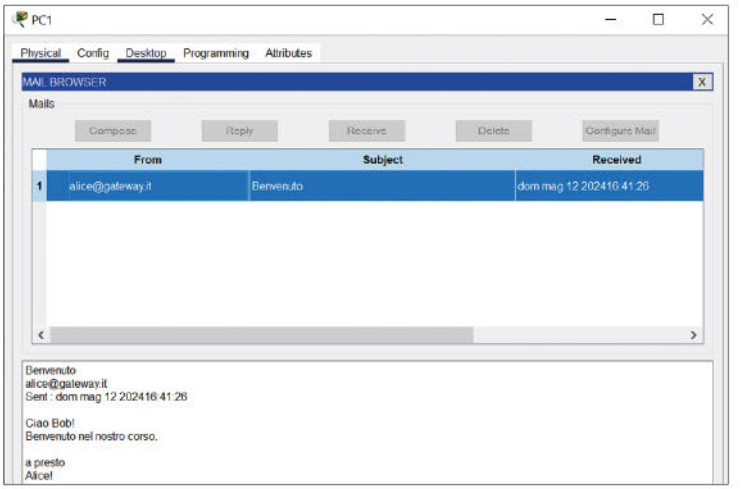


Ora il client di posta di Alice ha l'indirizzo IP del server. Crea una connessione TCP sulla porta 25 e poi invia l'e-mail al server corretto.



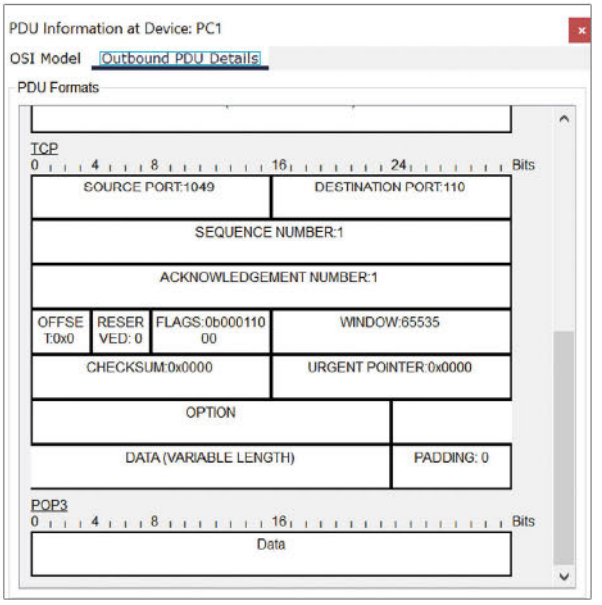
Passo 4: Bob legge il messaggio che gli ha inviato Alice

Dal PC1 di Bob, accedere al servizio e-mail tramite desktop e selezionare il menu *Receive* per scaricare le e-mail dalla mail box.



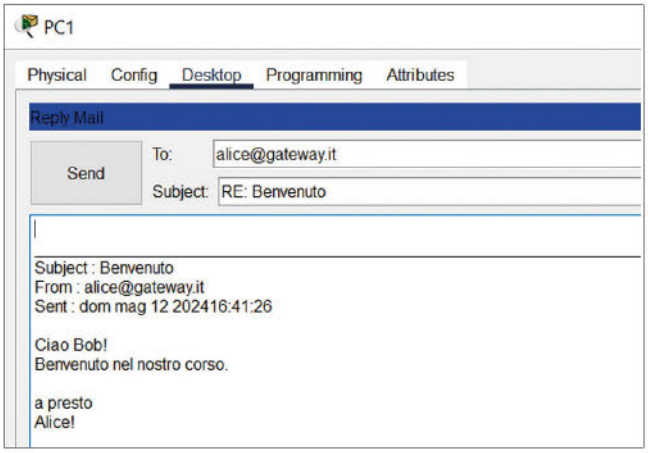
Il client di posta di Bob deve:

- usare un client DNS per risolvere il nome di dominio;
- aprire una connessione TCP con il server POP3 sulla porta 110 per scaricare i messaggi dalla sua mail box.

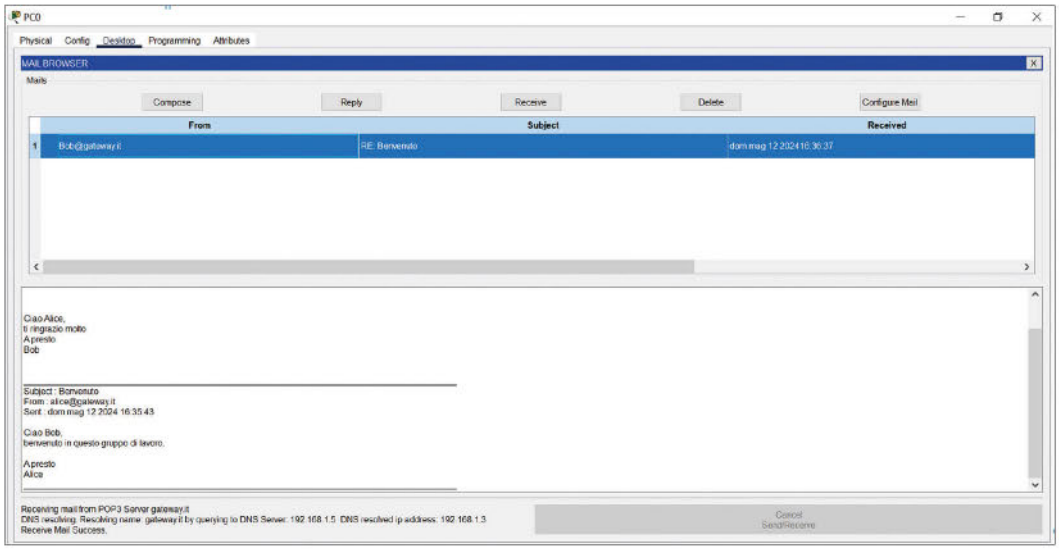


Passo 5: Bob risponde alla mail di Alice

Dal servizio e-mail del PC di Bob selezionare *REPLAY*, selezionare il messaggio a cui rispondere e scrivere il testo della mail. Rispondendo all'e-mail di Alice, il destinatario sarà alice@`gateway.it`, e l'oggetto della e-mail di risposta sarà quello della e-mail di Alice con anteposto "RE:" per far capire che è la risposta ("REply") a un messaggio arrivato in precedenza.



Alice riceverà:



ATTIVITÀ 5

Posta elettronica: utilizzo dei comandi di POP3 da riga di comando

Scenario

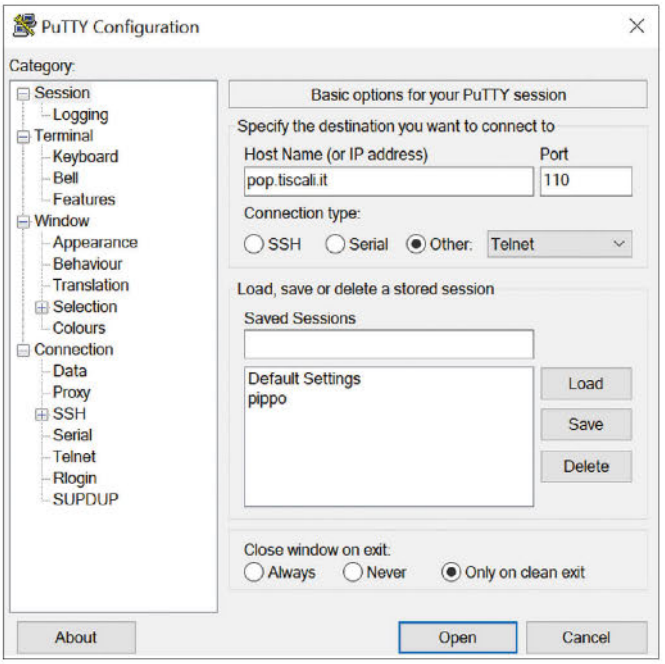
In questa attività ci colleghiamo al server POP3 di tiscali.it, per gestire le caselle di posta di un utente di cui saranno mascherati (in questa sede) nome e password.

Obiettivo

Utilizzare i comandi del protocollo POP3 da riga di comando.

Svolgimento

Utilizzare PuTTY per collegarsi al server POP3 di Tiscali.



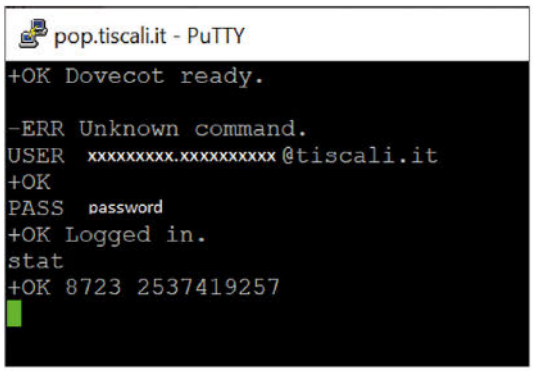
Il server risponde con `+OK`:

```
Server > +OK
Client > USER <Indirizzo della casella di posta dell'utente>
Server > +OK
Client > PASS <password dell'utente>
Server > +OK
```

con un messaggio di conferma dell'avvenuto login.

A questo punto è possibile fornire dei comandi POP3. Per esempio:

- il comando `stat` fornisce il numero di mail in arrivo nella mail box e il numero di byte occupati (come in figura);
- con il comando `RETR` n è possibile scaricare il messaggio numero *n*.



ATTIVITÀ 6

Posta elettronica: utilizzo dei comandi di ICMP da riga di comando

Scenario

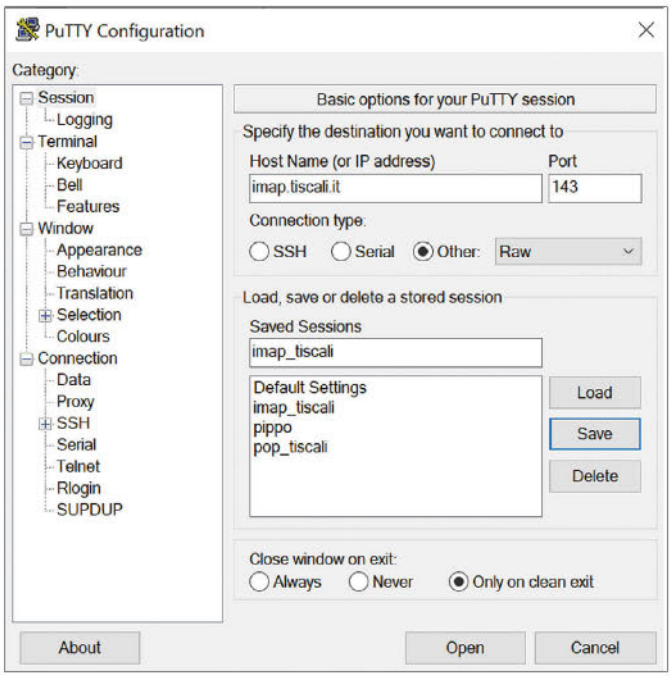
In questa attività ci colleghiamo al server IMAP di tiscali.it, per gestire le caselle di posta di un utente di cui saranno mascherati (in questa sede) nome e password.

Obiettivo

Utilizzare i comandi del protocollo IMAP da riga di comando.

Svolgimento

Utilizzare PuTTY per collegarsi al server IMAP di Tiscali.



Il server risponde con `* OK`

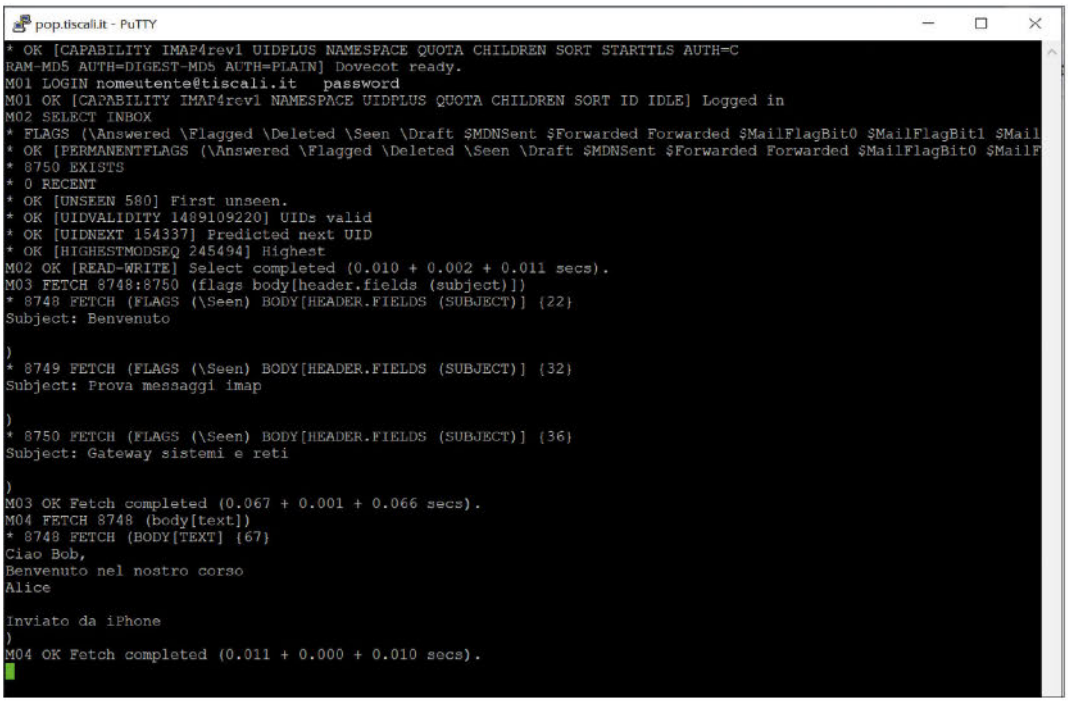
```
Server > * OK
Client > 1 LOGIN <Indirizzo casella di posta dell'utente> <pas-
sword>
Server > +OK
```

con un messaggio di conferma dell'avvenuto login.
A questo punto è possibile fornire dei comandi IMAP. Ogni comando inviato dal client è preceduto da un tag utilizzato per identificare il messaggio. La corrispondente risposta del server avrà lo stesso tag. Nel nostro esempio, usiamo i tag M01, M02, ...

Per esempio:

- `SELECT` "`INBOX`" seleziona la mailbox di arrivo dei messaggi. Nell'esempio il server risponde, tra le altre cose, che sono presenti 8750 mail (`8750 EXISTS`);

- il comando `FETCH 8748:8750 (flags body[header.fields (subject)])` mostra il Subject (oggetto) delle mail con UDI (identificativo) compreso tra 8748 a 8750 (le ultime tre arrivate);
- il comando `8748 FETCH (BODY[TEXT])` mostra il testo del messaggio numero 8748;
- il comando `LOGOUT` è usato per terminare la connessione.



ATTIVITÀ 7

FTP: utilizzo dei comandi di FTP da riga di comando

Scenario

In questa attività ci colleghiamo al server FTP di ietf.org, in modalità anonima, per leggere i file presenti.
La modalità anonima utilizza

- Utente: `anonymous`
- Password: `anonymous`

Obiettivo

Utilizzare i comandi del protocollo FTP da riga di comando.

Svolgimento

Aprire il prompt dei comandi, posizionarsi nella cartella desiderata e digitare `FTP`.
Appare il prompt dei comandi `ftp>`.
Dopo l'autenticazione (in modalità anonima) è possibile inviare comandi FTP. Per esempio:

- il comando `ls` lista i file presenti sul server;

- il comando `get robots.txt` scarica il file `robots.txt` sul dispositivo dell'utente nella cartella corrente.

```
ftp> open ftp.ietf.org
Connesso a ftp.ietf.org.
220 FTP server ready
200 UTF8 set to on
Utente (ftp.ietf.org:(none)): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
ietf-ftp-service-is-retired.txt
robots.txt
226 Transfer complete
ftp: 48 bytes received in 0.00secondi 16.00Kbyte/sec)
ftp> get robots.txt
200 PORT command successful
150 Opening ASCII mode data connection for robots.txt (26 bytes)
> R:Errore di I/O
226 Transfer complete
ftp: 28 bytes received in 0.00secondi 28000.00Kbyte/sec)
ftp>
```

ATTIVITÀ 8

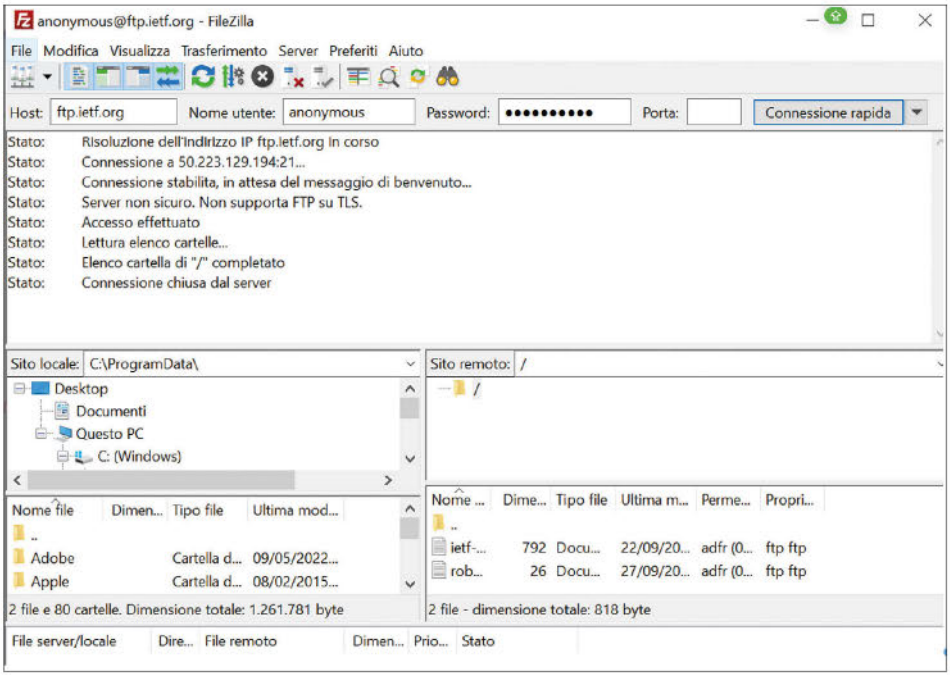
FTP: utilizzo del protocollo FTP dall'interfaccia grafica di un client

Scenario

In questa attività utilizziamo un client FTP con interfaccia grafica per collegarci al server FTP di `ietf.org` (come nell'attività precedente) in modalità anonima, per vedere e leggere i file.

Consegna

Utilizzare FileZilla (un client FTP) per collegarsi al server FTP e accedere al file system.



notabene

FileZilla (client) è usato per la connessione a un server FTP. Si tratta di un'applicazione open-source, utilizzata spesso per trasferire file su un server Web per la pubblicazione di siti Internet.

Svolgimento

Aprire FileZilla e impostare i parametri richiesti:

- Host: `ftp.ietf.org`
- Nome Utente: `anonymous`
- Password: `anonymous`

Nella parte superiore della finestra scorrono i messaggi che ci comunicano in che stato è la connessione. Al termine la connessione è stabilita e, tramite interfaccia grafica con il mouse, è possibile operare sui file (solo per le operazioni ammesse in modalità anonima).

ATTIVITÀ 9
Il protocollo SRTP con Wireshark

Scenario

Analizzare il traffico del protocollo SRTP (*Secure Real-time Transport Protocol*), la versione sicura, crittografata, di RTP, all'interno di una video conferenza. RTCP (*Real-time Transport Control Protocol*) è utilizzato insieme a RTP per il monitoraggio della qualità del servizio e identificare i partecipanti alla sessione di videoconferenza.

Consegna

Analizzare i pacchetti del protocollo SRTP con Wireshark in una videoconferenza Google Meet.
Successivamente analizzare i campi del protocollo RTCP.

Svolgimento

Passo 1: cattura dei pacchetti RTP

- Creare una nuova riunione con Google Meet e partecipare alla riunione.
- Aprire Wireshark e selezionare l'interfaccia di rete da cui si desidera catturare i pacchetti.
- Durante la cattura, Wireshark registrerà tutti i pacchetti che transitano attraverso l'interfaccia. Per visualizzare solo il traffico RTP, inserire il filtro "rtp" nella barra dei filtri.

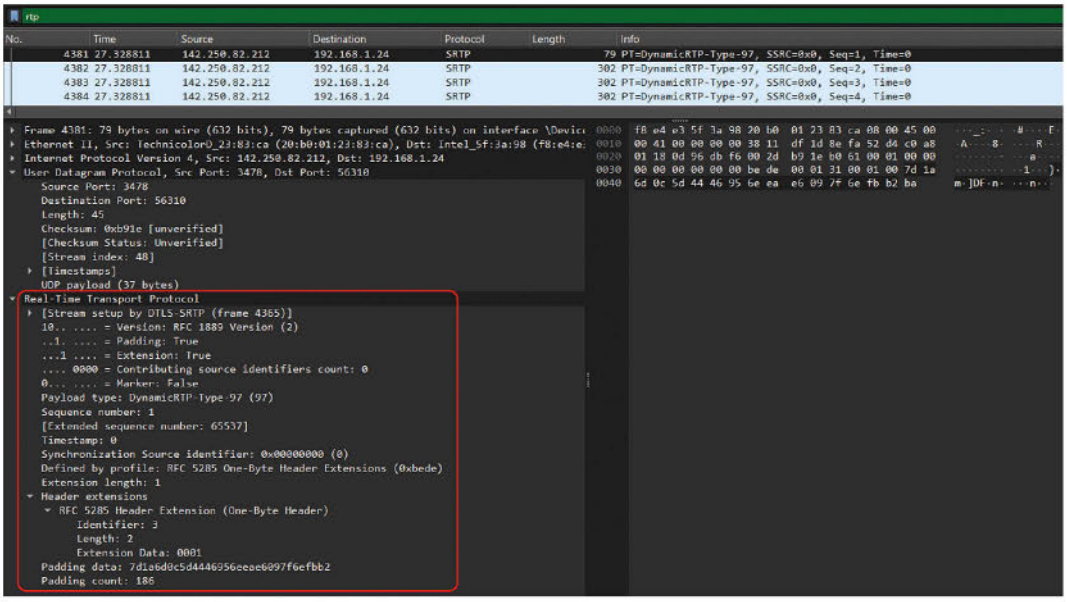
Si noti che per filtrare i pacchetti SRTP si utilizzano le stesse tecniche di filtraggio di RTP, con la differenza che i dati non saranno in chiaro e, per interpretarli, è necessario disporre delle chiavi appropriate.

Passo 2: esame dei campi RTP

- Selezionare un pacchetto per visualizzare i dettagli nel pannello inferiore di Wireshark.
- Verificare l'utilizzo del protocollo UDP.
- Espandere la sezione *Real-Time Transport Protocol* per analizzare i campi di RTP:
  a. numero di sequenza;
  b. timestamp;

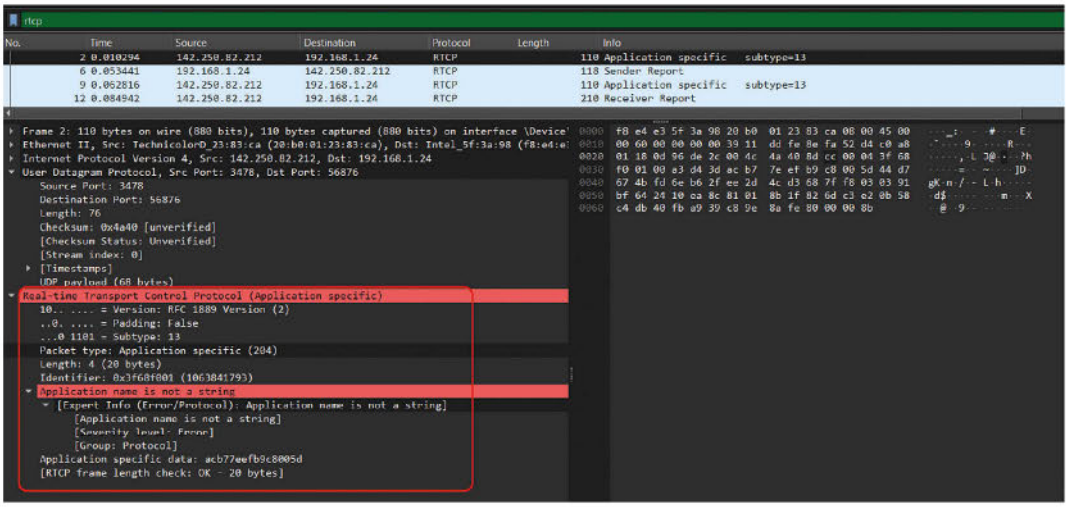
c. identificatore SSRC;
d. Padding data e padding count.

Nella figura che segue, che mostra una finestra di Wireshark, la sezione Real Time transport Protocol è evidenziata da un riquadro rosso.



Passo 3: cattura ed esame dei pacchetti RTCP

- Procedere come per i passi 1 e 2, inserendo il filtro "rtcp" nella barra dei filtri.
- Selezionare un pacchetto per visualizzare i dettagli nel pannello inferiore di Wireshark.
- Espandere la sezione *Real-Time Transport Protocol* per analizzare i campi di RTCP. Nel caso mostrato in figura, il campo "Packet Type" identifica l'applicazione specifica (4 byte) seguita dai dati dell'applicazione.



SINTESI

SERVIZI INTERNET

Il livello Applicazione di Internet è costituito da protocolli client/server utilizzati dagli utenti. Alcuni protocolli sono standard affermati: DNS, Posta Elettronica, FTP e i protocolli per la videoconferenza

DNS (DOMAIN NAME SYSTEM)

Il DNS è il servizio che associa a un nome di un host in Internet il corrispondente indirizzo IP. È un protocollo client/server che poggia su UDP e lavora sulla porta 53. Utilizza database distribuiti.

FTP

File Transfer Protocol (FTP) è utilizzato per accedere al file system di un server remoto. È un protocollo client/server che poggia su TCP e lavora su due porte: la porta 21 per l'invio dei comandi del protocollo e un'altra porta per il trasferimento dei dati (file).

INDIRIZZO DI POSTA ELETTRONICA

Ogni utente può avere una o più mailbox, alle quali accede autenticandosi con user name e password. A ogni mail box è associato un indirizzo univoco formato da:

1. nome utente
2. @ (simbolo "chiocciola" che significa "presso" e in inglese si legge "at")
3. nome server

GERARCHIA DEI NOMI

I nomi in Internet sono organizzati in una gerarchia di livelli (es: `www.unimi.it`)

- Primo livello: è rappresentato dall'etichetta più a destra.
- Secondo livello: in genere individua una organizzazione. Ogni dominio di secondo livello può contenere un indeterminato numero di domini di terzo livello.
- Livelli successivi: specificano via via i sottodomini di terzo livello, quarto livello, fino a individuare uno specifico host (ultima etichetta a sinistra del nome).

SERVER DNS

Il DNS è composto da una rete di name server (distributori di nomi) così organizzati:

- Server dei nomi locali (*Local Name Server*). La richiesta di risoluzione di un nome è inviata al server dei nomi locali di un'organizzazione, il cui indirizzo IP è inserito a mano nell'host. Il server dei nomi locali conosce l'indirizzo del root server.
- Server dei nomi radice (*Root Name Server*). Quando il server dei nomi locali non può soddisfare immediatamente la richiesta di un host, assume il ruolo di client DNS e invia la richiesta al Root Name Server.
- Server dei nomi assoluto (*Authoritative Name Server*) che ha le informazioni sulla corrispondenza tra nome dell'host e il suo indirizzo IP.

RECORD DELLE RISORSE

Struttura in cui sono organizzate le informazioni sui server DNS. Un record delle risorse è costituito dai seguenti campi: `<Name, Value, Type, Class, TTL>`

VIDEOCONFERENZA RTP-RTCP

RTP (*Real-time Transport Protocol*) è un protocollo utilizzato per la videoconferenza. Effettua il trasporto in tempo reale dei dati audio e video. Poggia su UDP.
È affiancato dal protocollo RTCP (*Real-Time Control Protocol*), che ne arricchisce le funzionalità.

POSTA ELETTRONICA

È un metodo di comunicazione testuale per inviare messaggi in formato digitale tramite la rete internet. Utilizza il protocollo SMTP per l'invio dei messaggi e i protocolli POP3 e IMAP per la lettura dei messaggi.

ARCHITETTURA

Il funzionamento del sistema di posta è diviso in due parti:

1. invio del messaggio (protocollo SMTP): il messaggio è inviato dal mittente a un server di posta che è sempre in esecuzione (*submission*) e qui memorizzato nella casella di posta del mittente (mailbox), quindi trasferito al server di posta in arrivo (*relay*) e qui memorizzato nella casella di posta del destinatario;
2. lettura del messaggio (protocollo POP3 o IMAP): il destinatario legge dalla sua casella di posta i messaggi ricevuti.

NOMI DI PRIMO LIVELLO

I TLD (*Top Level Domain*) sono divisi in due gruppi:

- Nazionali: ccTLD (Es. it per l'Italia, fr per la Francia…)
- Generici: gTLD, usati per indicare categorie generiche di siti web. Per esempio .com, .gov

STRUTTURA DEL MESSAGGIO

Una e-mail è formata da tre parti:

- Busta (*envelope*)
- Intestazione (*header*)
- corpo del messaggio (*body*)

SMTP

È il protocollo utilizzato per il trasferimento dei messaggi dal mittente fino al server del destinatario. È un protocollo client/server che poggia su TCP e lavora sulla porta 25.

POP3

È un protocollo utilizzato dal client di posta del destinatario per accedere alla sua casella di posta e leggere le mail che, una volta scaricate, sono eleminate dalla casella di posta sul server.
È un protocollo client/server che poggia su TCP e lavora sulla porta 110.

IMAP

È un protocollo client/server utilizzato dal client di posta del destinatario per accedere alla sua casella di posta e leggere le mail che permangono sul server. Consente all'utente di gestire la propria casella di posta da qualsiasi dispositivo. Poggia su TCP e lavora sulla porta 143.

Verifica delle CONOSCENZE

Vero o Falso?

1 DNS è usato per tradurre indirizzi IP in nomi Internet. V F

2 I nomi dei server in Internet sono di tipo gerarchico. V F

3 Il DNS è un protocollo di livello applicazione. V F

4 .org è un dominio di primo livello. V F

5 DNS poggia su TCP. V F

6 POP3 lavora sulla porta 25. V F

7 SMTP è un agente di trasferimento. V F

8 Il protocollo SMTP trasferisce messaggi da un server a un altro. V F

9 `RETR` è un comando SMTP. V F

10 Per usare SMTP gli utenti devono essere connessi a Internet contemporaneamente. V F

11 Il tipo MIME serve per trasmettere dati speciali. V F

12 `RCPT TO` è un comando SMTP. V F

13 FTP lavora sulle porte 20 e 21. V F

14 FTP trasferisce pagine Web. V F

15 DNS utilizza un'unica tabella residente su un server in Internet. V F

16 Type A indica che *name* è un indirizzo IP. V F

17 I nomi dei server Internet sono usati perché più facili da ricordare. V F

18 La posta elettronica non utilizza protocolli di livello trasporto perché usa gli agenti di trasferimento. V F

19 Una Web mail non usa protocolli di livello applicazione. V F

20 La mail-box è uno spazio di memoria. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

21 Il DNS restituisce:

a. solo indirizzi IP
b. solo nomi dei server
c. dei valori il cui significato dipende dal campo type
d. dei record delle risorse

22 Il DNS non è un protocollo client-server perché:

a. quando viene invocato non si conosce l'indirizzo del server
b. è solo un traduttore
c. non c'è il server
d. nessuna delle precedenti risposte è esatta

23 I Mail User Agent:

a. trasferiscono i messaggi tra i server
b. trasferiscono i messaggi tra i client
c. inviano i messaggi dal computer locale dell'utente al server del destinatario
d. inviano i messaggi dal server del mittente al computer locale del destinatario

24 I campi *to* e *from*:

a. sono comandi di POP3
b. fanno parte dell'intestazione del protocollo SMTP
c. fanno parte del body SMTP
d. sono usati dal client per connettersi al server

25 Il campo *Content-Type*:

a. contiene il messaggio
b. specifica una categoria a cui associare il contenuto del messaggio (cucina, giardinaggio, …)
c. specifica il tipo di dati presenti nel messaggio
d. è specificato nell'object

Domande per la prova orale

26 Qual è lo scopo del DNS e cosa rappresentano i record A, CNAME, MX?

27 Quali sono le differenze tra i protocolli SMTP, POP3 e IMAP?

28 Cos'è il protocollo FTP e quando è necessario utilizzarlo?

29 Descrivi l'architettura del sistema di posta elettronica.

30 Descrivi l'architettura del servizio DNS.

31 Come è strutturato il nome di un host in Internet?

32 Come sono organizzati i server DNS?

33 Qual è il significato della 5-upla < name, value, type, class, TTL>?

34 A che livello dell'architettura di rete si colloca il DNS? Su quale porta lavora?

35 Quali sono le caratteristiche principali di RTP (*Real-time Transport Protocol*)?

Verifica delle ABILITÀ

36 Un utente sta navigando nel Web e sta visualizzando una pagina. A un certo punto "clicca" su un punto sensibile (collegamento ipertestuale) e gli appare un'altra pagina Web.
Descrivi come funziona il sistema e che cosa è successo da quando ha "cliccato" a quando ha visualizzato la nuova pagina.

37 Completa la seguente tabella.

	Esempio	Differenze	Servizio che effettua la risoluzione del nome
Nomi dei calcolatori in Internet	.....	.....	.....
Indirizzi dei calcolatori in Internet	.....	.....	.....

38 Si consideri il protocollo SMTP. Si supponga che Anna (client `abc.com`) voglia inviare un messaggio di posta elettronica a Paolo (cliente di un ISP che riceve posta su `xyz.com`). Il messaggio è inerente alle sue vacanze estive. Definisci il protocollo in maniera schematica utilizzando i comandi opportuni.



39 Utilizza il simulatore Wireshark per catturare un messaggio DNS e analizzane i principali campi.

40 Progetta, utilizzando Packet Tracer, una rete in cui un client HTTP effettua una richiesta a un server HTTP, passando da un server DNS per la risoluzione del nome.

41 Completa la tabella indicando il numero di porta e il protocollo di livello trasporto usati dai servizi indicati.

Servizio	Porta
SMTP	.....
SMTP sicuro	.....
POP3	.....
POP3 sicuro	.....
IMAP	.....
IMAP sicuro	.....
DNS	.....
FTP	.....

PDF
Esercizi in più

The HTTP protocol

Abstract

In addition to the WWW supported by the HTTP protocol, other Internet services are widespread and used, each supported by a particular protocol. The DNS is primarily used for resolving Internet names. In general, users refer to Internet hosts via the names that can be easily remembered and have a hierarchical structure.
In fact, the network and transport layer protocols use IP addresses to reference a node in the network: the DNS is an application that solves the problem of translating a name into an IP address. Another popular service is the e-mail service. This is structured into two parts: one, implemented by the SMTP protocol, to transfer messages among servers that host the users' mailboxes; the other, implemented by the POP3 protocol, to allow the user to see the recipient's mailbox.
The FTP is typically used for client to server file transfer. It requires authentication and is the most commonly used method to publish on the Internet.

Questions

Answer all questions

1 List the differences between an Internet name and an IP address

2 Describe the architecture of an e-mail system

3 What are first level domains?

4 Why does FTP use two ports?

Choose the correct answer

5 The DNS service:
- a uses the TCP protocol
- b is solely used to provide an IP address
- c is an application layer protocol
- d is a transport layer protocol

6 A mail box:
- a is an electronic mail service
- b is a memory space
- c is a transfer agent
- d is a network protocol

7 The FTP protocol:
- a can only transfer files
- b allows to operate on the system of a remote host
- c is a mail service
- d uses port 25

8 The POP3 protocol:
- a transfers messages from the sender's mail server to the recipient's mail server
- b allows the user to consult his/her mailbox
- c uses ports 20 and 21
- d is used for HTML file transfer

Crosswords

Across

1 Internet name resolver

4 Type for mail server name

5 Top-level domain

7 Used for e-mail transfer

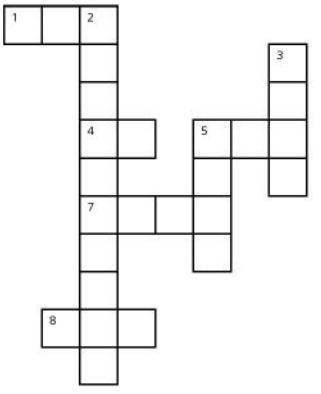
8 TLD for government sites

Down

1 Transfer of e-mail from the client to the sender's server

3 An SMTP command

5 Specifies the meaning of Value in the resource record



Verifica delle COMPETENZE

Tema 1

1 Dopo aver descritto la struttura di un URL, esponi il significato di:
`http://www.abcd.com/prodotti.html`

2 Indica schematicamente i passi che vengono eseguiti quando un utente, esplorando il Web, "clicca" su un collegamento ipertestuale.

3 Considera il contenuto della barra degli indirizzi.

https://www.ricettario.it/menu/proposta.php?primo=risotto&secondo=arrosto

a Supponendo di voler ottenere lo stesso risultato utilizzando un form, completa il tag seguente:

```
<form action="..." method="...">
Nome:    <input type="text" name="...">
Mese:    <input type="text" name="...">
```

b Indica il contenuto della QUERY_STRING: .....

4 Considera la seguente situazione:
il 12 dicembre 2024 alle ore 13.00 Anna, cliente dell'ISP `nomesito` (`anna@nomesito.it`) deve mandare un messaggio a Marco, cliente di `nomesito1` (`marco@nomesito1.it`) per disdire un appuntamento. Il testo del messaggio è il seguente: «Mi dispiace, non posso venire a cena. Ci vediamo un'altra volta. A presto. Anna.» Solitamente Marco legge la posta tutte le sere, verso le ore 21.00. Quella sera Marco si collega a `nomesito1.it` e trova cinque messaggi, di cui quello di Anna è il numero 3.



Scrivi la sequenza di comandi SMTP C/S per inviare tutte le informazioni di cui sopra e la sequenza dei comandi POP3 C/S per scaricare il messaggio di Anna.

5 Considera la seguente riga:

`http/1.1 404 NOT FOUND`

Indica il significato e il contesto in cui è utilizzata.

6 Dopo avere esposto la sintassi del protocollo HTTP (C/S), fai le dovute considerazioni sulle differenze tra i protocolli SMTP e HTTP (mettili a confronto).

7 Completa la tabella.

Applicazione	Porta	Applicazione	Porta
HTTP	.....	HTTPS	.....
SMTP	.....	SMTPS	.....
POP3	.....	POP3S	.....
FTP	.....	FTPS	.....

8 Considera il seguente form contenuto in una pagina web:



a. Scrivi il relativo codice HTML.

b. Supponendo di utilizzare il metodo "get", scrivi il contenuto della variabile "QUERY_STRING" dopo l'attivazione di INVIA.

9 Esponi la differenza tra pagina web statica e pagina web dinamica.

10 Dopo aver citato tutti i "metodi" previsti da HTTP, ipotizza una sessione di lavoro HTTP nella quale ci si deve collegare al sito

`www.cangurus.au/cang/send.php?n=1&t=urgent`

con Telnet o PuTTY. Scrivi tutti i comandi e le risposte che si devono dare e ricevere dal server per ottenere la pagina richiesta.

11 Esponi le caratteristiche (definizione, consiste in..., usato per..., ecc.) dei seguenti servizi Internet: MIME, DNS, FTP, ISP, HTTP, POP3.

12 Bob (`bob@gbob.com`) vuole inviare ad Alice (`alice@gali.edu`) una e-mail, che contiene il messaggio "Ciao", tramite il protocollo SMTP. Quali comandi deve dare?

13 Fai un esempio di URL di tipo gTLD, che comprenda un dominio di secondo livello con un server che ha nome `plutus`.
Il server contiene un albero di due cartelle (`/cartpippo/paper`) e un file di nome `zio.jpg`.

14 Confronta il sistema di posta elettronica con il sistema di posta ordinario. Evidenzia vantaggi e svantaggi dell'uno e dell'altro.

15 Confronta il sistema di posta elettronica con i sistemi di messaggistica istantanea. Evidenzia vantaggi e svantaggi dell'uno e degli altri. Considerando il galateo (*netiquette*), quali consigli (almeno quattro) daresti per scrivere una e-mail di risposta all'inserzione relativa a un'offerta di lavoro o per parlare con i colleghi di lavoro?

16 Il programmatore è stato molto distratto nel suo collegamento a un server web, usando PuTTY, per prelevare il file `theproj.htm` che risiede nella root del server. Puoi aiutarlo a riscrivere correttamente la sessione?

```
(C=client, S=Server))
C: GET http://www.w3.org/www/theproj.htm
S: Host: www.w3.org
S: Accept: image/gif
S:User-Agent: sapo/2.0
S: HTTP/1.1 Status OK Document follows
S: Server: Apache/1.3.27
S: content type: image/html
C: <HTML>...
..... documento HTML .....
C:<HTML>
```

17 Utilizza Postman per ottenere da `www.jsonplaceholder.org` le seguenti informazioni:

- dati dell'utente id=1;
- dati di tutti gli utenti;
- inviare un nuovo post.

Per ciascuna richiesta specifica l'API endpoint utilizzata.

18 Utilizza Packet Tracer per progettare una rete che disponga di:

- un server web;
- un server di posta elettronica;
- un server DNS.

Utilizza il servizio DNS per risolvere il nome di un host (`www.pallino.it`) presente nell'URL usato per la richiesta di una pagina web. Configura i client di posta e il server di posta affinché due dispositivi della rete possano inviare e ricevere e-mail.

Orientamento al lavoro

ORIENTAMENTO STEM Tema 1

Applicazioni Web

Contesto

Le applicazioni web e mobile stanno cambiando rapidamente, diventando sempre più interattive e facili da usare rispetto alle soluzioni tradizionali. Viviamo in un'epoca di grande innovazione tecnologica, dove l'Intelligenza Artificiale accelera i cambiamenti e ci costringe a rivedere continuamente i nostri metodi di lavoro. La sfida principale è trovare un equilibrio tra innovazione, design avanzato e scalabilità, per creare soluzioni su misura che possano crescere con le esigenze dei clienti. L'AI gioca un ruolo cruciale in questo contesto, migliorando l'interattività e la personalizzazione delle applicazioni, prevedendo le tendenze future e garantendo la sicurezza. Così facendo, si riduce il rischio che le soluzioni proposte diventino obsolete e si aumenta il ritorno sull'investimento, assicurando un valore duraturo.

Intervista a

Enthonj Franco, classe 1990, informatico con una profonda passione per la scienza e la tecnologia. Lavora da 15 anni con un approccio innovativo all'interno di una piccola ma dinamica azienda specializzata in analisi dati, consulenza e sviluppo di applicazioni web e mobile su misura per le aziende. I settori in cui opera variano dal farmaceutico all'aerospaziale.
Attualmente ricopre un ruolo manageriale e guida il team di sviluppo verso il raggiungimento degli obiettivi di progetto. Partecipa attivamente a tutte le fasi del processo, dalla risoluzione dei bug alla pianificazione e valutazione dei tempi. Il suo obiettivo è trasformare idee in soluzioni concrete, unendo competenze tecniche e strategiche.

Quali sono i settori aziendali che si occupano di applicazioni web e in cosa consistono le applicazioni web che sviluppa?

Il mondo delle web app richiede una combinazione di competenze tecniche e gestionali, coinvolgendo professionisti di vari settori.
L'analisi dei dati elaborati dall'Intelligenza Artificiale sta trasformando numerosi ambiti. Il mercato dei cloud provider è in espansione, con nuove aziende che competono con i giganti del settore. Anche i servizi finanziari stanno evolvendo, adottando pratiche delle grandi aziende tecnologiche e offrendo sempre più servizi tramite app e portali web, riducendo la necessità delle filiali tradizionali.
Nel settore sanitario, le web app facilitano la telemedicina e la gestione dei dati dei pazienti, permettendo consulti online e monitoraggio della salute. Nell'istruzione, l'e-learning è in forte crescita grazie a piattaforme dedicate. Nel marketing, si sviluppano strumenti per l'analisi e la gestione delle campagne pubblicitarie online. Infine, i media e l'intrattenimento utilizzano web app per servizi di streaming e social networking.
In questo contesto, molte professioni sono coinvolte nello sviluppo e nella gestione delle web app. Queste vanno dal marketing e design, che attraggono clienti e migliorano l'esperienza utente, agli analisti di dati e ingegneri dei processi, i cui lavori spesso non sono visibili agli utenti finali.

Chi sono i clienti e i fornitori?

L'azienda per cui lavoro è una piccola realtà che, grazie all'esperienza e alle competenze acquisite in quasi vent'anni di attività, collabora con grandi multinazionali. Il nostro approccio fortemente orientato all'innovazione e l'attenzione personalizzata che riserviamo ai clienti ci hanno permesso di differenziarci dalle grandi società di consulenza, ottenendo la piena soddisfazione di chi utilizza i nostri prodotti o si avvale del nostro know-how. A differenza dei nostri concorrenti, che propongono soluzioni standard con limitate possibilità di personalizzazione, il nostro punto di forza è la capacità di sviluppare soluzioni su misura, particolarmente apprezzate nel settore business.
Nel corso degli anni, abbiamo anche sviluppato un team dedicato alla consulenza e allo sviluppo nel settore e-learning. In particolare, forniamo soluzioni per corsi professionali ed esami online, certificati secondo le normative degli enti autoritativi di diversi paesi.
Il nostro principale fornitore è il servizio di connettività, che ci garantisce manutenzione e monitoraggio costante per la sicurezza del data center dove si trovano i nostri server dedicati. Collaboriamo inoltre con diversi fornitori di software per le nostre operazioni quotidiane, come la piattaforma

che utilizziamo per la gestione del codice e la risoluzione di problemi e richieste di modifica su progetti specifici. Per l'hardware, ci affidiamo a vari fornitori per la scelta e l'acquisto di dispositivi fisici, come PC, tablet e smartphone.

Qual è il mercato oggi e qual è la previsione per i prossimi anni?

Il mercato dello sviluppo software è in piena espansione, trainato dalla crescente digitalizzazione in molti settori. L'Intelligenza Artificiale gioca un ruolo sempre più centrale, consentendo alle aziende di ottimizzare i processi e analizzare i dati con maggiore efficacia. Non solo le grandi aziende tecnologiche, ma anche aziende tradizionalmente lontane dal mondo tecnologico, come istituti di credito e aziende di produzione, stanno investendo in queste innovazioni per non restare escluse dalla rivoluzione digitale.
Le previsioni indicano una continua crescita del mercato, alimentata dagli investimenti in AI e automazione, che permetteranno alle imprese di migliorare i processi e adattarsi rapidamente ai cambiamenti del mercato. L'attenzione all'esperienza utente e all'interfaccia è diventata fondamentale, poiché le applicazioni più intuitive aumentano la soddisfazione del cliente e la fidelizzazione, aspetti cruciali in un mercato sempre più competitivo e in rapida evoluzione.
In sintesi, il settore dello sviluppo software sta attraversando una trasformazione senza precedenti, con prospettive future molto promettenti per le aziende che sapranno innovare e adattarsi alle nuove sfide. L'Intelligenza Artificiale sta rivoluzionando il modo in cui le applicazioni vengono sviluppate e utilizzate, permettendo una maggiore automazione e personalizzazione.

Qual è la figura professionale che è richiesta in questo ambito?

Nel settore informatico, le figure professionali più richieste sono quelle in grado di affrontare le sfide legate alla digitalizzazione e all'automazione. Gli sviluppatori versatili (full-stack) sono particolarmente ricercati per la loro capacità di lavorare sia sulla parte visibile (front-end) che su quella nascosta (back-end) delle applicazioni web e mobile. Allo stesso tempo, con la crescente importanza dei dati, gli scienziati dei dati (data scientist) e gli ingegneri dei dati (data engineer) sono fondamentali per l'analisi e la gestione delle grandi quantità di informazioni che le aziende raccolgono. Gli esperti in Intelligenza Artificiale e apprendimento automatico (machine learning) sono altre figure chiave, poiché le imprese cercano di implementare soluzioni automatizzate per ottimizzare i processi e migliorare l'efficienza. Infine, gli ingegneri delle operazioni di sviluppo (DevOps), che si occupano di migliorare la collaborazione tra i team di sviluppo e quelli delle operazioni IT, stanno diventando sempre più importanti perché aiutano a creare, testare e distribuire il software in modo più efficiente.

Che tipo di formazione deve avere?

Per trovarsi a proprio agio in questo settore, la formazione ideale dovrebbe essere basata su materie scientifiche, con una solida preparazione in informatica o in discipline correlate come ingegneria informatica, ingegneria elettronica, matematica e fisica. Un percorso di studi universitario in questi ambiti fornisce le basi teoriche e pratiche necessarie, come la programmazione, le strutture dati, gli algoritmi e i sistemi operativi.
La formazione continua è un altro aspetto fondamentale, poiché il settore evolve rapidamente e le tecnologie cambiano costantemente. Approfondimenti su temi attuali come l'Intelligenza Artificiale, il machine learning, le operazioni di sviluppo, la sicurezza informatica e la gestione dei dati sono importanti per non diventare obsoleti insieme al codice. In questo contesto, una buona padronanza dell'inglese, ancora una difficoltà per molti italiani, rappresenta un requisito essenziale.
Inoltre, per eccellere in questo campo è importante sviluppare competenze trasversali. Abilità come il problem solving, il pensiero analitico e la capacità di lavorare in team multidisciplinari sono cruciali per affrontare le sfide del settore. Anche la conoscenza di metodologie agili, come Scrum, e di gestione dei progetti completa il bagaglio ideale di competenze. Infine, può sembrare scontato, ma è fondamentale ricordare che l'ingrediente più importante è la passione con cui si fanno le cose.

Ci racconta un po' la sua esperienza, la sua storia, il rapporto con colleghi?

La mia passione per l'informatica è nata fin da subito, a metà degli anni Novanta, armeggiando con il Commodore 64 di mio fratello. Più che giocare, ero affascinato dal funzionamento della macchina: la tastiera, il lettore a nastro e i comandi da digitare. Sono sempre stato attratto dal "dietro le

quinte" della tecnologia: smontare dispositivi, trovare glitch nei videogiochi, superare limiti imposti. Ricordo con entusiasmo quando, da bambino, giocando con il GameBoy della Nintendo, ho scoperto un bug che mi ha permesso di creare un Pokémon imbattibile. Un'altra esperienza è stata quella di stabilire un record di "impennata" in GTA Vice City, sfruttando un albero nascosto nella mappa del gioco che mi permetteva di mantenere la moto in equilibrio all'infinito. Mentre la PlayStation girava da sola, sono uscito a fare un giro in bicicletta con un amico, tornando dopo qualche ora per scoprire di aver realizzato un record difficilmente replicabile senza questo trucco.
Durante gli anni delle scuole superiori, frequentando l'istituto tecnico con indirizzo informatico, l'utilizzo del computer è diventato quotidiano. Dividevo i miei pomeriggi scrivendo le prime righe di codice per realizzare semplici applicazioni, videogiochi e i primi siti web statici, oltre a produrre musica elettronica nel tempo libero rimasto. È stato allora che ho capito che la programmazione era la mia vera vocazione.
Dopo il diploma, sono entrato a far parte dell'azienda dove tuttora lavoro, che mi ha offerto l'opportunità di crescere professionalmente. Ho approfondito le mie conoscenze in algoritmi, basi di dati e linguaggi di programmazione, acquisendo sul campo competenze tecniche ma anche gestionali. Oggi mi occupo di tutto il ciclo di vita di un progetto, dalla fase di analisi iniziale alla gestione del team di sviluppo e al rapporto con il cliente.
Una delle soddisfazioni più grandi è aver visto crescere il nostro team da tre a tredici persone. Condividiamo tutti la passione per l'informatica e questo ci rende un gruppo coeso e affiatato.

La cosa più bella e quella più brutta della sua esperienza lavorativa?

L'ambiente aziendale dinamico in cui lavoro, unito alla possibilità di operare su progetti e settori diversi, mi ha consentito di ampliare le mie competenze e di affrontare sfide sempre nuove. Credo che il vero piacere di questa professione risieda proprio nel trovare soluzioni agli ostacoli: dall'intuizione che risolve un bug software complesso, all'ottimizzazione di un processo lento, fino al gusto di risolvere rompicapi tecnici. Tra i ricordi più positivi, c'è sempre la soddisfazione di ricevere il riconoscimento del cliente per il lavoro svolto.
Il rapporto con i colleghi, nel corso degli anni, è stato sempre positivo e collaborativo, creando un ambiente di lavoro stimolante e produttivo. La condivisione di metodologie ed esperienze tecniche è fondamentale, e i progetti realizzati hanno spesso contribuito a migliorare l'efficienza dei clienti.
Ovviamente ci sono stati anche momenti difficili, fortunatamente rari. Ricordo un episodio in cui il cliente ci accusava di causare rallentamenti con il nostro software, e abbiamo trascorso giorni intensi cercando di individuare il problema, per scoprire che la causa era un disco del server NAS, di cui noi non avevamo il controllo. Un altro caso singolare è stato quando, dopo mesi di sviluppo e continui cambiamenti nelle specifiche, il cliente ha affermato di aver replicato l'intero applicativo in meno di una settimana utilizzando ChatGPT, mettendo così in dubbio il nostro operato. L'Intelligenza Artificiale ha certamente un enorme potenziale, ma a volte qualcuno sembra scivolare nella fantascienza...

È contento del suo lavoro? Lo rieglierebbe?

Nonostante mi trovi spesso a dover affrontare la pressione derivante dal carico lavorativo e un conseguente aumento dello stress, che talvolta rende complessa la gestione delle problematiche legate ai progetti, sono riuscito a mantenere saldo il mio impegno grazie a una forte passione per il mio lavoro. Questa passione, unita al desiderio di esprimere la mia creatività, mi permette di vedere ogni sfida come un'opportunità per crescere e migliorare. La soddisfazione che deriva dal trovare nuove soluzioni innovative, risolvendo problemi complessi, è ciò che mi spinge a superare le difficoltà quotidiane. In un settore in continua evoluzione, colmo di novità rivoluzionarie, ho la possibilità di imparare costantemente e di sperimentare tecnologie all'avanguardia, o nuove funzionalità che possono tornare utili anche nella vita quotidiana al di fuori del lavoro. Questo stimolo mi dà conferma di aver fatto le scelte professionali giuste fino a oggi, rafforzando la mia motivazione a continuare su questa strada, non facile, ma senza dubbio mai noiosa.

Sfida finale

ORIENTAMENTO STEM

Tema 1

L'evoluzione di Internet

Scenario

Ti viene chiesto di riflettere sulla seguente analogia proposta da Gino Roncaglia, che rapporta l'evoluzione di Internet con le diverse fasi della storia umana e mette in luce come, nonostante la sterminata quantità di informazioni, i contenuti in rete siano, nella maggior parte dei casi, granulari e frammentati.

Le età di Internet: dalla preistoria all'età delle cattedrali

- **Cacciatori-raccoglitori**. All'inizio, negli anni Ottanta-Novanta del secolo scorso, gli utenti di Internet erano come cacciatori-raccoglitori, alla ricerca dei pochi contenuti digitali disponibili. Piccole tribù di nerd si spingevano in brevi scorribande nello spazio virtuale, per quanto era loro consentito da connessioni precarie con il loro modem, per raccogliere quello che trovavano in rete e consumarlo poi nella "caverna" del proprio home computer una volta staccata la connessione.
- **Agricoltori e primi insediamenti**. Con la nascita del Web (da metà degli anni Novanta al 2000), si sono formati i primi insediamenti informativi, simili ai primi villaggi agricoli. Il termine "sito web" non è casuale: un insediamento informativo, luogo di "coltivazione" dei contenuti e punto di riferimento per gli utenti che lo visitano.
- **Artigiani e mercanti**. Dall'inizio degli anni 2000, con il Web 2.0, lo scenario cambia e si moltiplicano i contenuti generati dagli utenti, che non sono più ancorati a un singolo sito web, ma circolano e vengono scambiati. Spesso si tratta di contenuti brevi e frammentati come nei social network, con la conseguente perdita delle competenze legate alla complessità.



Cacciatori-raccoglitori
Gli utenti di Internet hanno connessioni precarie che li costringono a brevi scorribande virtuali alla ricerca dei pochi contenuti digitali disponibili. Assomigliano a cacciatori-raccoglitori preistorici.

1980-90 — 1995-2000



Agricoltori e primi insediamenti
Con la nascita del web, si formano i primi insediamenti informativi, simili ai villaggi agricoli. I "siti web" divengono punti di riferimento per gli utenti.

↑ **Fig. A** Le età di Internet.

- **Costruttori di cattedrali**. Il futuro potrebbe vedere la costruzione di contenuti digitali complessi e strutturati, simili alle grandi cattedrali del passato, come già è possibile vedere in embrione in Wikipedia (2001). L'avvento dell'Intelligenza Artificiale, che può creare testi, immagini, musica e video complessi partendo da semplici input, potrebbe aiutare a produrre contenuti articolati e strutturati. Strumenti come ChatGPT (2022) e altri modelli generativi stanno rivoluzionando molte industrie creando testi, immagini, video e altro partendo da semplici prompt.

Decidi, in base alla tua esperienza personale e con l'utilizzo di diverse fonti (rete, amici, compagni, genitori, docenti, AI), di approfondire questo argomento partendo dallo studio della nascita del Web e del suo sviluppo fino a oggi.

Obiettivi

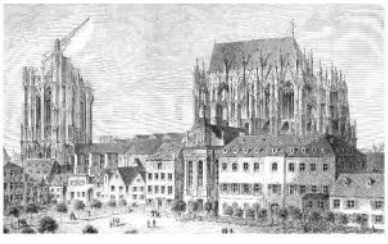
- **Studiare la nascita e lo sviluppo del Web dalle origini a oggi.**
- **Intercettare le principali parole chiave del Web.**
- **Approfondire le innovazioni tecnologiche recenti e significative, come l'Intelligenza Artificiale Generativa, e analizzare il suo impatto nella costruzione di contenuti digitali complessi e strutturati.**
- **Riflettere sui rischi del Web (fake news, hate speech…) per una maggiore consapevolezza dei rischi digitali.**
- **Sviluppare competenze di cittadinanza attiva, utilizzate come quadro di riferimento per le attività a livello dell'Unione Europea, nazionale e regionale.**
- **Organizzare un confronto per sostenere o confutare le idee presentate.**

Artigiani e mercanti
Con il Web 2.0, i contenuti generati dagli utenti si moltiplicano e circolano liberamente, spesso in forma breve e frammentata come nei social network.



2000

2001-2022



Costruttori di cattedrali
Wikipedia è un esempio di contenuti complessi e strutturati, simili alle cattedrali del passato. ChatGPT e altri modelli generativi rivoluzionano la vita creando testi, immagini, video e altro partendo da semplici prompt.

Consegna

1. Consultare e analizzare i documenti proposti, cercare altri documenti affidabili, utilizzare le vostre esperienze personali in rete, con AI e sui social network.
2. Redigere un documento finale in forma tabellare per sintetizzare il risultato della ricerca e del confronto. La tabella deve contenere delle "parole chiave" che sintetizzano un concetto ritenuto rilevante (di seguito è fornita una Traccia con esempi), con le fonti utilizzate per attuare argomentazioni pro e contro.

Traccia

Parola Chiave	Concetto Rilevante	Fonte	Argomentazioni Pro	Argomentazioni Contro
Nascita del Web	Evoluzione da cacciatori-raccoglitori ad agricoltori.	*L'età della frammentazione* di Gino Roncaglia.	Rivoluzione nell'accesso all'informazione.	Contenuti frammentati e granulari.
Web 2.0	Artigiani e mercanti.	Wikipedia	Maggiore partecipazione degli utenti.	Perdita di competenze legate alla complessità.
Intelligenza Artificiale	Costruttori di cattedrali, ChatGPT e modelli generativi.	Rapporti dell'Unità Europea e del World Economic Forum.	Creazione di contenuti complessi e articolati.	Rischi legati alla trasparenza e all'uso improprio.
Regolamenti sull'AI	Uso dell'Intelligenza Artificiale: trasparenza, uso pubblico, sistemi ad alto rischio.	Regolamenti UE sull'uso dell'Intelligenza Artificiale.	Maggiore controllo e trasparenza.	Potenziali limitazioni all'innovazione.
Rivoluzione digitale/mentale	Impatto delle nuove tecnologie sull'evoluzione umana. La fine delle mediazioni. Smaterializzazione.	*The Game* di Alessandro Baricco: «il mondo digitale come un effetto e non come una causa».	Maggiore accesso diretto alle informazioni. Riduzione dei costi e accessibilità.	Perdita di contesti e mediazioni professionali. Rischi di sicurezza informatica. Sfide etiche e morali.
Hate speech (Cyberbullismo, Cyberstalking, Sexting...)	Problemi legati alla comunicazione online.	Rapporti su Cybersecurity.	Maggiore consapevolezza dei rischi digitali.	Rischi per la sicurezza personale e psicologica.
Fake news	Motivazioni e modalità di diffusione delle notizie false.	Rapporti su fenomeni sociali.	Maggiore consapevolezza dei rischi digitali e verifica delle fonti.	Difficoltà nel controllo e nella mitigazione. Rischi per la salute fisica e mentale.

Interroghiamo l'Intelligenza Artificiale

Tema 1



Tu e un tuo compagno o una tua compagna scegliete 5 domande dall'elenco.

Successivamente, lavorando individualmente, interrogate l'AI usando due chatbot diverse. Ciascuno conserva le schermate con le risposte e riassume le risposte ottenute. Infine, confrontate le risposte. Le chatbot hanno dato risposte analoghe? Oppure ci sono state differenze? Quando tu e il tuo compagno o la tua compagna avete riassunto le risposte della chatbot, avete considerato come importanti gli stessi concetti?

1. Come cambieranno i libri di testo con l'ausilio dell'Intelligenza Artificiale nei prossimi anni?
2. Ci serviremo ancora della posta elettronica nel futuro o quella funzione verrà delegata ai social?
3. Qual è la differenza tra HTTP e HTTPS?
4. Come evolverà il protocollo HTTP/HTTPS nei prossimi anni?
5. Quali sono i principali metodi HTTP (GET, POST, ecc.) e come vengono utilizzati?
6. Cos'è un URL e quali sono le sue parti principali?
7. Qual è il ruolo di un server web in una comunicazione HTTP?
8. Spiega il concetto di codice di stato HTTP e fornisci alcuni esempi (es. 200, 404, 500).
9. Cos'è un cookie e a cosa serve nel contesto del Web?
10. Qual è il ruolo delle sessioni HTTP nella navigazione?
11. Come funziona il caching HTTP e perché è importante?
12. Quali sono le differenze tra un sito statico e un sito dinamico?

13. Spiega il funzionamento di un browser web nella gestione di una pagina HTML.

14. Qual è il ruolo delle API REST nel contesto del Web?

15. Come vengono implementate le connessioni sicure tramite HTTPS?

16. Quali sono gli sviluppi previsti per il Web nei prossimi tre anni?

17. Cos'è un server DNS e qual è la sua funzione?

18. Come funziona la traduzione dei nomi di dominio in indirizzi IP?

19. Cos'è un indirizzo IP e qual è la differenza tra IPv4 e IPv6?

20. Qual è il ruolo dei server di posta elettronica nel servizio e-mail?

21. Spiega la differenza tra POP3, IMAP e SMTP.

22. Quale sarà la relazione tra i motori di ricerca e l'Intelligenza Artificiale?

23. Qual è la differenza tra un protocollo client-server e un protocollo Peer-to-Peer?

24. Cos'è il VoIP e quali sono i suoi vantaggi rispetto alla telefonia tradizionale?

25. Cos'è il Cloud Computing e quali sono i suoi principali vantaggi?

26. Come viene garantita la sicurezza nei servizi di cloud storage?

27. A quali cambiamenti della mentalità pensi che potrebbe portare l'uso dell'Intelligenza Artificiale nelle ricerche sul Web?

28. Qual è il ruolo dei certificati digitali nei servizi online?

29. Quali sono i principali protocolli utilizzati per la videoconferenza online?

30. Come l'utilizzo dell'Intelligenza Artificiale potrebbe cambiare la videoconferenza?

31. Quale sarà l'impatto dell'Intelligenza Artificiale sui programmi scolastici?

32. L'uso di un portafoglio digitale ha modificato i comportamenti dei consumatori? In che modo?

Tema 2

Sicurezza di un sistema informatico

Unità

3 La sicurezza informatica
4 Crittografia e autenticazione
5 La sicurezza perimetrale
6 VPN e protocolli sicuri
7 Le reti senza fili

Prerequisiti

- Architettura di Internet
- Architettura Client/Server
- Protocollo HTTP
- Protocollo TCP
- Protocollo IP
- Elementi base di un router
- Configurazione di rete di un dispositivo
- Elementi base di progettazione reti locali

Conoscenze

- Fondamenti della sicurezza informatica
- Attacchi, minacce e tecniche di difesa
- Vulnerabilità
- La crittografia
- L'autenticazione
- I firewall
- La DMZ
- Le Access Control List
- Il proxy server
- Le VPN
- I protocolli sicuri

Abilità

- **Progettare** reti interconnesse con attenzione all'aspetto della sicurezza
- **Conoscere** le tecniche di crittografia
- **Conoscere** le tecniche di autenticazione
- **Comprendere** il funzionamento dei protocolli sicuri

Competenze

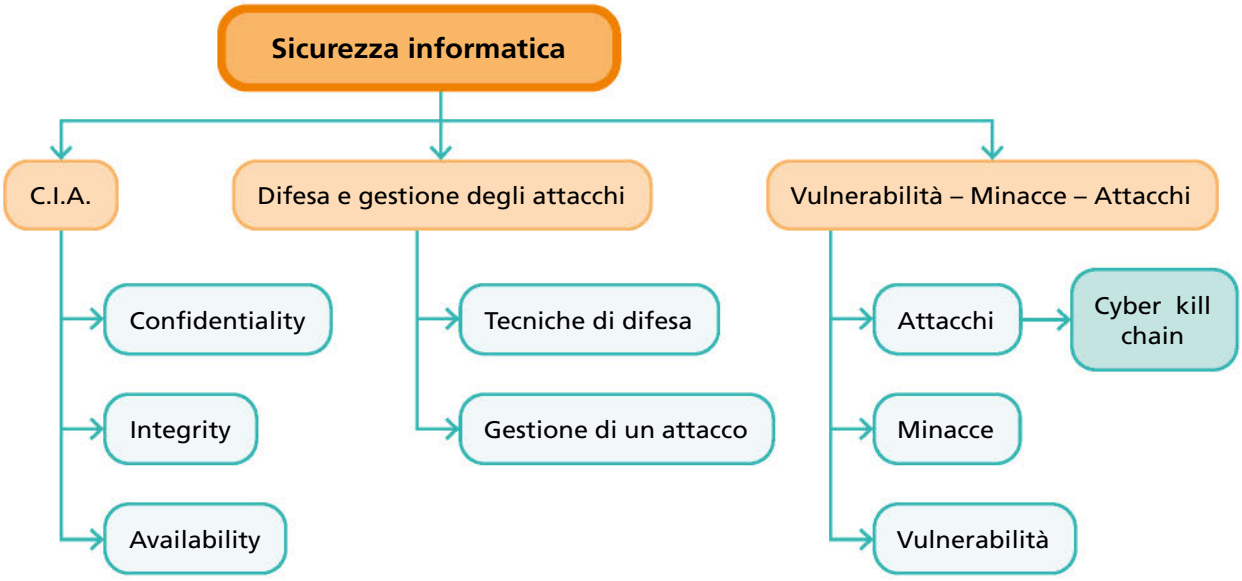
- **Gestire** progetti secondo le procedure e gli standard previsti dai sistemi aziendali di gestione della qualità e della sicurezza
- **Configurare** sistemi di sicurezza perimetrale
- **Configurare** VPN
- **Comprendere** l'importanza della pianificazione e della gestione della sicurezza informatica all'interno di un'organizzazione



Unità

3

La sicurezza informatica



Visione d'insieme

- Obiettivi della sicurezza informatica.
- Vulnerabilità, minacce, attacchi relativi a un sistema informatico.
- Tecniche di difesa e di gestione di un attacco informatico.

1 Introduzione

Domenica, 1 agosto 2021. È domenica sera. Roma è ancora in area gialla per le restrizioni legate alla pandemia di COVID-19. Anche oggi Giulia ha dovuto fare i conti con le misure di sicurezza necessarie a contrastare l'influenza. È preoccupata per il perdurare della pandemia e decide di prenotare il vaccino sul sito della Regione Lazio. Ci prova, ma il sito è irraggiungibile. Dopo qualche tentativo vano, Giulia lascia perdere, imprecando contro le istituzioni pubbliche. Tuttavia, questa volta ha torto. Non si tratta di un comune malfunzionamento: nella notte tra sabato e domenica, la Regione Lazio è stata colpita da un pesante attacco informatico, un ransomware (un atto di estorsione che richiede un riscatto), che ha bloccato tutti i servizi.

Venerdì, 12 maggio 2017. I sistemi di rilevazione di tutto il mondo stanno segnalando un attacco massiccio di ransomware. Con il passare delle ore, quello che sembrava un normale attacco si sta rivelando qualcosa di molto più inquietante. Dietro la richiesta di riscatto, il malware WannaCry porta con sé la capacità di entrare nei sistemi e agire su di essi dando comandi legittimi, con la possibilità di distruggere l'intero sistema. Nel momento più difficile, ecco però che un ricercatore, il Clark Kent/Superman di noi utenti, scopre che il malware possiede una "sicura" che lo può disattivare e... il mondo è salvo.

Anno 2010. L'impianto di arricchimento dell'uranio della centrale nucleare di Natanz, in Iran, è bloccato a causa di un virus che rende difficile la rilevazione di malfunzionamenti. Stuxnet ha sfruttato le vulnerabilità dei controllori logici programmabili (PLC) utilizzati per l'automazione negli impianti, che neppure erano collegati in Internet.

Abbiamo citato questi tre attacchi, realizzati in tempi diversi, con modalità diverse, verso obiettivi diversi, solo per esemplificare la dura realtà con cui abbiamo tutti a che fare. In particolare, gli ultimi due malware hanno segnato un cambio di passo. WannaCry nasconde, dietro un normale ransomware, un attacco molto più complesso e importante che utilizza tecniche nuove rispetto alle precedenti. Stuxnet rimane il prototipo di un malware utilizzato nel contesto di una guerra cibernetica.

La questione non è **se** subiremo o meno un attacco, ma piuttosto **quando** questo accadrà (o è già avvenuto, magari senza che lo si sappia). Dopo anni di esposizione a ogni tipo di phishing e malware, non nutriamo più illusioni di invulnerabilità (Figura 1). L'accelerazione della digitalizzazione, con la necessità dei collegamen-



➜ **Fig. 1** Una mappa degli attacchi informatici in tempo reale è uno strumento che, anche visivamente, ci aiuta a comprendere l'entità del problema e i rischi che corriamo (https://cybermap.kaspersky.com)..

ti da remoto, ci ha reso tutti più consapevoli dei rischi e degli investimenti necessari nei processi di sicurezza. Questi investimenti spaziano dalla progettazione dei dispositivi fino alla sicurezza delle reti e, soprattutto, alla promozione di una cultura della sicurezza a livello aziendale e individuale. Dobbiamo imparare dai nostri errori passati e dai colpi che abbiamo subito.

Un'osservazione prima di cominciare.
Nel campo dell'informatica, è pratica comune l'uso di personaggi come Alice, Bob, Cindy (o Carol), Trudy ed Eve per rappresentare i diversi ruoli in uno scambio di messaggi su una rete. Alice e Bob sono i protagonisti «positivi» che comunicano tra loro, mentre Cindy agisce come un intermediario non autorizzato, intercettando la comunicazione senza che Alice e Bob ne siano a conoscenza. Trudy è l'intruso che cerca di alterare o interrompere la comunicazione, mentre Eve, il cui nome è un gioco di parole con *eavesdropper* (spione), si limita ad ascoltare segretamente.
Nel corso di questo e dei successivi capitoli, utilizzeremo questi personaggi per illustrare i vari ruoli coinvolti nelle comunicazioni di rete (**Figura 2**).

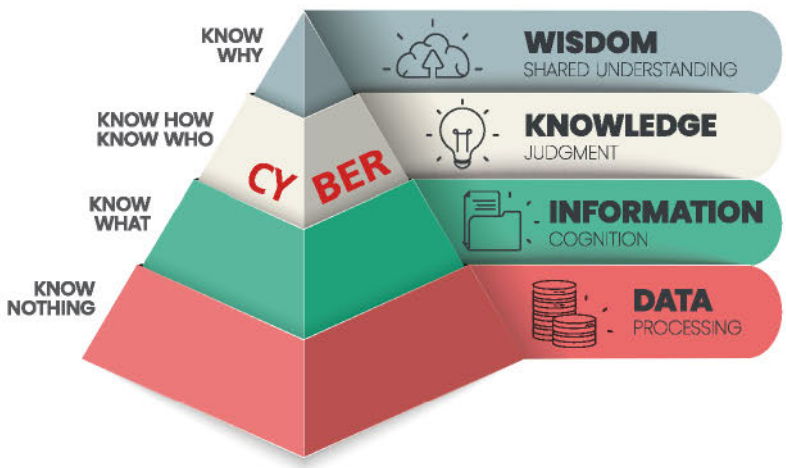
Fig. 2 I personaggi della comunicazione di rete.



2 La cybersecurity

La sicurezza informatica, o **cybersecurity**, è l'insieme di pratiche, tecnologie e processi utilizzati per proteggere le reti, i sistemi e i programmi dagli attacchi digitali. È interessante notare che il termine «cyber» descrive un'ampia gamma di applicazioni, che vanno dal cervello umano alla regolazione automatica, fino ai mondi virtuali (come lo spazio cibernetico). La sicurezza informatica si colloca al livello 3 del modello **DIKW** (**D***ata*, **I***nformation*, **K***nowledge*, **W***isdom*, **Figura 3**), posizionandosi sopra l'informatica, il cui scopo principale è elaborare e conservare i dati. La sicurezza informatica non si limita solo a questo, ma si pone nell'ottica di comprendere le informazioni per identificare i rischi, mitigare i danni, proteggere le infrastrutture e garantire la continuità operativa. In questo senso, la cyber security utilizza la conoscenza acquisita per attuare misure di protezione e strategie di difesa contro gli attacchi informatici.

Fig. 3 Posizionamento del cyber nel modello DIKW (*Data, Information, Knowledge, Wisdom*).



notabene

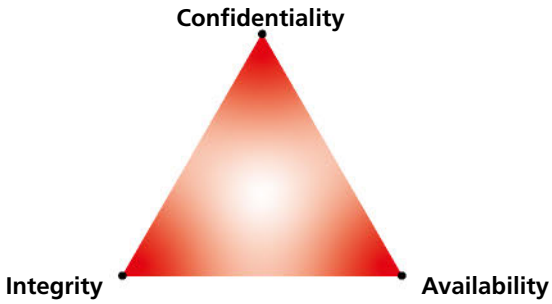
Il concetto del triangolo della sicurezza, originariamente proposto da H.W. Heinrich per la sicurezza sul lavoro, ha ispirato metodologie analoghe nella sicurezza informatica per l'analisi e la prevenzione degli incidenti.

I fondamenti della sicurezza informatica

Il modello "CIA" è fondamentale per la sicurezza delle informazioni, e si può visualizzare come un triangolo ai cui vertici sono posizionati i tre obiettivi (Figura 4):

- **C – Confidentiality** (*Riservatezza*): garantisce che le informazioni private non siano rese disponibili o divulgate a persone non autorizzate e che gli accessi siano impediti a chi non ha le credenziali necessarie.
- **I – Integrity** (*Integrità*): garantisce che le informazioni siano protette da modifiche non autorizzate, accidentali o volontarie. Per questo sono utilizzate tecniche di crittografia e protocolli di comunicazione che controllano l'integrità dei dati. Anche i sistemi di backup possono essere considerati strumenti che assicurano l'integrità.
- **A – Availability** (*Disponibilità*): garantisce che i dati siano sempre disponibili, tramite l'adozione di meccanismi di ridondanza e backup.

Se un **attacco** riesce a compromettere **anche uno solo** di questi elementi può causare un **incidente** informatico con gravi conseguenze, come la perdita di informazioni, la violazione della privacy o l'interruzione dei servizi.



→ **Fig. 4** Il triangolo CIA (*Confidentiality, Integrity and Availability*) o RID (Riservatezza, Integrità, Disponibilità).

Pit Stop

1 Quali sono i tre obiettivi della sicurezza informatica?

notabene

Esiste la possibilità di minacce interne, più subdole di quelle esterne, in circostanze in cui un dipendente o un collaboratore, in modo accidentale o intenzionalmente, accede indebitamente a dati confidenziali oppure opera impropriamente su server e infrastrutture di rete.

3 Il lato oscuro della cybersecurity

Attacchi e minacce

Un **attacco** informatico è un atto volontario che sfrutta una minaccia per compromettere un sistema.
Una **minaccia** (*threat*) è un evento esterno che tende a violare qualche obiettivo di sicurezza. Spesso è un codice eseguibile che penetra nei sistemi e si diffonde nei file per danneggiare o rubare informazioni. Una prima classificazione delle minacce distingue tra (Figura 5):

- Malware: software malevoli, come virus e worm, trojan e backdoor, ransomware, spyware, rootkit, adware (si veda il paragrafo specifico con la Tabella 1).
- **Social Engineering** è la capacità di spacciarsi per quello che non si è, sfruttando la fiducia della vittima e manipolandola per strappare informazioni riservate. L'ingegnere sociale riesce a introdursi nella rete di un'organizzazione ingannando il personale che, ingenuamente, gli fornisce codici e informazioni. Sono spesso utilizzate tecniche di phishing, che consistono nell'inviare comunicazioni fraudolente (e-mail, messaggi, link malevoli) che però sembrano provenire da una fonte affidabile.

- **APT** - *Advanced Persistent Threats* (attacchi mirati e persistenti): tecniche di hacking sofisticate per il sabotaggio e lo spionaggio (Figura 6).

Fig. 5 Una panoramica delle minacce più note.

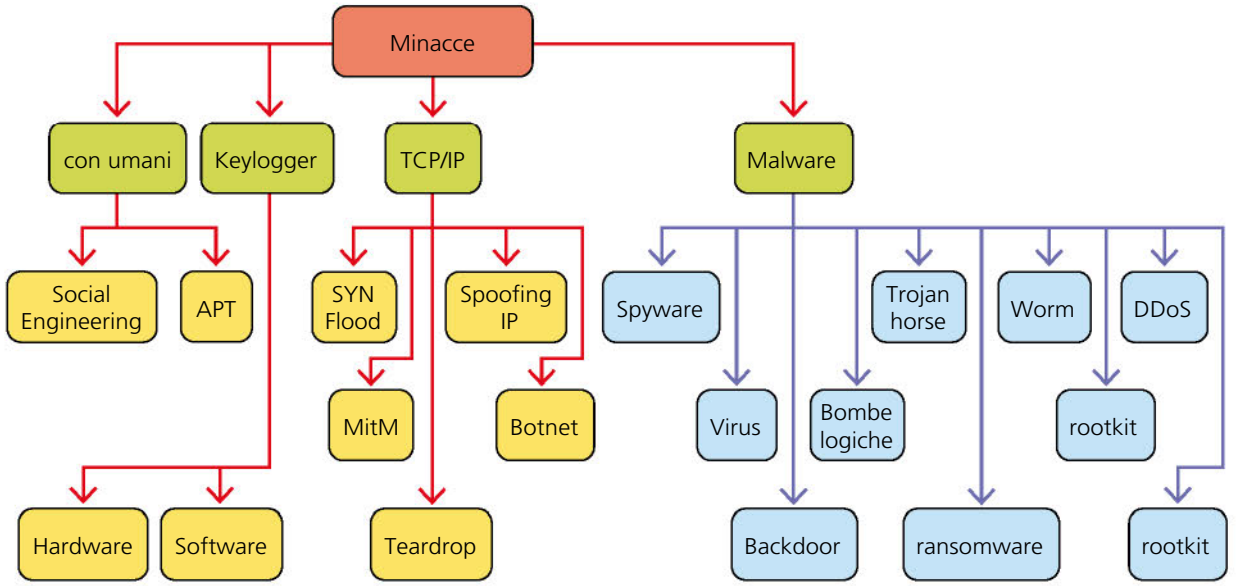
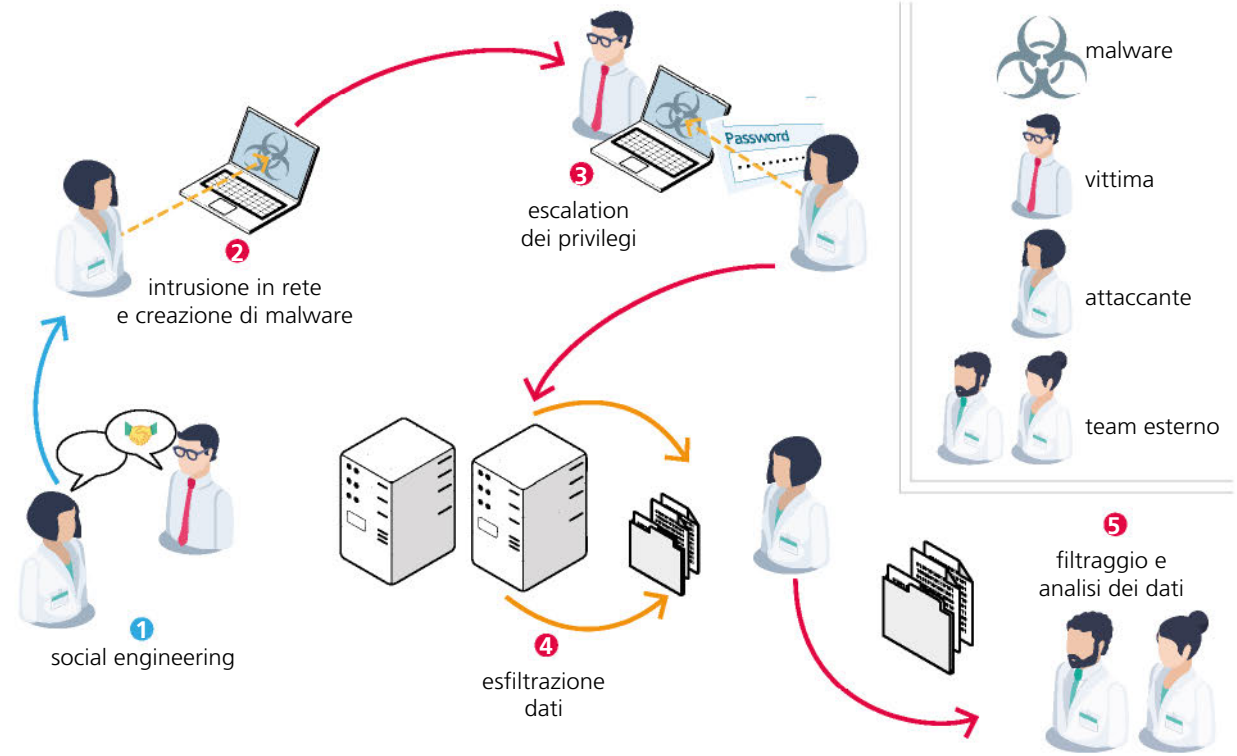


Fig. 6 Come lavora APT. Il primo passo di un attacco APT consiste nell'identificare l'obiettivo e pianificare l'azione (**1**); il secondo consiste nell'intrusione in rete (**2**); il passo successivo è la creazione di backdoor e malware, che consentono di accedere al sistema con credenziali utente valide (**3**). L'escalation dei privilegi (**4**) permette di ottenere i diritti per operare al massimo livello ed esfiltrare tutti i dati ritenuti interessanti inviandoli, criptati, al team esterno (**5**).



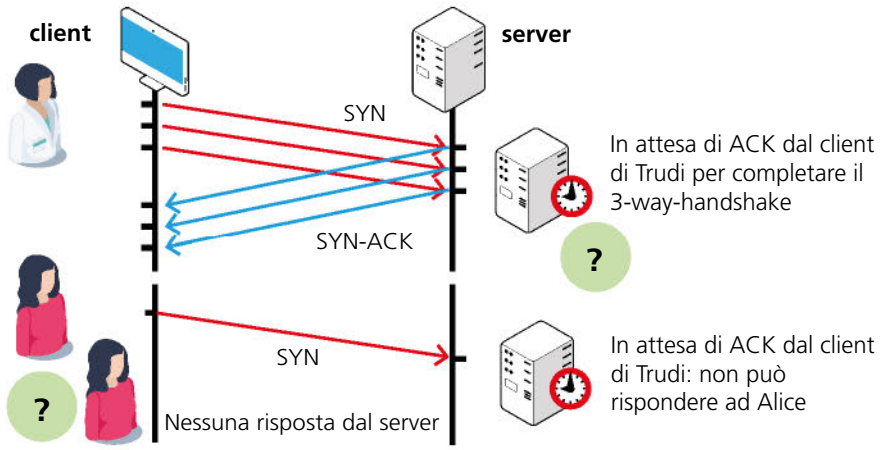


Fig. 7 In un attacco SYN Flood la fase di three-way handshake relativa all'apertura del protocollo TCP non viene mai completata causando la paralisi del server.

Pit Stop

2 Cosa si intende per minacce informatiche, e quali sono?

3 Cos'è l'ingegneria sociale?

- Attacchi con i protocolli dello stack TCP/IP:
  - **SYN Flood**: sovraccarica di richieste SYN il server, fino a farlo collassare (Figura 7);
  - **Spoofing IP**: inganna il sistema facendo credere che il traffico provenga da una fonte fidata. Altera l'indirizzo IP sorgente nei pacchetti di rete;
  - **Man in the Middle** (MitM): gli hacker si inseriscono in una comunicazione fra due parti, interrompono la conversazione per filtrare e rubare i dati (Figura 8a e 8b);
  - **Teardrop**: vengono inviati frammenti parziali di pacchetti IP che il sistema di destinazione non riesce a riassemblare e va in tilt;
  - **Botnet**: rete di dispositivi infettati da software malevolo. Gli hacker possono controllare una botnet, senza che il proprietario ne sia consapevole, con l'obiettivo di sferrare attacchi multipli. Spesso gli attaccanti utilizzano una botnet per lanciare attacchi **DDoS** (***D**istributed **D**enial **o**f **S**ervice*), che sono una delle principali minacce informatiche. Un attacco DDoS ha come obiettivo di disattivare un sito web o un servizio online sovraccaricando di richieste il server che li ospita. Il sistema colpito subisce un rallentamento o un blocco, rendendo la risorsa non più disponibile.

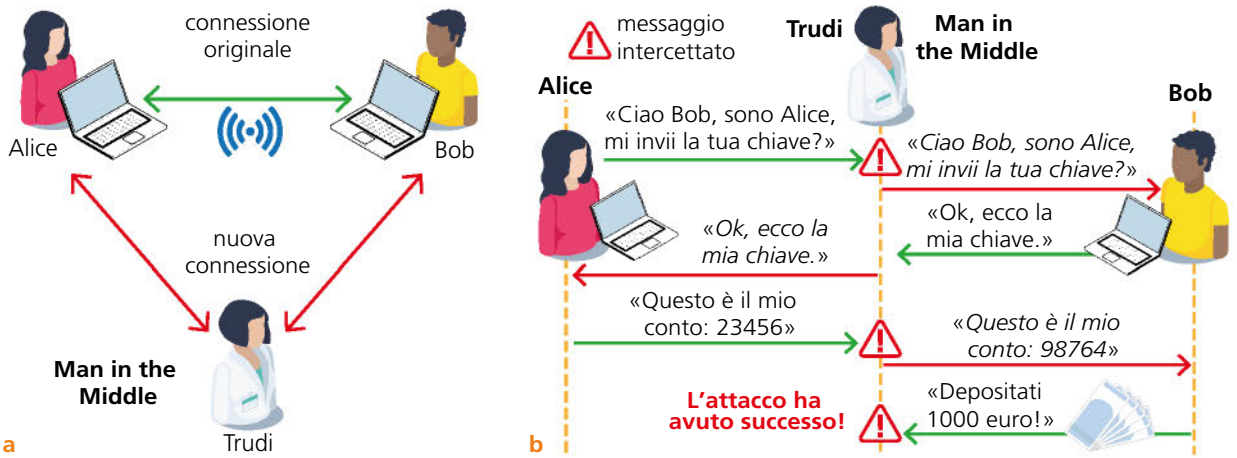


Fig. 8 a. Trudy, l'intruso, si inserisce tra Alice e Bob e si spaccia di volta in volta per uno dei due interlocutori, senza che essi se ne accorgano. **b.** Con la chiave crittografica intercettata, Trudy è in grado di ingannare Alice e Bob e di dirottare il denaro di Bob verso di sé.

La parola a... Kevin Mitnick



Kevin Mitnick (a destra nella foto) a un convegno a Milano nel 2002 con l'ethical hacker Andrea Minigozzi.

Kevin Mitnick (1963-2023) è stato uno dei più famosi e audaci esperti di ingegneria sociale. Per anni ha messo in crisi l'FBI americana con la sua abilità a introdursi in sistemi telefonici e informatici tra i più protetti e importanti della nazione. Nel libro in cui racconta la sua vita Kevin scrive: «il mio primo incontro con quella che avrei imparato a chiamare ingegneria sociale avvenne durante il liceo. Fu lì che iniziò la mia tanto strombazzata carriera di hacker. Anche se non posso entrare nei dettagli, vi basti sapere che una delle pulsioni che mi spinsero a compiere i primi passi fu il desiderio di essere accettato dal gruppo degli hacker. Tutte queste attività servivano soltanto a soddisfare la mia curiosità innata, per vedere cosa ero in grado di fare e scoprire informazioni segrete su sistemi operativi, cellulari e tutto quanto mi stimolasse. Dopo il mio arresto ho ammesso che le mie azioni erano illegali e di avere invaso la privacy altrui. Ma le mie malefatte erano spinte dalla curiosità. Volevo sapere tutto su come funzionavano le reti telefoniche e la sicurezza informatica... Adesso sono cambiato. Sfrutto il mio talento e il sapere sterminato che ho accumulato sulle tattiche dell'ingegneria sociale per aiutare governo, aziende e singoli a prevenire, individuare e controbattere le minacce portate alla sicurezza dell'informazione» (Kevin D. Mitnick, *L'arte dell'inganno*, Feltrinelli 2013).

Incidenti e vulnerabilità

Un **incidente di sicurezza** è un evento che mette a rischio l'integrità, la riservatezza o la disponibilità dei dati nei sistemi o nelle reti di computer: può rendere inaccessibile una risorsa in rete, ingannare gli utenti o introdurre persone non autorizzate all'interno dei sistemi.
Un incidente informatico può verificarsi solo se esistono determinate condizioni propizie, come *debolezze* e *vulnerabilità*. Ad esempio, un errore di programmazione può introdurre debolezze nel software. Se tale errore è sfruttabile (*exploit*) da un attaccante, allora il software diventa vulnerabile, poiché il bug si trasforma in una falla di sicurezza che può essere utilizzata per compromettere il sistema.

notabene

Il termine *exploit* si riferisce al tentativo da parte di un malintenzionato di sfruttare una vulnerabilità a lui nota per mettere in atto una minaccia.

Definiamo più dettagliatamente:

- **Debolezza** (*weakness*). È un difetto o una falla interna a un sistema informatico che, se scoperta da un malintenzionato, potrebbe essere sfruttata per eludere le misure di sicurezza. Queste debolezze possono interessare varie componenti del sistema, inclusi hardware, software e reti. Un esempio di debolezza è un codice che contiene errori di progettazione o implementazione. La debolezza è intrinseca alla natura dell'oggetto e non dipende dal suo utilizzo.

Comprendi con l'analogia

Una vulnerabilità di un sistema è come il tallone di Achille: anche se è l'unico punto debole, può essere fatale



Secondo il mito, l'eroe greco Achille, figlio della ninfa Teti e del mortale Peleo, uno dei protagonisti della guerra di Troia, venne immerso dalla madre nelle acque del fiume Stige nel tentativo di renderlo immortale. Ma la madre lo tenne per un tallone, che non venne quindi toccato dalle acque sacre, rimanendo così vulnerabile. Durante l'assedio di Troia, Paride scagliò una freccia che, guidata da Apollo, trovò il suo bersaglio proprio nel solo punto debole di Achille: il tallone. La fine dell'eroe dimostra che anche la più piccola, insospettabile vulnerabilità può avere conseguenze devastanti.

Pit Stop

4 Che cosa distingue una vulnerabilità da una debolezza?

- **Vulnerabilità** (*vulnerability*). È una debolezza specifica in un sistema informatico che può essere sfruttata attraverso un exploit, un codice o una sequenza di comandi, per compromettere la sicurezza del sistema. Una vulnerabilità è direttamente legata all'utilizzo di un componente e alla presenza di una minaccia capace di sfruttarla.

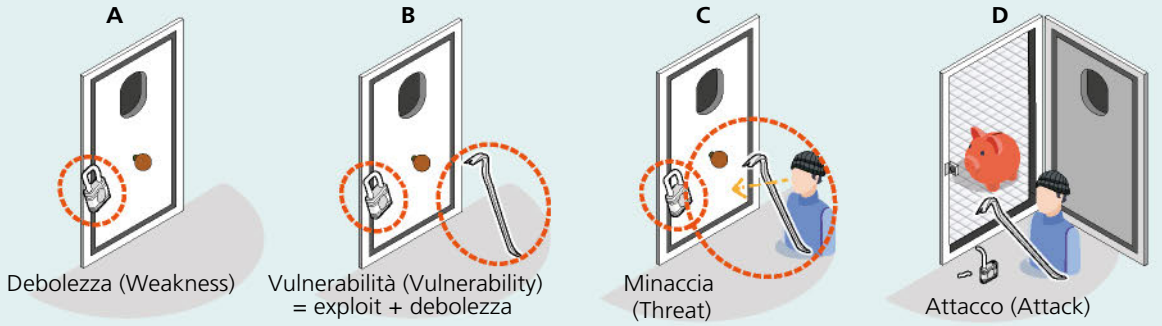
Classificazione delle vulnerabilità

Da un punto di vista generale possiamo distinguere tre diversi tipi di vulnerabilità:

- **Vulnerabilità intrinseche**. Sfruttano la natura aperta della rete e degli elementi che ne fanno parte:
  - i dispositivi presentano porte fisiche di diversi tipi (Ethernet, USB, Wi-Fi, ecc.) che permettono l'interazione, ma possono anche esporre a rischi;
  - i protocolli di Internet sono progettati per facilitare la comunicazione; le applicazioni possono utilizzare fino a 65 000 porte logiche, rendendo i sistemi altamente vulnerabili (immagina una casa con 65 000 ingressi!);
  - i software invecchiano rapidamente e gli aggiornamenti non sempre vengono applicati tempestivamente a causa di costi elevati e tempi lunghi;
  - le vulnerabilità ancora non scoperte, note come zero-day, rendono ogni dispositivo in rete potenzialmente attaccabile.

Comprendi con l'analogia

Un exploit è come un ladro con un grimaldello che apre un lucchetto non sicuro



Immagina la tua casa con una porta protetta solo da un vecchio lucchetto (**A**). Anche se la porta è chiusa, non è sicura: un ladro potrebbe facilmente forzarla e rubare i tuoi beni.
Il lucchetto rappresenta una password debole o una connessione non sicura, come telnet, che lascia i tuoi dati esposti.
Un malintenzionato (**D**) con un grimaldello (**C**) può sfruttare questa debolezza e divenire una minaccia alla sicurezza.
Questo è analogo a un exploit che sfrutta una falla di sicurezza su un sistema informatico.
Se il ladro riesce a entrare (**E**), potrebbe sottrarre o danneggiare i tuoi beni, proprio come un attacco informatico potrebbe compromettere o cancellare i tuoi dati.
Per proteggere la tua casa, potresti sostituire il vecchio lucchetto con una serratura moderna e sicura, più difficile da forzare, installare un allarme o rinforzare la porta.
Allo stesso modo, per proteggere i tuoi dati, dovresti usare password forti, connessioni cifrate e avere un buon sistema antintrusione.
Come per la casa, così per i dati digitali è essenziale avere difese solide e prevenire gli attacchi prima che possano arrecare danni.

- **Vulnerabilità tecnologiche**. Hardware, software e protocolli possono presentare lacune ed errori di progettazione e programmazione che dei malintenzionati possono sfruttare per compromettere la sicurezza.
- **Vulnerabilità umane**. La natura umana, che è andata costruendosi nel corso di centinaia di migliaia di anni, ci rende reattivi a stimoli immediati, come il passaggio di un insetto o un rumore inaspettato. Tuttavia, non mostriamo la stessa prontezza di fronte a contenuti sospetti su una pagina web o in una e-mail. Cliccare senza riflettere su link dubbi o condividere impulsivamente informazioni sensibili sono gli aspetti più critici, a causa dell'imprevedibilità del comportamento umano, che può essere facilmente ingannato o indotto a commettere errori.

notabene

Si suol dire che, spesso, il problema di sicurezza risiede «tra la tastiera e la sedia», cioè riguarda i comportamenti dell'utente (chiamato anche *layer 8* in analogia con i 7 livelli ISO/OSI).

Da un punto di vista pratico **CWE** (**C***ommon* **W***eakness* **E***numeration*) e **CVE** (**C***ommon* **V***ulnerabilities and* **E***xposures*) sono due strumenti fondamentali per navigare nella "giungla" delle vulnerabilità e per proteggere i sistemi informatici dalle insidie nascoste e sempre più sofisticate. MITRE Corporation, in collaborazione con il Dipartimento della Sicurezza degli Stati Uniti, aggiorna costantemente il database di debolezze e vulnerabilità, assegnando loro un ruolo vitale nella difesa contro le minacce. In particolare:

- **CWE** fornisce un elenco di debolezze che si riscontrano nel software e nell'hardware, offrendo una classificazione standard che permette agli sviluppatori di individuare con facilità eventuali problemi e di non ricadere negli stessi errori.
  Ad esempio, se ci interessa studiare le debolezze legate al buffer overflow, cioè al fatto che la lunghezza dei valori in input non sia controllata e sfori la massima dimensione di memoria disponibile (buffer), il sito del MITRE con la CWE-120 e seguenti ci viene in aiuto con esempi e commenti (Figura 9).
- **CVE** cataloga le diverse vulnerabilità, assegnando loro un identificativo unico (**CVE-ID**), che serve come riferimento per valutare le vulnerabilità e gli strumenti di protezione.
  A ciascuna vulnerabilità è assegnato un punteggio standard che aiuta a comprenderne l'impatto e a stabilire le priorità di intervento (**CVSS** – **C***ommon* **V***ulnerability* **S***coring* **S***ystem*). Il punteggio va da 0, la vulnerabilità con impatto più basso, a 10, che indica la massima gravità ("Critica"). Il criterio di assegnazione del punteggio combina diversi fattori come: la modalità di attacco, che può avvenire tramite rete geografica o locale, accesso fisico ecc.; la complessità dell'attacco; i privilegi necessari per sfruttare la vulnerabilità; la necessità, o meno, di interazione con un utente.
  Se, ad esempio, ci interessa capire le vulnerabilità di un sistema IoT, possiamo basarci su CVE-2023-26801, che illustra come un aggressore possa eseguire comandi arbitrari su dispositivi che sono stati compromessi (Figura 10). Tale vulnerabilità è stata sfruttata da una variante del malware Mirai, molto noto per i suoi attacchi devastanti del 2017. Si tratta di una grave vulnerabilità, con punteggio CVSS di 9.8.

Pit Stop

5 Cosa si intende per CVE e CWE?

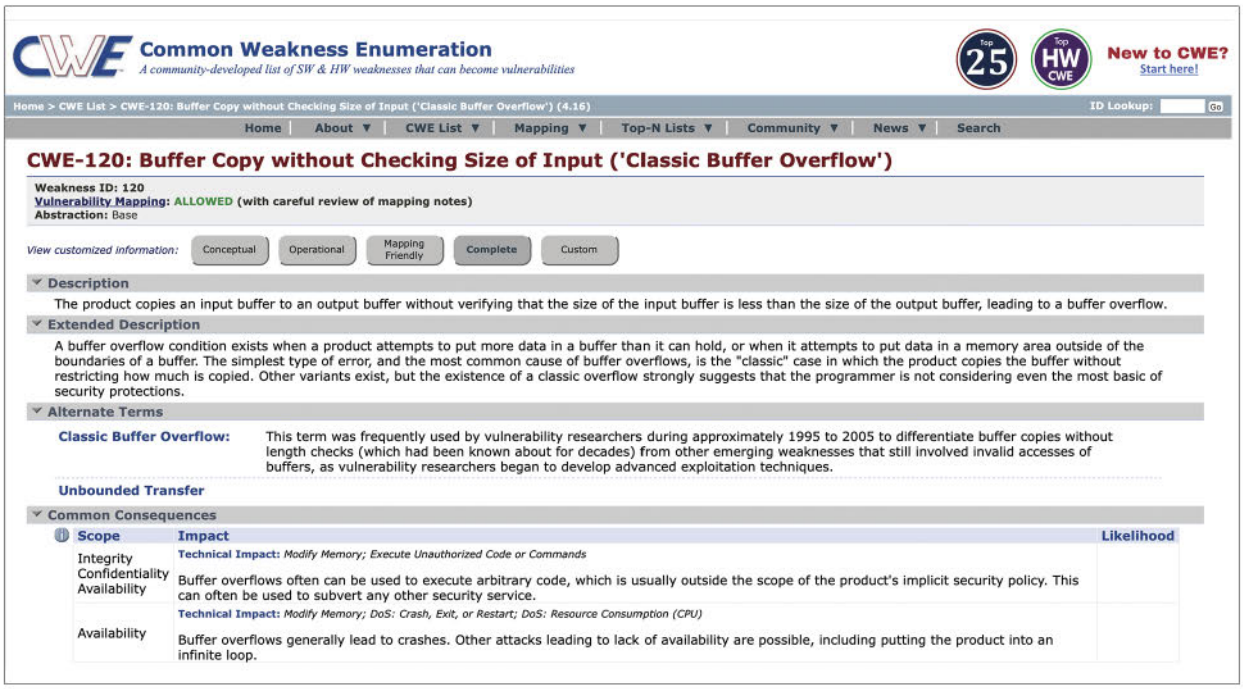
6 Qual è la missione di MITRE?

Malware: struttura e tipologie

Un approfondimento deve essere riservato ai malware, per l'importanza che rivestono negli attacchi informatici.
Il termine "malware" è una contrazione delle parole inglesi "malicious" e "software", e sta a indicare qualsiasi tipo di codice malevolo che cerca, illecitamente, di penetrare in un sistema (reti, computer, dispositivi intelligenti).

Gli obiettivi di un malware possono essere molteplici: dal furto dei dati alla loro alterazione, allo spionaggio, fino alla compromissione delle funzioni di un sistema per bloccarlo o assumerne il controllo.
Nella maggior parte dei casi, i malware infettano i dispositivi con l'inconsapevole complicità degli utenti che, ignari o meno del pericolo, visitano siti web sospetti, scaricano file infetti e aprono allegati di false e-mail. Occorre anche precisare che molti attacchi si basano sulla fragilità e i limiti umani che gli ingegneri sociali sono bravissimi a sfruttare.

a



b

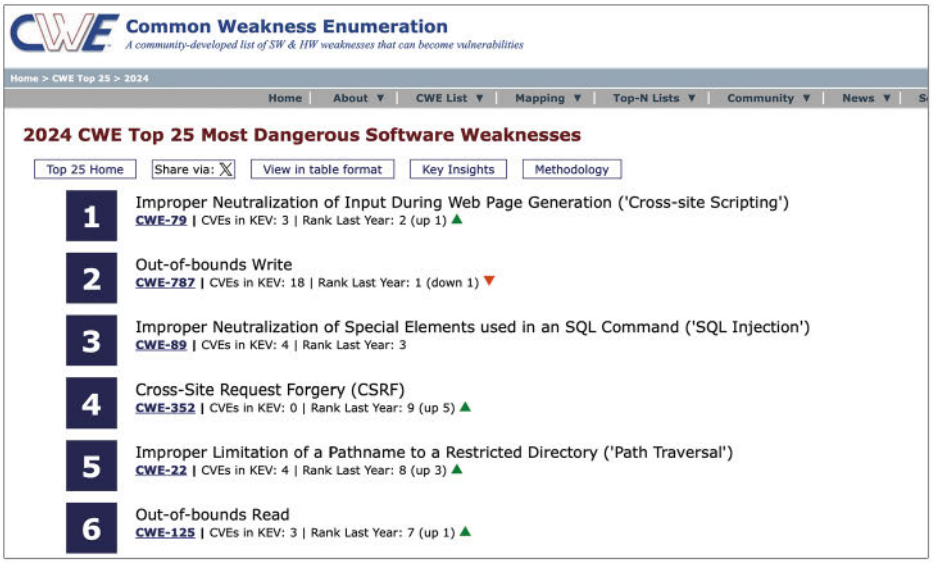


Fig. 9 a. La ricerca della debolezza CWE-120 sul sito del MITRE (`https://cwe.mitre.org`). **b.** Un esempio con la classifica delle debolezze 2024.

Pit Stop

7 Cos'è un malware e come si può prevenire?

8 Fai un elenco delle tipologie di malware.

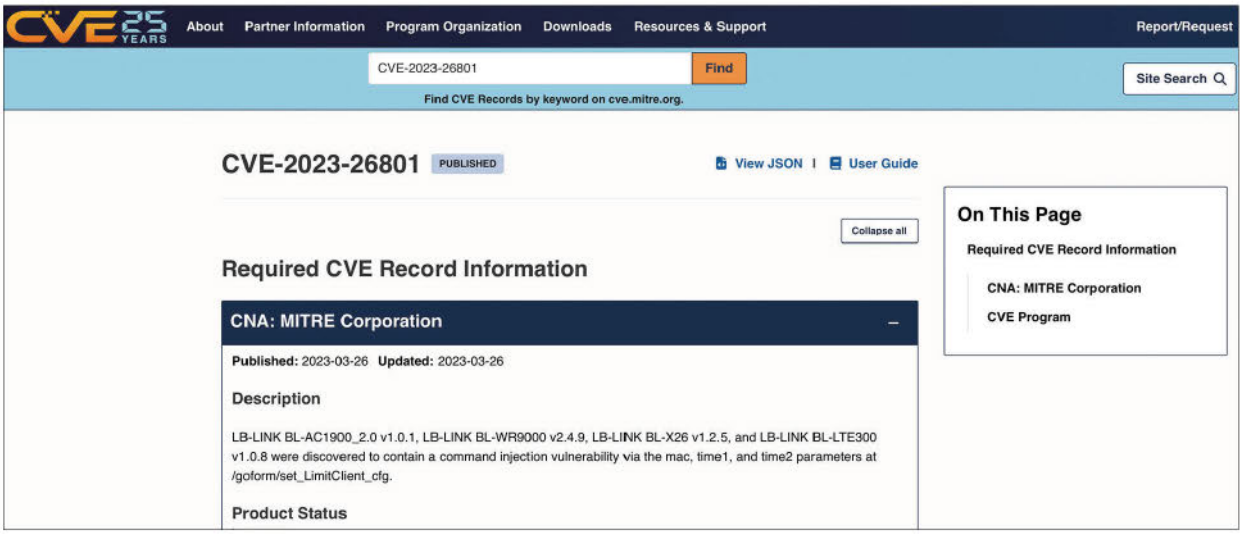


Fig. 10 La ricerca della vulnerabilità CVE-2023-26801 sul sito gestito dal MITRE (`https://cve.org/`).

La struttura del malware

In generale un malware è composto da due componenti con funzioni diverse:

- il **vettore** è il mezzo attraverso il quale il malware si diffonde (un file, un link, un dispositivo di archiviazione esterno) e il cui scopo specifico è penetrare il sistema, sfruttando le sue vulnerabilità ed eludendo le sue difese;
- il **carico utile** (**payload**) contiene le istruzioni specifiche che il malware eseguirà una volta penetrato nel sistema, come cifrare file, rubare dati, impedire il funzionamento del sistema, ecc.

La costante evoluzione e proliferazione dei malware impone la necessità di classificarli in precise categorie : la **Tabella 1** offre una panoramica, necessariamente limitata, di alcune delle categorie di malware più noti e delle modalità di attacco e difesa. La tabella contiene alcuni riferimenti agli standard CVE. Inoltre occorre notare che il terreno su cui si gioca la sicurezza informatica non è costituito da elementi fisici come strade, montagne o fiumi, ma è definito dal modello TCP/IP e, precisamente, dal livello a cui l'attacco fa riferimento.



Comprendi con l'analogia

Un malware è come un missile che trasporta una testata esplosiva

Possiamo immaginare il malware come un missile pronto a essere lanciato contro un obiettivo. Il missile rappresenta il pacchetto di attacco completo: è costituito da un vettore, che è il veicolo che porta a bersaglio la testata, e dalla testata, che contiene il payload, o carico bellico (diverso a seconda dello specifico scopo dell'attacco). Nel caso del malware, il carico utile rappresenta il codice che il malware eseguirà una volta dentro il sistema bersaglio, che effettuerà operazioni che possono includere, ad esempio, la raccolta di informazioni, la distribuzione di spam, il furto di dati o l'esecuzione di attacchi DoS. In alcuni casi, per sondare la vulnerabilità del sistema senza eseguire immediatamente azioni dannose, il missile possiede solo il vettore, senza la testata. Per esempio nel caso dell'attacco WannaCry (citato nell'introduzione di questa unità) il "vettore" ha veicolato un ransomware, trasportando nella "testata" un codice malevolo (l'exploit chiamato EternalBlue) che sfrutta una vulnerabilità di un protocollo disponibile sui sistemi operativi Microsoft. In realtà il vettore avrebbe potuto trasportare un qualsiasi codice, ad esempio un keylogger, un software che registra tutto ciò che viene digitato, incluse le password.

Tipologia di malware	Obiettivi/effetti	Modalità di infezione	
Virus (la pandemia informatica)	I virus sono codici malevoli che si agganciano a software esistenti, variando le dimensioni dei file che li ospitano.	• Si trasmettono tramite file infetti, spesso come allegati di e-mail o dispositivi di archiviazione rimovibili, come chiavette USB. • Richiedono un'azione diretta dell'utente per propagarsi. • Si caricano nella memoria centrale del sistema e restano residenti, pronti a infettare altri programmi. • Spesso i virus vengono generati a partire da altri virus (polimorfismo).	
Worm (verme informatico)	Gli worm sono programmi autonomi che non hanno bisogno di un programma ospite per essere eseguiti.	• Vengono diffusi tramite la rete e spesso si servono della posta elettronica. • Può capitare che siano gli utenti stessi a mandarli in esecuzione, scambiandoli per programmi utili.	
Trojan / Backdoor (cavallo di Troia / porta sul retro)	I trojan sono software che, in analogia con lo stratagemma del cavallo di Troia, si introducono nel sistema sotto sembianze di software legittimo, ma consentono ai malintenzionati di spiare la vittima, rubare dati e ottenere accesso tramite backdoor per controllare il sistema. Una backdoor è un codice che crea un canale di comunicazione in Internet, utilizzando una porta logica, dei protocolli (TCP o UDP), per il controllo a distanza.	I trojan si diffondono scaricando file compromessi da siti web o allegati di e-mail. Possono anche essere inseriti intenzionalmente in applicazioni e giochi che funzionano su dispositivi fissi e mobili. Esistono ad esempio trojan per cellulari che, accedendo alla posizione GPS del dispositivo da tenere sotto controllo, possono monitorare gli spostamenti della vittima.	
Ransomware (ransom = riscatto)	Malware che crittografa i file dell'utente, rendendoli inaccessibili fino al pagamento di un riscatto.	• Sfruttano la vulnerabilità dei sistemi e l'ingegneria sociale. • E-mail di phishing: gli utenti ricevono e-mail apparentemente legittime con allegati o link malevoli. • Siti Web Compromessi possono contenere script o file infetti.	
Spyware (programma spia)	Software che raccoglie informazioni sull'utente senza il suo consenso.	• E-mail di phishing. • Siti web compromessi. • Rete interna. • Dispositivi rimovibili.	
Rootkit (root = privilegi di amministratore)	Fornisce agli hacker l'accesso e il controllo su un dispositivo preso di mira.	• Download di file da siti web non sicuri. • Allegati di e-mail sospette. • Dispositivi rimovibili.	

↑ **Tab. 1** Classificazione dei malware.

	Prevenzione	Esempi emblematici	Livello TCP/IP	Classificazione (CVE-ID)
	• Software antivirus. • Aggiornare costantemente il sistema operativo e gli applicativi. • Fare attenzione a siti web o allegati di e-mail sospetti.	• ILOVEYOU: creato nel 2000, aveva bisogno di un file ospite per attivarsi che, in questo caso, era l'allegato e-mail che gli utenti dovevano aprire manualmente. Una volta attivato, si diffondeva inviando copie di sé stesso a tutti i contatti e-mail dell'utente tramite un file allegato.	Applicazione	Non esiste un CVE specifico poiché è stato rilasciato prima che il sistema CVE fosse adottato universalmente.
	• Aggiornare costantemente il sistema operativo e gli applicativi. • Utilizzare software antivirus.	• Morris Worm: il primo worm distribuito in Internet da Robert Morris nel 1988, di cui si abbia notizia. • Mirai: creato nel 2017 ha infettato centinaia di migliaia dispositivi IoT domestici, come telecamere e termostati, paralizzando molti siti web, tramite attacchi DDoS (denial of service distribuiti).	Rete/Trasporto/ Applicazione	CVE-2023-26801
	• Aggiornare costantemente il sistema operativo e gli applicativi. • Fare attenzione a siti web o allegati di e-mail sospetti.	• Emotet: emerso nel 2014, cambia ogni volta la sua "firma" (hash) e aggiorna gli indirizzi IP e le porte TCP utilizzate per comunicare con il centro di comando e controllo. Una nuova versione di Necron è stata identificata nel 2024. Si è infiltrata in diverse applicazioni come Spotify e giochi molto noti, come Minecraft.	Trasporto/ Applicazione	CVE-2021-43890
	• Aggiornare costantemente il sistema operativo e gli applicativi. • Fare attenzione a siti web o allegati di e-mail sospetti.	• WannaCry: cripta i file presenti sui computer attaccati e chiede un riscatto per ottenere la chiave di decrittazione (2017). • LockBit: blocca l'accesso ai sistemi informatici in cambio di un riscatto (2019).	Applicazione	CVE-2017-0144 CVE-2023-3824
	• Aggiornare costantemente il sistema operativo e gli applicativi. • Evitare di aprire allegati o link sospetti. • Utilizzare software antivirus.	• Pegasus: sviluppato originariamente dagli israeliani, nel 2021 ha preso di mira i telefoni cellulari (con versioni iOS e Android) raccogliendo password e messaggi di testo, tracciando la posizione e altro ancora.	Applicazione	CVE-2023-41064 e CVE-2023-4863
	• Aggiornare costantemente il sistema operativo e gli applicativi. • Evitare di scaricare software da fonti non attendibili.	• Stuxnet: progettato appositamente per colpire i sistemi di controllo industriale (SCADA), è ritenuto responsabile di aver inferto danni irreparabili a una centrale nucleare iraniana nel 2010.	Applicazione/Sistema Operativo	CVE-2010-2772

Segue ▶

Tipologia di malware	Obiettivi/effetti	Modalità di infezione	
Adware (advertising, pubblicità)	Software che mostra pubblicità indesiderata all'utente. Anche se non sono malevoli, sono molto fastidiosi.	• Si diffondono tramite programmi gratuiti o shareware. • Siti web compromessi. • Vulnerabilità del software. • Dispositivi rimovibili.	
Keylogger (keystroke logger)	Applicazioni software o dispositivi hardware che registrano tutto ciò che viene digitato sulla tastiera.	• Keylogger Software: vengono installati con la complicità di Trojan o un Rootkit. Registrano, in background, tutte le pressioni dei tasti, compresi nomi utente, password ecc. • Keylogger hardware: i dispositivi fisici vengono collegati alla tastiera del computer e registrano ogni tasto premuto senza che il sistema operativo ne sia a conoscenza.	

Comprendi con l'analogia

Virus biologici e informatici

Funzione	Virus informatico	Virus biologico
Diffusione	Passa da un file all'altro inserendo il proprio codice e infettando sempre più dispositivi	Si diffonde da un organismo all'altro infettando sempre più soggetti
Replicazione	Utilizza le risorse del sistema per riprodursi e diffondersi	Si replica all'interno delle cellule dell'ospite
Effetti	Può danneggiare file o app e compromettere le prestazioni del computer	Causa malattie negli organismi che infettano
Prevenzione e cura	Software antivirus per proteggere i computer: individuato il virus, viene messo in quarantena e rimosso	Vaccini, elementi di protezione individuale per prevenire la malattia; quarantena e farmaci per trattare l'infezione.

4 Le strategie dell'attacco informatico

L'attacco informatico è un processo complesso che si snoda attraverso diverse fasi, ciascuna guidata da obiettivi specifici. Le motivazioni di un attaccante possono variare dall'ottenere un guadagno finanziario al provocare l'interruzione di servizio, dal furto di informazioni sensibili a motivazioni politiche.
Gli aggressori impiegano pochissimo tempo a creare nuove minacce e diffondere malware. Al contrario, occorre molto tempo per rilevare e contrastare le minacce. È importante acquisire il modo di pensare di un attaccante perché vale sempre l'antico detto di Sun Tzu, l'autore del famoso manuale di strategia militare conosciuto come *L'arte della guerra*, che così recita: «*se conosci il nemico e te stesso, la tua vittoria è sicura*».

	Prevenzione	Esempi emblematici	Livello TCP/IP	Classificazione (CVE-ID)
	• Strumenti dedicati a individuare e rimuovere gli adware. • Mantenere il software aggiornato.	• Fireball ha infettato oltre 250 milioni di PC in tutto nel 2018. Modifica le impostazioni del browser dell'utente (browser hijacker) per ottenere vantaggi da pubblicità online.	Applicazione	-
	• Non lasciare incustodito il computer e controllare chi vi accede fisicamente. • Porre attenzione ai programmi che si installano. • Mantenere aggiornato il software antivirus.	• Keylogger Software applicazioni varie che catturano password, e messaggi e le inviano direttamente all'aggressore via e-mail. • Keylogger hardware: vari dispositivi simili a un normale adattatore o una prolunga del cavo della tastiera che memorizza la sequenze di tasti premuti, in una memoria non volatile (flash), simile a una chiavetta USB.	Applicazione	-

La parola a ... Sun Tzu



Sun Tzu fu un filosofo e generale cinese che divenne celebre per le sue brillanti campagne militari condotte tra il VI e il V secolo a.C. Scrisse un importante trattato di strategia militare, *L'arte della guerra*, che si diffuse in tutta la Cina, anche tra i non militari, per la saggezza e i consigli impartiti per affrontare le sfide della vita. «Se conosci il nemico e conosci te stesso, nemmeno in cento battaglie ti troverai in pericolo», è una delle frasi più citate, anche nella cybersecurity. E ancora: «Se conosci il nemico e te stesso, la vittoria non sarà mai in dubbio. Se conosci il cielo e la terra, la vittoria sarà totale».
Sun Tzu, tuttavia, non si limitò a fornire precetti per sconfiggere i nemici sul campo di battaglia, ma offrì anche suggerimenti preziosi, validi allora come oggi: «Ottenere cento vittorie in cento battaglie non è segno di suprema abilità. Sottomettere l'esercito nemico senza combattere è segno di suprema abilità» (Sun Tzu, *L'arte della guerra*, trad. di M. Rossi, Mondadori).

Assalitori invisibili

Tra i flussi di dati, esistono figure che navigano nell'ombra senza essere viste: sono gli **hacker**, assalitori invisibili che si insinuano nelle maglie delle reti. Eludono i firewall con astuzia, si camuffano dietro linee di codice e sistemi crittografici complessi. Sono maestri nel trovare vulnerabilità, creare backdoor, fabbricare exploit e orchestrare attacchi sofisticati, penetrando in reti aziendali, database e dispositivi personali.
Ma qual è la vera natura degli hacker? La risposta non è semplice. Una prima distinzione si basa sulle intenzioni che li guidano: da una parte ci sono coloro che operano nell'interesse pubblico, detti anche **white hat**, che cercano di migliorare la sicurezza per tutti. Dall'altra, ci sono i **black hat**, che agiscono

notabene

L'hacking etico e malevolo possono utilizzare strumenti simili per difesa e attacco, ma ciò che li distingue sono le intenzioni e il contesto in cui operano: non lo strumento, ma l'obiettivo.

notabene

Nel 2011, Lockheed Martin, un'azienda statunitense leader nel settore aerospaziale e della difesa, ha adattato il concetto di "kill chain", che in ambito militare descrive le diverse fasi di un attacco, dall'identificazione del bersaglio alla verifica dell'avvenuta neutralizzazione, al contesto della sicurezza informatica. L'intento era quello di analizzare e neutralizzare le cosiddette minacce persistenti avanzate (APT), fornendo così un modello applicabile a una vasta gamma di minacce cibernetiche

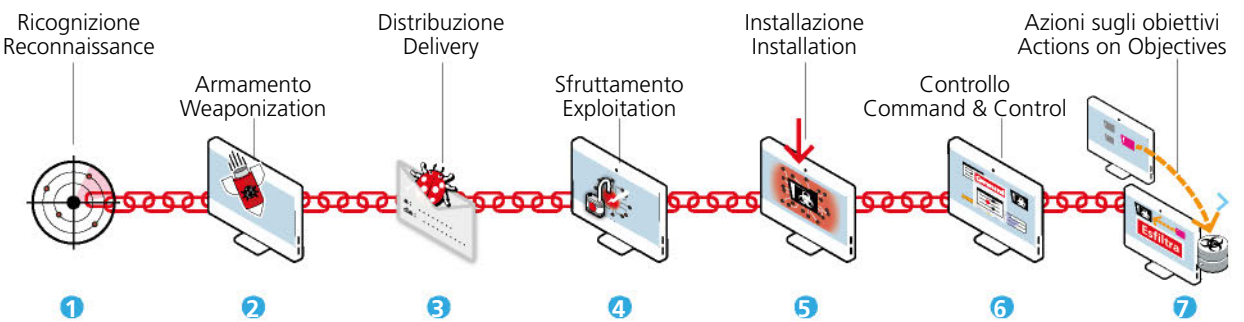
con intenzioni criminali, violando i sistemi per rubare dati, diffondere malware, compiere frodi o altre azioni illegali. In mezzo a questi estremi, esistono i **grey hat**, figure ambigue che possono oscillare tra la legalità e l'illegalità, a seconda delle circostanze. Tra questi, ricordiamo i **principianti** (***script kiddie***) che utilizzano strumenti creati da altri per condurre attacchi informatici rudimentali e spesso non dispongono di competenze avanzate. Gli **hacktivist** che cercano di promuovere cause politiche o sociali attraverso attacchi informatici. Infine, gli **hacker sponsorizzati** (***state sponsored***) che agiscono con il supporto di governi o organizzazioni per perseguire obiettivi specifici. Le loro azioni possono essere etiche quando mirano a migliorare la sicurezza, o malevole quando si dedicano a spionaggio o sabotaggio.

Cyber Kill Chain

Il ciclo di vita di un attacco informatico è documentato dalla Cyber Kill Chain, un modello che suddivide le azioni degli aggressori in fasi che si susseguono come anelli di una catena: dalla raccolta di informazioni su un obiettivo, alla preparazione e distribuzione del malware, fino all'attacco finale. Se un difensore riesce a intervenire, spezzando un anello della catena, l'attacco è destinato a fallire.

Il modello prevede sette fasi (Figura 11):

1. **Ricognizione** (*Reconnaissance*). In questa fase iniziale, l'hacker va in perlustrazione e seleziona i bersagli per raccoglie informazioni dettagliate sull'organizzazione scelta come obiettivo. In particolare si concentra su:
   – informazioni sulle scelte tecnologiche, finanziarie e organizzative dell'organizzazione da attaccare. Fa ricerche sul reddito, sulla presenza sui social network, sulla mailing list, utilizza altre tecniche di ricerca come WHOIS e strumenti di geolocalizzazione
   – scelta dei metodi di attacco più efficaci, facili ed economici.
   – puntare direttamente all'organizzazione (top down), oppure passare dai suoi fornitori (bottom-up)
2. **Armamento** (*Weaponization*). In questa fase, l'attaccante pianifica l'attacco identificando le vulnerabilità presenti, ad esempio nelle applicazioni web o nei sistemi.
   L'obiettivo è creare "armi" malevoli per l'attacco, preparando gli strumenti e le risorse necessarie, come la creazione di malware personalizzati o l'utilizzazione di vettori già pronti, acquistati sul Dark Web. Ad esempio, la preparazione di un attacco "watering hole" prevede la compromissione di siti web abitualmente frequentati da gruppi di utenti specifici per creare botnet (si veda l'Analogia)



↑ **Fig. 11** Cyber Kill Chain. Il termine "kill chain" era originariamente utilizzato dai militari, per descrivere le fasi degli attacchi.

3. **Distribuzione** (*Delivery*). L'attaccante invia il malware al sistema da colpire. La distribuzione di malware può avvenire attraverso diverse modalità. Il phishing è uno dei metodi più comuni. La trasmissione del payload può avvenire in due modi:
   – da un utente inconsapevole che, ad esempio, accede a un sito web compromesso, oppure apre un file PDF dannoso che gli è arrivato via e-mail;
   – dall'aggressore con iniezione SQL (SQL Injection) o altre tecniche di compromissione che sfruttano i punti deboli.
4. **Sfruttamento** (*Exploitation*). Il payload dannoso sfrutta una vulnerabilità per aprirsi un varco nel sistema ed eseguire un codice dannoso.
5. **Installazione** (*Installation*). L'attaccante installa il malware nel sistema infetto servendosi, ad esempio, di una "backdoor" per mantenere un accesso per lungo tempo.
6. **Comando e Controllo** (*Command and Control*). L'attaccante controlla l'applicazione da remoto. Prende il controllo delle risorse interne utilizzando le credenziali acquisite nelle fasi precedenti e cerca di nascondere le proprie tracce per non rivelarsi (diversione e isolamento), per non attirare l'attenzione.
7. **Azioni sull'obiettivo** (*Actions on Objectives*). L'attaccante rende persistente la propria azione mantenendosi nella rete interna il più possibile. Crea nuovi account, installa backdoor, scala i privilegi di accesso e, utilizzando canali di comunicazione criptati, **esfiltra** i dati della vittima, trasferendoli sui propri server.

La parola "**esfiltrare**", che ha origini militari, significa "portare fuori da un ambiente o da un territorio". Nella cybersecurity, l'esfiltrazione dei dati è il processo mediante il quale le informazioni sensibili vengono sottratte da un sistema e trasmesse a un ente esterno. Questo può avvenire attraverso vari metodi, come l'uso di protocolli nascosti, dati crittografati, servizi cloud, tecniche di steganografia ecc.
Come vedremo nel prossimo paragrafo è fondamentale adottare misure di sicurezza per proteggere i sistemi da queste minacce partendo dalla sensibilizzazione degli utenti e arrivando all'utilizzo di soluzioni SIEM (*Security Information and Event Management*) per il monitoraggio costante dell'ambiente.

notabene

MITRE ATT&CK (*Adversarial Tactics, Techniques & Common Knowledge*, `https://attack.mitre.org/tactics/enterprise/`) è un database liberamente accessibile che cataloga le tecniche e le procedure dei criminali informatici secondo una "matrice delle tattiche" (Enterprise Tactics), considerando le azioni degli aggressori dalla raccolta iniziale di informazioni fino all'esecuzione finale dell'attacco.

Comprendi con l'analogia

L'attacco malware di tipo "watering hole" è simile all'agguato di un predatore



Un leone affamato si è appena appostato tra la vegetazione della savana, vicino a una pozza d'acqua. Aspetta la sua preda. Una gazzella, ignara del pericolo, si avvicina per bere. Il leone passa all'attacco. Balza fuori dall'erba alta e si lancia verso l'animale. Il leone è veloce, afferra la gazzella con le zampe anteriori e affonda i suoi artigli nella schiena del povero animale. La gazzella viene sopraffatta e diventa il pasto del leone.
Questa strategia è comune nel regno animale, ma vale anche per gli attacchi informatici di tipo "watering hole": gli hacker individuano e compromettono siti web frequentati abitualmente da gruppi di persone che hanno interessi comuni (ad esempio associazioni di settore). I malintenzionati attendono pazientemente che la vittima visiti il sito malevolo e clicchi su un link compromesso. La pazienza è premiata: l'attacco viene sferrato e il computer della vittima è infettato.

5 La difficile arte della difesa informatica

Avremmo voluto intitolare questo capitolo con una frase d'impatto, come «I bastioni della difesa informatica». Purtroppo, la realtà è diversa, e ci siamo dovuti accontentare di un titolo meno efficace, ma più veritiero.
La Grande Muraglia (Figura 12a) fu costruita per fermare la penetrazione di popoli stranieri nel territorio cinese, ma non bastò a fermare gli invasori, che si limitarono ad aggirare l'ostacolo. Analogamente, la sicurezza dei sistemi in rete non può essere ridotta a una miope difesa perimetrale del proprio territorio, ma deve essere vista come il controllo di una grande città metropolitana, dove ogni giorno migliaia di pendolari attraversano i confini, apportando esperienze e idee (Figura 12b).



a



b

↑ **Fig. 12** Due aspetti della difesa informatica.

In un attacco informatico, a differenza di una guerra convenzionale, **chi difende è sempre in svantaggio**, per diverse ragioni:

- chi attacca opera al di fuori della legge, mentre chi difende deve rispettarla;
- gli attacchi informatici non sono frontali, ma spesso avvengono in modo silenzioso, dietro le linee, e talvolta non si è nemmeno consapevoli di essere sotto attacco o di aver subito un attacco;
- gli attacchi possono essere realizzati rapidamente sfruttando varianti di malware o innestandosi su di essi;
- i malware con le loro varianti possono continuare a vivere per anni (un'era geologica in termini di programmazione!).

Uno dei pochi vantaggi del difensore è la **possibilità di disegnare**, **a proprio piacimento**, **il campo di battaglia**. Spetta al difensore, infatti:

- organizzare la propria rete e disporre i sistemi di difesa (firewall, server di autorizzazione, DMZ) nel modo più efficace;
- variare la topologia della rete e dei dispositivi per rendere difficile il lavoro di ricognizione dell'attaccante;
- predisporre delle trappole ("honeypot") che facciano credere all'attaccante di essere penetrato nel sistema della vittima, ma che, in realtà, servono a quest'ultima per studiare il suo comportamento, gli strumenti e le modalità di attacco.

Tutto ciò, in teoria. La riconfigurazione di una rete, e l'aggiornamento dei sistemi operativi e delle applicazioni che su di esso girano, richiedono un notevole impegno in termini di tempo e costi, che non sempre sono sostenibili.

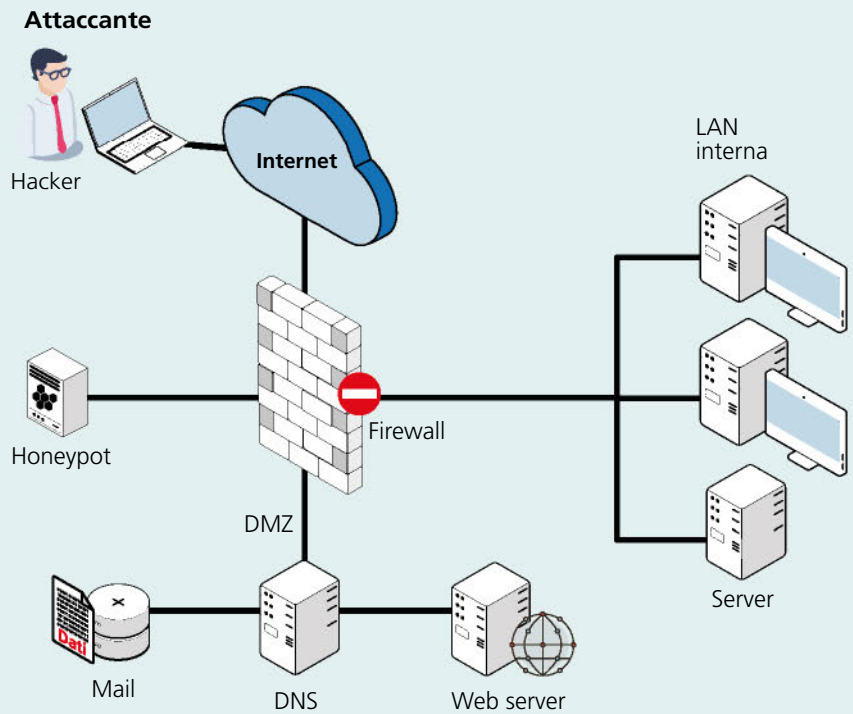
La sicurezza informatica, oltre a costare, pone anche delle limitazioni a chi la utilizza. Per esempio non è possibile accedere dalla rete aziendale a certi siti o ricevere allegati di un certo genere.
Tuttavia la sicurezza è necessaria. Nessuno di noi acquisterebbe un'auto che, pur costando meno, non ha superato i crash test, o non indosserebbe le cinture di sicurezza solo perché sono un po' fastidiose e possono creare qualche impaccio nella guida.

Comprendi con l'analogia

Gli honeypot per gli hacker sono come barattoli di miele per le api.



Quando ero alle scuole superiori, avevo una vera ossessione per le api e il loro affascinante modo di comunicare e operare. Un giorno di aprile, in una splendida giornata di sole, decisi di studiare questi formidabili insetti. Preparai un barattolo di miele e lo posizionai sul davanzale della finestra.
Poco dopo, un'ape operaia si avvicinò. Attratta dal profumo dolce del miele, si posò sull'apertura del vaso e, dopo qualche minuto, carica del prezioso alimento, si allontanò verso l'alveare. Nel giro di un'ora, decine di api vennero a trovarmi. Le osservai attentamente e le potei studiare da vicino.
Il barattolo di miele, proprio come gli honeypot informatici, può essere una trappola irresistibile. Così come l'ape viene attirata dal miele, gli attaccanti informatici vengono attratti da sistemi progettati appositamente con debolezze e vulnerabilità. L'osservazione delle mosse degli attaccanti ci permette di imparare, saggiare le loro tecniche e proteggere i nostri sistemi.



Un tipico caso di posizionamento di honeypot in rete, in modo che sia accessibile dall'esterno senza compromettere la sicurezza della rete interna.

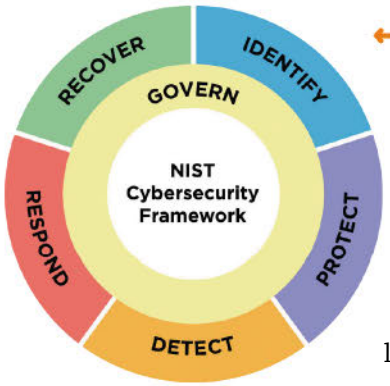


Fig. 13 Il NIST è un'agenzia del Dipartimento del Commercio degli Stati Uniti che si dedica alla promozione dell'innovazione della scienza delle misurazioni e della tecnologia. Redige standard e pubblica linee guida, in particolare nel campo della sicurezza informatica e della privacy. Le linee guida presenti in CSF 2.0 offrono un riferimento importante per chi opera in questo campo.

Sulle tecniche di difesa e di gestione degli attacchi, Il **Cybersecurity Framework** (**CSF**) **2.0** del *National Institute of Standards and Technology* (**NIST**) offre delle linee guida che guidano il processo per individuare e ridurre i rischi relativi alla sicurezza informatica (**Figura 13**). Rientrano tra i suoi obiettivi l'analisi degli attacchi, le procedure per la preparazione e la risposta a situazioni critiche e il ripristino della normalità.

Incident Response Life Cycle

"Incident Response LifeCycle" è un modello per la gestione degli incidenti informatici, proposto dal NIST (*National Institute of Standards and Technology*). La Revisione 3 del NIST SP 800-61 introduce un approccio che distingue chiaramente la fase di preparazione dalla fase di risposta agli incidenti, e sottolinea l'importanza dell'apprendimento e miglioramento continuo. La **Figura 14** illustra il modello.

- La parte di sinistra si riferisce alla Preparazione all'incidente con le necessarie funzioni di pianificazione.
- A destra è rappresentato il ciclo di vita della risposta (*Incident Response Life Cycle*) a incidenti e comprende i blocchi che illustrano le azioni pratiche che devono essere intraprese in caso di attacco, al fine di mitigare gli effetti degli incidenti e ripristinare le normali attività.

Pit Stop

9 Che cos'è l'Incident Response Life Cycle?

Il significato delle frecce arancioni nella figura evidenzia il passaggio di informazioni tra le diverse funzioni:

- la freccia 1 indica che l'output della fase "Attività post-incidente" diventa un input per la fase "Preparazione". In altre parole, le **lezioni apprese** durante la gestione di un incidente vengono inviate alla funzione di **Identificazione**, in cui sono analizzate, classificate e, quindi, utilizzate per migliorare i piani di preparazione e prevenzione per gli incidenti futuri;
- la freccia 2 suggerisce che la funzione di Risposta può richiedere **ulteriori indagini** se emergono nuovi dettagli durante la gestione dell'incidente;
- la freccia 3 rappresenta lo scambio di informazioni tra le diverse funzioni del processo di risposta agli incidenti per **migliorare continuamente** le strategie attraverso l'apprendimento.

notabene

Nella pratica quotidiana, le minacce informatiche possono essere mitigate adottando alcune precauzioni e contromisure. Queste includono: mantenere il software aggiornato, effettuare backup regolari, utilizzare password complesse con autenticazione a due o più fattori, utilizzare un antivirus, servirsi di una connessione sicura con protocollo HTTPS, prestare attenzione alle e-mail sospette e utilizzare una VPN per proteggere dati e privacy.

Analizziamo ciascun blocco.

Fase di Preparazione (*Preparation*)

La preparazione è la fase pre-incidente. È il momento in cui un'organizzazione si prepara ad affrontare gli attacchi informatici. Prevede tre fasi:

- **Governo** (*Govern*). L'obiettivo è individuare delle strategie di sicurezza da adottare: pianificare gli obiettivi, effettuare l'analisi dei rischi e assegnare le priorità ai diversi eventi che possono avvenire. In questa fase sono definiti i regolamenti, le procedure e le linee guida (policy) che stabiliscono come gestire la sicurezza all'interno dell'organizzazione. In questo modo, si cerca di prevenire gli accessi non autorizzati e proteggere i dati, mitigando eventuali danni che possono verificarsi. Si prevedono anche azioni di sensibilizzazione e formazione per i dipendenti, e lo stanziamento di fondi per il software e l'hardware necessari alla sicurezza.

- **Identificazione** (*Identify*): è la fase in cui si cerca di valutare i rischi e identificare debolezze e vulnerabilità dei sistemi. L'obiettivo della fase di identificazione è studiare l'impatto di un incidente, anche a partire dagli errori commessi in precedenza. L'analisi deve tener conto della probabilità del verificarsi di un evento e della sua criticità, quali e quanti utenti sono coinvolti, che credenziali hanno ottenuto gli aggressori e come sono state utilizzate
- **Protezione** (*Protect*): Una volta individuate le vulnerabilità, è necessario prendere misure di prevenzione per contenere i rischi e per proteggere i beni aziendali, hardware e software, da potenziali attacchi. Queste misure riguardano l'aggiornamento delle versioni di sistemi operativi e delle applicazioni per la correzione delle vulnerabilità conosciute, la protezione dei dati con la crittografia, la revisione della configurazione della rete aziendale con l'introduzione, se necessario di blocchi di controllo intermedi come firewall, sistemi specializzati di rilevamento delle intrusioni e controllo degli accessi.

notabene

La pandemia COVID-19 ha spinto molte aziende ad adattarsi velocemente alle sfide imposte dal lavoro a distanza, adeguando le proprie politiche di sicurezza informatica all'aumento delle minacce e alle nuove normative sulla privacy.

Fase di Risposta agli incidenti (*Incident Response Life Cycle*)

- **Rilevamento** (*Detect*). È la fase che riguarda la rilevazione e l'identificazione di eventi sospetti o anomalie che potrebbero essere il sintomo di un attacco o una violazione della sicurezza. Durante questa fase si esegue l'analisi degli eventi sospetti che provengono dalla rete e dai sistemi. Sono controllati, ad esempio, il log degli utenti con tentativi fatti e password errate, il log dei firewall con le attività sulle porte per il traffico dall'esterno verso l'interno e viceversa, le e-mail sospette, i siti compromessi, Ogni evento viene correlato e può scatenare scenari diversi a seconda della priorità che gli è assegnata.
  Nei sistemi di sicurezza come SIEM (*Security Information and Event Management*), sono di norma impiegate operazioni automatiche basate sull'Intelligenza Artificiale, che consentono di analizzare e gestire grandi quantità di informazioni. L'utente, in questo contesto, viene sollevato dal compito di analizzare manualmente i dati. La sua responsabilità principale è prendere decisioni basate sui suggerimenti forniti dagli algoritmi intelligenti del sistema.

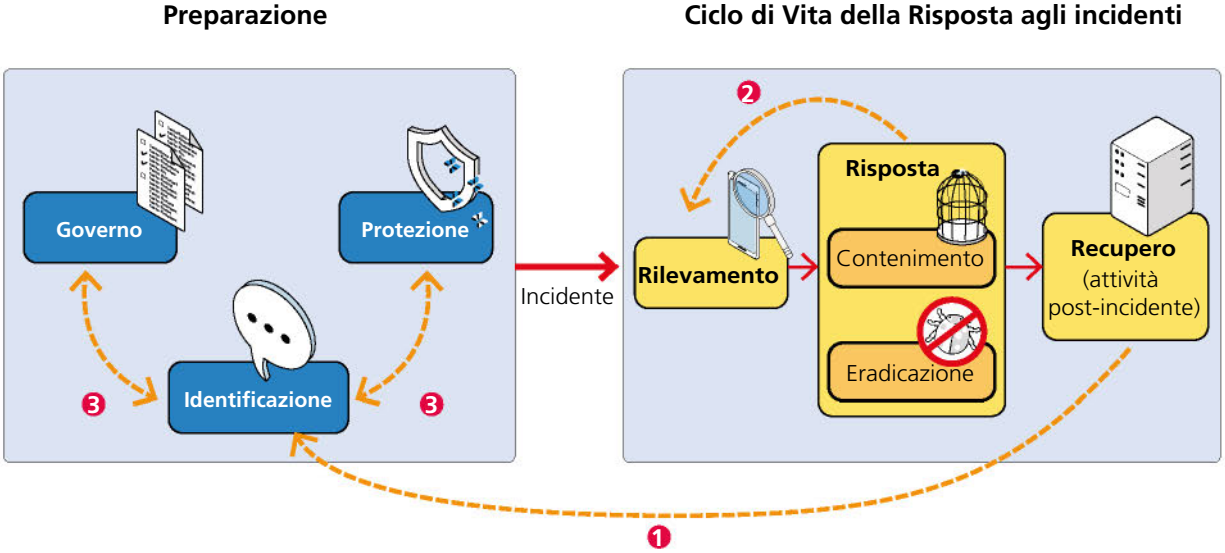


Fig. 14 Il modello NIST SP 800-61 Revisione 3 offre un modello operativo relativo risposta agli incidenti di sicurezza. Le frecce verdi rappresentano: **1.** l'output della fase "Attività post-incidente" è un input per la fase "Preparazione" (blocco Identificazione); **2.** La funzione di Risposta può richiedere nuovi approfondimenti nel caso siano emersi emessi nuovi dettagli; **3.** scambio di informazioni per il migliorare le risposte a incidenti futuri.

notabene

L'OWASP (*Open Worldwide Application Security Project*) è una fondazione senza scopo di lucro che lavora per migliorare la sicurezza del software. Fornisce la top 10 delle vulnerabilità più sfruttate, tra cui: difetti di progettazione software, configurazioni di sistema errate, componenti vulnerabili e obsoleti, errori di autenticazione e problemi legati alla crittografia.

- **Risposta** (*Respond*). È il momento di contenere l'attacco evitando ulteriori danni, promuovendo un insieme di azioni:
  - **contenimento** (*Containment*). La prima attività consiste nell' isolare le macchine colpite, spegnendole e rimuovendole dalla rete. È importante considerare che la disattivazione dei sistemi può avere un impatto negativo sull'organizzazione. Pertanto, è fondamentale informare la direzione sulla gravità dell'incidente, prima di agire.
  - **Eradicazione - Mitigazione** (*Eradication*). Durante l'eradicazione, si rimuovono completamente le minacce disinstallando i software dannosi, pulendo i file infetti, e correggendo le vulnerabilità. Tuttavia, prima della rimozione del malware è necessario analizzare a fondo le cause che hanno provocato l'incidente. A questo scopo ci si basa sugli Indicatori di compromissione (*Indicators of compromise* – IOC) che sono gli elementi necessari per analizzare i comportamenti di un particolare malware (**Tabella 2**). Questi indicatori possono anche costituire la prova forense di potenziali intrusioni in un sistema o in una rete, anche se occorre stare attenti a non inquinare le prove, salvare i file su disco e acquisire il dump della memoria volatile prima che il sistema venga spento.
- **Recupero** (*Recovery*). La fase di riparazione inizia subito dopo la rimozione del malware e riguarda il ripristino dei sistemi e il ritorno alla normalità, con l'esecuzione di una serie di azioni:
  - **Recupero dei dati**. Si procede al recupero dei dati che sono stati persi o danneggiati. Questo può avvenire attraverso la ricostruzione da zero del sistema o il ripristino a partire da un backup affidabile.
  - **Analisi post-incidente**. Dopo aver risolto l'incidente, si riflette sulle cause che hanno provocato l'evento.

  Imparare dagli errori commessi avrà una ricaduta sul modulo "identificazione" e servirà per prevenire problemi che potrebbero verificarsi in futuro. Valutare i danni causati dall'incidente prevede anche di informare gli enti preposti, oltre che il personale, i clienti e i fornitori, sulla gravità dell'incidente e sulle azioni intraprese per affrontarlo.

Variazioni significative nel traffico in entrata e in uscita dalla rete, ad esempio, i dati che passano attraverso il firewall variano improvvisamente da pochi GigaByte al giorno a decine di GigaByte.
Rallentamento nell'esecuzione dei processi e presenza di applicazioni sconosciute.
Comparsa di nuove credenziali di amministratore o con privilegi particolari.
Tentativi di accesso ripetuti o di dubbia provenienza.
Aumento del traffico su porte di rete che non vengono normalmente utilizzate .
Modifiche non autorizzate alle impostazioni dei registri di sistema.
File manomessi o posizionati in cartelle in cui non dovrebbero essere presenti.

→ **Tab. 2** Alcuni Indicatori di compromissione.

Pit Stop

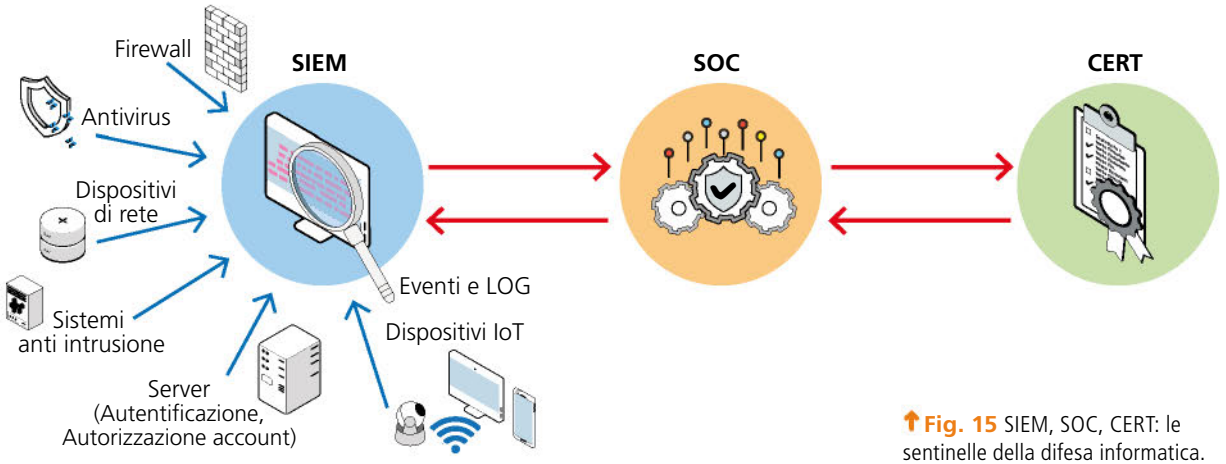
10 Quali sono le fasi della Cyber Kill Chain che gli hacker devono superare per riuscire a portare a termine un attacco informatico?

SIEM, SOC, CERT: le sentinelle della difesa informatica

Nel vasto panorama della sicurezza informatica, diversi attori rivestono ruoli cruciali come difensori, collaborando attivamente per salvaguardare le organizzazioni dalle minacce. Analizzeremo in particolare tre di questi protagonisti (come illustrato nella **Figura 15** e nella **Tabella 3**):

- **SIEM** (*Security Information and Event Management*). Questo sistema raccoglie e organizza i dati provenienti dalla rete, comportandosi come una sentinella che sta in prima linea a rilevare movimenti e attacchi del nemico.
- **SOC** (*Security Operations Center*). Questo centro operativo esamina le informazioni raccolte da SIEM, cercando di capire cosa significano e individuando possibili pericoli.
- **CERT** (*Computer Emergency Response Team*). Questo gruppo di lavoro sviluppa strategie di difesa, usando le informazioni raccolte da SIEM e analizzate da SOC.

SIEM e SOC lavorano a stretto contatto, come una squadra, per monitorare e proteggere la rete. Il CERT fornisce un supporto importante, elaborando piani d'azione basati sulle informazioni ricevute dal SOC.



↑ **Fig. 15** SIEM, SOC, CERT: le sentinelle della difesa informatica.

Comprendi con l'analogia

Il modello NIST per gli attacchi informatici è come una strategia per difendersi dall'influenza



La mia amica Camilla, che conosco fin dall'infanzia, è sempre stata molto cagionevole; per questo è molto prudente quando arrivano i primi freddi. Sa che l'influenza è in agguato e si prepara in anticipo: si fa il vaccino, compra un termometro e tiene sempre a portata di mano un comune medicinale a base di paracetamolo. Tuttavia, un giorno Camilla si sveglia e si sente un po' strana. Misura la temperatura con il suo termometro e legge 38,5 gradi: probabilmente ha l'influenza.
Camilla se bene cosa fare: prende il paracetamolo per abbassare la febbre e contenere i sintomi influenzali, e si isola restando a letto. Dopo qualche giorno, la febbre è passata ma rimane una forte tosse. Camilla si fa visitare dal medico che le prescrive un antibiotico per eradicare i batteri che sono sopravvenuti. Dopo aver preso l'antibiotico, Camilla si sente molto meglio, ma è ancora un po' debole. Per rimettersi in forze e ripristinare completamente le sue funzioni prende un ricostituente.
Durante tutto questo processo, Camilla ha imparato una lezione importante. Ha capito che, quella sera era meglio non uscire sudata, quando la temperatura era sotto lo zero, soprattutto se in discoteca c'erano 23 gradi. Oggi, Camilla ha deciso anche di spedire un rapporto al suo medico spiegando tutto ciò che è successo. E così Camilla ha gestito l'arrivo dell'influenza in modo simile a quanto proposto da NIST nel suo modello di risposta agli incidenti.

Definizione	SIEM (Security Information and Event Management)	SOC (Security Operation Center)	CERT (Computer Emergency Response Team)
Obiettivo	Rilevare le minacce, prima che si arrivi a un incidente che comprometta il sistema.	Ridurre gli effetti degli attacchi e cercare di prevenire il verificarsi di incidenti.	Raccogliere e diffondere informazioni sulla sicurezza. Identificare nuove vulnerabilità, condividere avvisi di sicurezza, fornire linee guida su come mitigare le minacce.
Ruolo	Sistema progettato per monitorare, raccogliere e analizzare volumi di eventi di sicurezza in tempo reale. si occupa grandi di monitorare le attività, raccogliere, analizzare e classificare i dati per individuare minacce.	All'interno di un'organizzazione, il team SOC è responsabile del monitoraggio, rilevamento, analisi e risposta in tempo reale, alle minacce e agli incidenti. Il team di un SOC è in genere composto da persone specializzate tra cui analisti della sicurezza, persone preparate a rispondere agli incidenti e a fare le prove di penetrazione nei sistemi (**Figura 16**).	Un team interno a un'azienda, o a un ente governativo che si occupa di incidenti di sicurezza informatica e che, in collaborazione con SOC, si interessa della risposta agli incidenti In Italia, oltre ai CERT delle diverse realtà aziendali, sono da citare quelli della Pubblica Amministrazione (CERT-PA) e dell'Agenzia per l'Italia Digitale (CERT-AGID). CSIRT (Computer Security Incident Response Team) ha un ruolo simile a CERT, ma più operativo.
Funzioni	Raccolta di log ed eventi provengono dai sistemi in rete e dalle applicazioni, che possono riguardare: • La gravità dell'attacco, il numero dei dispositivi infettati e i servizi compromessi. • La natura del malware, la sua firma, l'origine del vettore che ha diffuso l'attacco. • Le contromisure da prendere e gli aggiornamenti disponibili.	• Monitoraggio Continuo della rete aziendale per rilevare attività sospette o anomalie. Ad esempio controlla gli accessi al sito web aziendale rilevando indirizzi IP sospetti o di altra nazionalità. • Aggregazione e interpretazione dei dati (Threat Intelligence) • Attivazione delle contromisure necessarie per bloccare o limitare il danno. • Scelte strategiche per prevenire e combattere le minacce	Risoluzione degli Incidenti: analisi dell'incidente, mitigazione dei danni e ripristino del sistema. Redazione di linee guida linee guida per la gestione degli incidenti allerte riguardante nuove minacce aggiornamento e sviluppo delle tecniche di difesa campagne di sensibilizzazione pubblica
Intelligenza artificiale (IA)	L'intervento di IA sui sistemi SIEM, porta numerosi vantaggi legati all' automatizzazione dei processi di rilevamento: • riduce i tempi di risposta sollevando gli operatori da analisi manuali di eventi che, in aziende medio grandi, possono essere decine di migliaia al secondo; • aiuta a identificare modelli di comportamento anomali che potrebbero sfuggire all'analisi umana; • correla automaticamente tutti gli eventi rilevati in rete fornendo un quadro completo per comprendere che cosa è realmente avvenuto.	Utilizza strumenti di intelligenza artificiale per monitorare la rete in modo continuo per rilevare anomalie che potrebbero indicare possibili attacchi informatici. SOAR (Security Orchestration, Automation, and Response) è una metodologia che unisce le attività di: • coordinamento delle attività e dei processi di sicurezza (orchestrazione) • automazione per avere risposte • azioni di risposta con l'invio di notifiche, la revisione delle regole dei firewall ecc.)	Le grandi quantità di dati provenienti da diverse fonti, che vengono trattate da IA, possono individuare comportamenti sospetti e avvisare suonare come un campanello di allarme per il CERT che può fare capirne la gravità e assegnare la priorità. Inoltre l'IA può analizzare i dati storici e prevedere comportamenti futuri. In alcuni casi è possibile rispondere in modo automatico ad alcune attività sospette, bloccando l'accesso a risorse compromesse o isolando parti di rete. L'IA può esaminare eventi, attività e fornire prove per ricostruire gli incidenti e supportare l'analisi forense del CERT.

→ Tab. 3

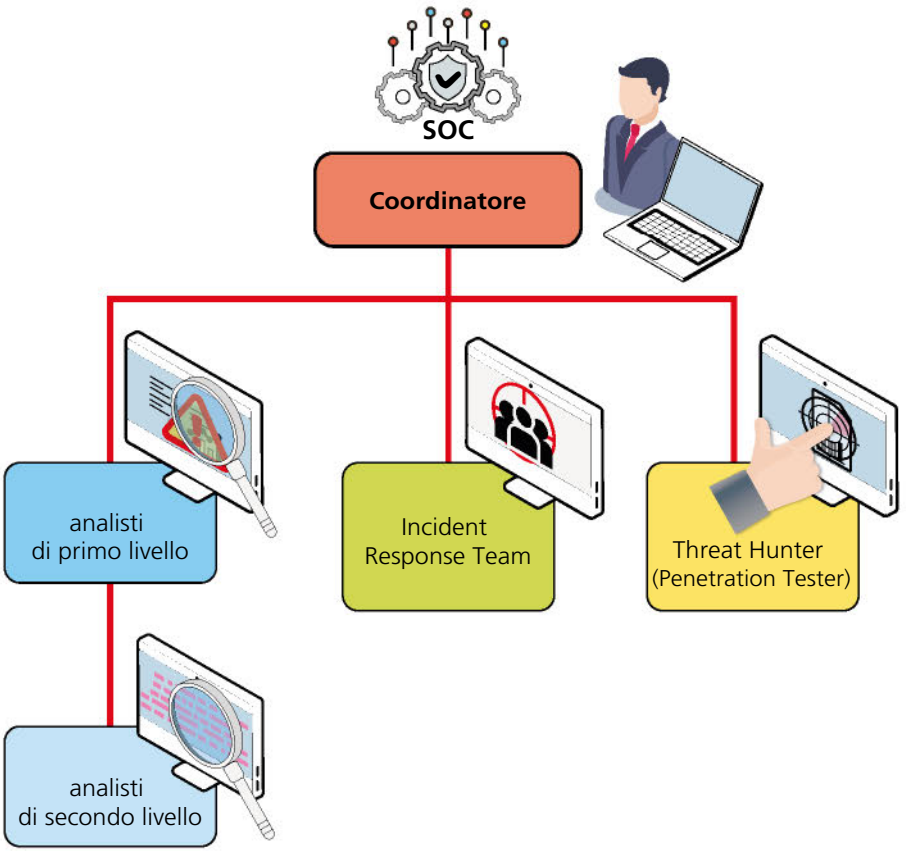


Fig. 16 Struttura semplificata di un team SOC di primo livello che valuta la gravità dell'incidente e, se necessario, richiede l'intervento degli analisti di sicurezza di secondo livello e, quindi, del gruppo *Incident Response Team* che pone rimedio ai problemi causati dall'incidente. I *Threat hunter* fanno indagini e prove (*Penetration Test*) sugli incidenti di sicurezza per determinare le cause dell'incidente.

Pit Stop

11 Quali caratteristiche distinguono SIEM da SOC?

12 Qual è il ruolo di un CERT?

Comprendi con l'analogia

Il primo livello di analisi del SOC (Security Operations Center) funziona come un triage ospedaliero.



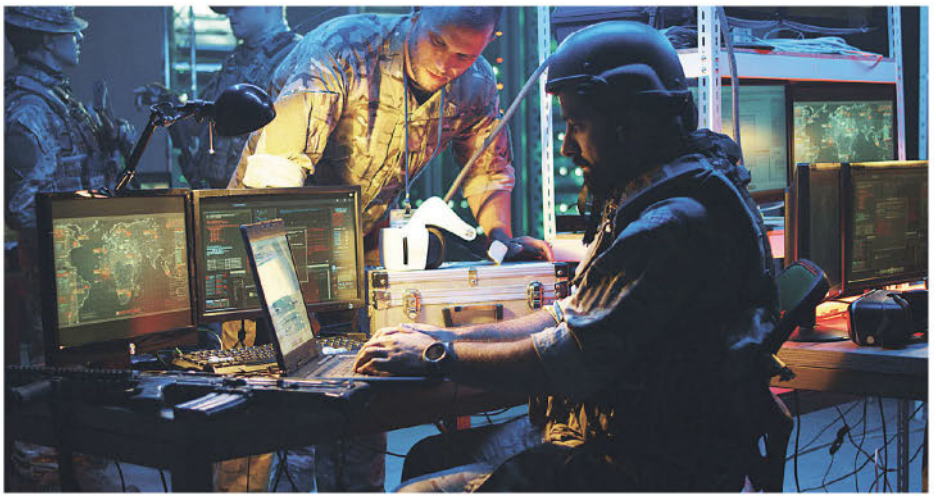
Nel triage ospedaliero, i pazienti vengono valutati e classificati in base alla gravità delle condizioni, assegnando loro un codice di priorità: **bianco**, **giallo**, **verde** o **rosso**. Allo stesso modo, il primo livello del SOC esegue un triage delle segnalazioni di sicurezza, innescando diversi scenari a seconda della loro gravità: per segnalazioni di codice bianco o verde, che potrebbero riguardare, ad esempio, un sito web malevolo da evitare o un malware bloccato dall'antivirus, il SOC gestisce la situazione internamente senza necessità di ulteriori interventi; per segnalazioni di codice giallo o rosso, che indicano una minaccia più grave, il SOC non solo interviene con il proprio team di risposta, ma coinvolge anche il CERT (*Computer Emergency Response Team*). Un esempio di segnalazione di codice giallo potrebbe essere un malware che sta cifrando dati ma non ha ancora esfiltrato informazioni, situazione critica ma non urgente. Un esempio di segnalazione di codice rosso potrebbe essere un malware che sta esfiltrando dati, una situazione critica che richiede un intervento urgente.

notabene

Un algoritmo di hash trasforma i dati contenuti in un file in una stringa di caratteri di dimensione fissa e univoca, la sua firma. Gli antivirus utilizzano gli hash dei file sospetti per identificare i malware conosciuti.

Approfondimento - Tecnologia

Le armi della guerra convenzionale vs “Cyber Warfare”



Le strategie e le armi impiegate in una guerra convenzionale si differenziano significativamente da quelle della guerra cibernetica, comunemente definita “Cyber Warfare”. Quest’ultima può precedere o operare parallelamente ai conflitti tradizionali.
Alessandro Curioni, un esperto di cyber security, caratterizza la guerra cibernetica come un conflitto silenzioso, in cui le armi sono invisibili e «hanno una relazione molto stretta con il loro obiettivo e da esso dipende la loro efficacia. Per fare un paragone con il mondo reale, si può immaginare una guerra in cui per distruggere ogni singolo tipo di struttura (un aeroporto, una strada, una centrale elettrica...) sia necessario costruire uno specifico missile. L’indissolubile rapporto che nel cyber lega arma e obiettivo viene definito dal termine vulnerabilità. Per colpire con successo è indispensabile l’esistenza di una o più debolezze che possano essere sfruttate per ottenere il risultato atteso» (Aldo Giannuli, Alessandro Curioni, *Cyber war. La guerra prossima ventura*, Mimesis, 2019).
Un’altra differenza riguarda l’analogia tra un attacco DDoS e un bombardamento fisico. Siamo purtroppo testimoni di come migliaia di bombe convenzionali, sganciate su un obiettivo, possano devastarlo, richiedendo anni per la ricostruzione e provocando tragedie umane indescrivibili. In contrasto, un attacco cibernetico DDoS, sebbene possa essere equiparato al lancio simultaneo di migliaia di bombe, non lascia danni fisici duraturi, consentendo una ripresa immediata delle attività non appena terminato.

Approfondimento
Cryptolocker

Laboratorio

ATTIVITÀ 1
Caso di studio: WannaCry

Scenario

WannaCry è un malware di tipo ransomware, che cripta i file presenti sui computer e chiede un riscatto per ottenere la chiave di decrittazione. Nel 2017 è stato responsabile di un'epidemia che ha coinvolto decine di migliaia di computer. Per le modalità di attacco, costituisce un punto fermo nello studio della sicurezza informatica.

Consegna

Presentare il caso e analizzare i fatti in modo critico. Compilare la tabella proposta, evidenziando la cronologia degli eventi, il funzionamento tecnico, l'impatto, la lezione appresa e le strategie per prevenire futuri attacchi di ransomware.

Svolgimento

Passo 1: introduzione
Il 27 maggio 2017 una grande quantità di sistemi nel mondo sono attaccati da un ransomware che, all'apparenza, non ha nulla di speciale. Molto presto, però, emerge la vera natura dell'attacco: dietro la richiesta di riscatto, il vettore del malware WannaCry trasporta nella testata l'exploit **EternalBlue**, un codice che sfrutta una vulnerabilità del sistema operativo, fa guadagnare l'accesso non autorizzato al sistema e invia comandi da remoto.

Passo 2: analisi tecnica
WannaCry sfrutta la vulnerabilità EternalBlue/DoublePulsar, precedentemente utilizzata dalla National Security Agency NSA americana e trafugata e resa di pubblico dominio dal gruppo hacker Shadow Brokers. EternalBlue e DoublePulsar (CVE-2017-0145) sono utilizzati in combinazione:

- EternalBlue è una vulnerabilità del protocollo Server Message Block v.1 (SMBv1) di Microsoft, che permette a un attaccante di far eseguire codice da remoto a un server SMBv1.
- DoublePulsar è una backdoor che viene installata segretamente nel computer, per accedere al sistema senza essere scoperti. Una volta dentro al sistema, l'attaccante può inserire codice malevolo o infettare e crittografare i dati presenti.

WannaCry possiede un'altra inquietante funzionalità che, però, ha permesso di fermare la diffusione del malware: il "**kill switch**", un "grilletto di sicurezza", scoperto dal ricercatore Marcus Hutchins nel momento più drammatico, quando sembrava tutto perduto. Marcus scopre che il malware, prima di iniziare la crittografia dei file, tenta di connettersi a un URL specifico. Se ci riesce, il ransomware procede con l'infezione, altrimenti il malware interrompe l'attacco. Marcus registra il dominio web e, magicamente, WannaCry interrompe il processo di crittografia e cessa di diffondersi. Il mondo tira un respiro di sollievo!

notabene

Il Server Message Block versione 1 (SMBv1) è un protocollo di rete utilizzato per accedere, in rete, a file, stampanti e altre risorse. A causa delle sue vulnerabilità, SMBv1 non è più installato sulle versioni Windows 11 e Windows Server 2019 e successive.

Passo 3: tabella di sintesi di WannaCry

Scenario incidente
• Data: 27 maggio 2017 • Enti interessati: computer in tutto il mondo • Informazioni di base: ransomware
IOC Elenco indicatori di compromissione
• Modifiche ai file di sistema/file crittografati. • Messaggio con richiesta di riscatto: WannaCry richiede un riscatto in Bitcoin per il recupero dei file crittografati. • Rilevamento da parte del sistema anti intrusioni (IDS) o firewall di comunicazione con domini o indirizzi IP sospetti: WannaCry comunica con server di comando e controllo per scaricare e installare ulteriori malware. • Utilizzo elevato della CPU o del disco, utilizzato da WannaCry per crittografare i dati. Scoperta della vulnerabilità EternalBlue.
Effetto e criticità
• Gravità: colpiti più di 300.000 computer in oltre 150 paesi per una perdita di centinaia di milioni di dollari. • Vittime (tra le più note): Servizio Sanitario Nazionale del Regno Unito, Honda, Nissan, FedEx. • Materiale sottratto: non ha sottratto dati. • Impedimento del servizio: interruzioni significative dei servizi, come la chiusura temporanea di fabbriche o l'annullamento di migliaia di operazioni chirurgiche e appuntamenti medici.
Modalità di attacco con analisi dettagliata della minaccia
EternalBlue e DoublePulsar sono utilizzati in combinazione: EternalBlue è una vulnerabilità del protocollo Server Message Block v.1 (SMBv1) di Microsoft. DoublePulsar è una backdoor. Presenza di un "kill switch" che interrompe l'azione di WannaCry. La presenza di un "grilletto di sicurezza", che può fermare l'attacco in qualsiasi momento, ci potrebbe far pensare a un'azione dimostrativa o a una prova per capire l'impatto del codice malevolo e saggiare le reazioni degli attaccati. Wannacry nell'attacco ha veicolato un ransomware, ma avrebbe potuto portare con sé anche altro, come ad esempio un keylog.
Protezione e prevenzione (Azioni correttive per eradicare il problema)
È fondamentale installare sui sistemi gli aggiornamenti più recenti per proteggere i dispositivi da queste e altre vulnerabilità. (*Microsoft aveva rilasciato la correzione della vulnerabilità nel marzo 2017, prima di WannaCry. Purtroppo non tutti gli utenti e le organizzazioni avevano installato questo aggiornamento con il conseguente contagio.*)
Fonti di riferimento e materiale
CVE-2017-0144 WannaCry e EternalBlue CVE-2017-0143 DoublePulsar

notabene

La National Security Agency (NSA) è un'agenzia degli Stati Uniti che si occupa della sicurezza delle comunicazioni e delle attività di intelligence legate alla cybersicurezza e alla sorveglianza elettronica, con l'intento di prevenire e mitigare gli attacchi cibernetici.

ATTIVITÀ 2
Caso di studio: LockBit

Scenario

Immaginate questa situazione: la vostra società di sicurezza informatica, di cui siete il responsabile, viene informata dal SOC che durante l'analisi del traffico in rete è stato individuato un file sospetto. Questo file presenta i seguenti Indicatori di Compromissione (IoC):

`MD5: af9ff037caca1f316e7d05db86dbd882`

`SHA-1: 844e9b219aaecb26de4994a259f822500fb75ae1`

Consegna

Analizzare gli indicatori e fornire evidenza del problema.

Svolgimento

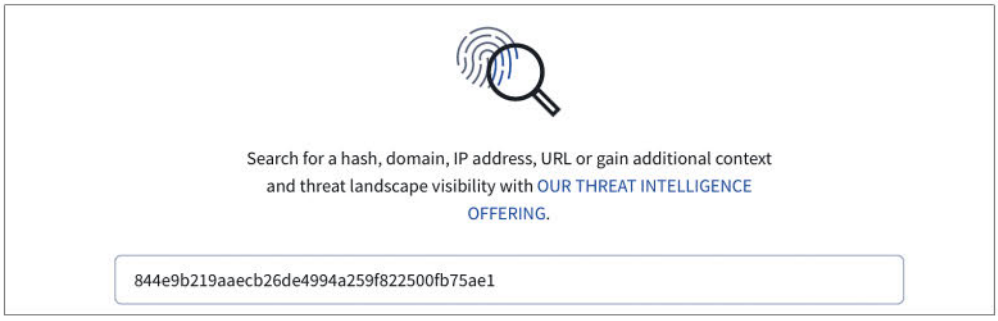
Passo 1: analisi con VirusTotal

Utilizziamo VirusTotal.

VirusTotal è un servizio online che permette di analizzare file e URL potenzialmente affetti da malware. VirusTotal aggrega molti prodotti antivirus e altre funzionalità, tra cui la distribuzione di regole YARA per identificare campioni e dispositivi compromessi (vedi l'**Attività 4**).

Procediamo in questo modo:

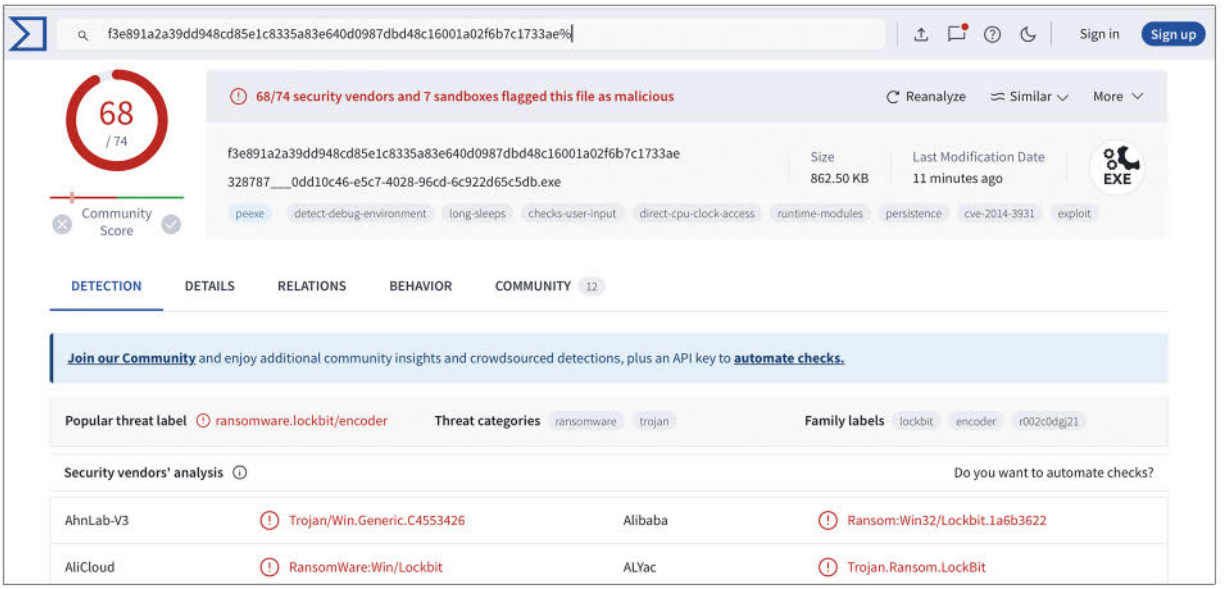
- Visitiamo il sito di VirusTotal all'indirizzo `https://www.virustotal.com`
- Inseriamo l'hash (SHA-1): `844e9b219aaecb26de4994a259f822500fb75ae1` nel campo di ricerca.



- Avviamo la ricerca.
- Analizziamo i risultati: VirusTotal mostra un rapporto dettagliato sul malware, che si basa su quanto riscontrato da diverse organizzazioni come Google, Microsoft, Kaspersky, Malwarebytes , McAfee ecc (**Figura 1**).

Passo 2: il malware LockBit

- Informazioni di base
  - Malware: *LockBitRansomware.exe* , un esemplare del ransomware **LockBit 2.0**.
  - Minacce: attacchi mirati contro organizzazioni per bloccare l'accesso ai sistemi informatici in cambio di un riscatto. Furto di dati e pubblicazione illegale come ricatto se la vittima non paga il riscatto.
  - LockBit funziona come un Ransomware-as-a-Service (**RaaS**), in cui gli sviluppatori del ransomware vendono il loro malware ad altri hacker, noti come affiliati RaaS (**Figura 2**).



↑ Fig. 1



→ Fig. 2

- Effetto e criticità applicata a un caso reale:
  - **Ente interessato**: Centro Elaborazione Dati della Regione Lazio.
  - **Data**: luglio 2021.
  - **Effetto**: dati crittografati e impedimento di servizio del portale "Salute Lazio" e della rete vaccinale.
  - **Modalità di attacco**:
    - infiltrazione nel sistema con le credenziali di un dipendente, con privilegi di accesso elevati, che in smart working accedeva alla rete della regione utilizzando una VPN;
    - utilizzo di un codice malevolo (probabilmente il trojan "Emotet"), distribuito tramite e-mail, che ha permesso di aprire una breccia e ottenere il pieno controllo del sistema tramite comunicazioni di comando e controllo da remoto;
    - installazione del ransomware, che ha criptato i dati e chiesto il riscatto.
  - **Protezione e prevenzione**: il successo dell'attacco è stato favorito dalla mancanza di una procedura di autenticazione a due fattori da parte del dipendente. Da qui la necessità di procedure di accesso più severe e una campagna di sensibilizzazione sui rischi del lavoro da remoto e sull'utilizzo di software e antivirus aggiornati.

Passo 3: riflessione

LockBit, che è apparso per la prima volta nel 2019, ha subito un'evoluzione significativa nel tempo, passando da LockBit 2.0 a LockBit 3.0 nel 2022. Questa evoluzione ha portato a miglioramenti nel funzionamento del suo codice e alla correzione di diverse vulnerabilità, rendendo LockBit una delle minacce ransomware più potenti e diffuse a livello mondiale. Questi attacchi evidenziano la gravità delle minacce poste da LockBit, in particolare per la loro continua evoluzione, un fenomeno comune a molti altri malware.

ATTIVITÀ 3
Caso di studio: un attacco APT

Scenario

Analisi di un caso reale di social networking analysis e spear phishing. Presentiamo un caso reale, usando nomi e luoghi di fantasia, che mostra un furto informatico che utilizza le tecniche APT (*Advanced Persistent Threats*).

Consegna

Presentare il caso e analizzare i fatti in modo critico, evidenziando la cronologia degli eventi, il funzionamento tecnico, l'impatto, la lezione appresa e le strategie per prevenire futuri attacchi di questo genere. Fare riferimento alla Cyber Kill Chain.

Svolgimento

Passo 1: la composizione dei Team di Hacking
L'organizzazione cyber-criminale ("CYR"), specializzata in attacchi APT (*Advanced Persistent Threats*), accetta un incarico a pagamento per il furto di informazioni. Il mandato è quello di impossessarsi dei dati di MPTec Spa, azienda ad altissima tecnologia. Per prima cosa, i cyber-criminali organizzano il lavoro distribuendo i compiti ai propri team, **Verde**, **Rosso** e **Blu**, che sono specializzati in attività diverse.

- **Team Verde**: specializzato nella ricognizione e nello studio del modo in cui l'azienda bersaglio è esposta sul Web, e nell'analisi dei social network e dei circuiti ADS (pubblicità online). Questi canali si servono di società specializzate che danno agli inserzionisti la possibilità di diffondere la pubblicità in rete. Gli annunci sponsorizzati compaiono spesso nei motori di ricerca accanto ai risultati sulle parole chiave su cui si desidera attivare la campagna pubblicitaria, denominati Search Advertising, oppure in pagine di contenuto specifico, su portali, social network e così via.
- **Team Rosso**: esperto nell'exploiting delle infrastrutture dell'azienda, cioè nella capacità di identificare e sfruttare le vulnerabilità per penetrare all'interno della rete aziendale e acquisire i diritti di accesso ai sistemi. Il Team Rosso deve stabilire e mantenere un canale nascosto per l'esfiltrazione dei dati. I dati raccolti devono essere parcheggiati su un server compromesso preparato in precedenza, venire criptati e poi trasmessi a CYR. Il Team Rosso deve anche provvedere a creare dei malware e strumenti di attacco specifici per quel particolare tipo di azienda.
- **Team Blu**: specializzato nell'analisi dei dati esfiltrati, verifica delle informazioni e loro valorizzazione monetaria.

Passo 2: attività di Ricognizione

- Il Team Verde inizia l'attività **cercando informazioni** interessanti sull'azienda. Vengono consultati forum, social network, siti web, pagine archiviate, cataloghi ecc. In particolare, accedendo a LinkedIn, si scopre che la dottoressa Martina Bianchi ricopre il ruolo di System Administrator in MPTec, e ha competenza sui sistemi Windows e SQL Server. Infatti, nel suo profilo, vi sono numerosi riferimenti (endorsement) a queste tematiche, ai corsi di formazione che ha frequentato e alle certificazioni ottenute.
- Il Team Verde **identifica il profilo Instagram** di Martina Bianchi e scopre che è appassionata di animali, specialmente di cani e gatti, e ha molte amicizie in questo settore (lo si vede bene dalle foto, dai gruppi a cui è iscritta e dai like sui profili amici). In nessuno dei profili vi è però l'indirizzo e-mail aziendale, ma solo quello privato della sua posta Gmail.

- Il Team Verde **continua la ricerca di altri dipendenti** dell'azienda, ed ecco che scopre Mario Rossi, capo reparto di produzione. Il suo nome compare tra quelli iscritti a una newsletter dedicata alla sicurezza sul lavoro e l'indirizzo e-mail è quello aziendale: mario.rossi@mptec.com. Correlando le informazioni, il Team Verde fornisce al Team Rosso il profilo aziendale e privato di Martina: sarà lei l'obiettivo (target) per l'ingresso in azienda tramite l'indirizzo martina.bianchi@mptec.com.

Passo 3: armamento e distribuzione

- Il **Team Rosso inizia a preparare il terreno per l'attacco**, raccogliendo immagini attinenti a cani e gatti, nomi degli amici sul profilo Instagram di Martina, eventi, fiere canine, ecc. Queste informazioni vengono utilizzate per creare **un'e-mail** pertinente da inviare a Martina.
- L'e-mail contiene l'invito a un finto evento canino come ospite VIP, con il programma in allegato. L'allegato, un PDF malevolo, una volta aperto, installerà nel computer aziendale di Martina un piccolo software, denominato "dropper", creato apposta per installare un malware e aprire una backdoor sul sistema. Questo software comunica agli attaccanti l'esatta configurazione del computer di Martina: sistema operativo, livello di aggiornamento, antivirus installato, ecc.
- Per assicurarsi che l'allegato penetri in azienda bypassando tutti i filtri di sicurezza, gli attaccanti utilizzano un server appena compromesso, sfruttando una vulnerabilità "zero day" del sistema operativo mai utilizzata prima.

Passo 4: sfruttamento (Exploitation) e Installazione

- Dopo che Martina ha **aperto l'allegato**, il Team Rosso produce il malware vero e proprio, confezionato per eludere l'antivirus di Martina e installarsi nel suo sistema operativo.
- Completata la creazione, tramite la backdoor aperta con il dropper, il nuovo software viene installato da remoto senza destare sospetti nella vittima, che continua a usare il computer senza accorgersi di nulla. Il canale per entrare in MPTec è stato aperto.
- Nel caso l'attacco fallisse per l'intervento dei software antivirus/antispam, il Team Rosso si concentrerà sui canali pubblicitari in uso all'azienda, creando un exploit da diramare sul circuito ADS; così facendo, tutti i computer che visualizzano la pagina del sito mptec.com/news saranno infettati dal banner pubblicitario.

Passo 5: controllo della vittima ed esfiltrazione dei dati

- Con il canale di accesso aperto, il Team Rosso esfiltra nomi utenti e password dal computer di Martina, guadagnando sempre più privilegi d'accesso fino ad arrivare a quello di Administrator, ad esempio, usando un keylogger software, in grado di intercettare tutto ciò che viene digitato sulla tastiera.
- Con questo nuovo privilegio, gli attaccanti iniziano a ricercare in azienda informazioni di valore. I dati raccolti vengono crittografati e parcheggiati su un finto server Proxy.
- I dati crittografati saranno trasferiti a CYR tramite una VPN (*Virtual Privte Network*), o un tool di trasferimento punto-punto. Il trasferimento passa ancor più inosservato se i file vengono divisi in pacchetti e spediti al proxy con un protocollo UDP che non lascia traccia.

Passo 6: vendita delle informazioni

Il Team Blu è ora in grado di **decifrare e leggere le informazioni**, filtrarle e venderle sul **dark web**, ottenendo risultati economici considerevoli.

ATTIVITÀ 4

Caso di studio: matrice MITRE ATTACK

La matrice delle tattiche e tecniche (*Enterprise tactics*) di MITRE ATT&CK è una base di dati liberamente consultabile. Contiene le informazioni, divise in categorie, relative alle azioni che gli aggressori mettono in atto nei loro attacchi, su diverse piattaforme. Queste categorie contengono voci relative alla raccolta di informazioni, all'esecuzione dei malware, alla persistenza, fino all'esfiltrazione dei dati.

Scenario

La società MPTec Spa ha subito un attacco informatico. L'incidente è stato scoperto quando alcuni dipendenti si sono accorti di aver ricevuto una **e-mail di phishing** contenente dei file sospetti.
Fatte le dovute analisi, il SOC ha scoperto che gli attaccanti sono riusciti a infiltrarsi nella rete aziendale e a caricare nella cartella "root" del disco (C:\root) il file `gameover.txt`

```
C:\root>dir
 Directory di C:\root          .
21/05/2024  15:31               368 gameover.txt
C:\root>type gameover.txt
aW1wb3J0IHdnZXQNCg0KdXJsID0gJ2h0dHBzOi8vcHJvb2Yub3ZoLm5l-
dC9maWxlcy8xTWIuZGF0Jw0KbG9jYWxfcGF0aCA9ICcvcm9vdC8xTWIuZGF0Jw0KD-
Qp0cnk6DQojIERvd25sb2FkIHRoZSBmaWxlDQogICAgZmlsZW5hbWUgPSB3Z2V0L-
mRvd25sb2FkKHVybCwgb3V0PWxvY2FsX3BhdGgpDQogICAgcHJpbnQoZiJGaWxlI-
GRvd25sb2FkZWQ6IHtmaWxlbmFtZX0iKQ0KZXhjZXB0IEV4Y2VwdGlvbiBhcyBlO-
g0KICAgIHByaW50KGYiQW4gZXJyb3Igb2NjdXJyZWQ6IHtlfSIpDQo
```

notabene

I file utilizzati in questa attività sono a puro titolo dimostrativo e sono innocui.

Consegna

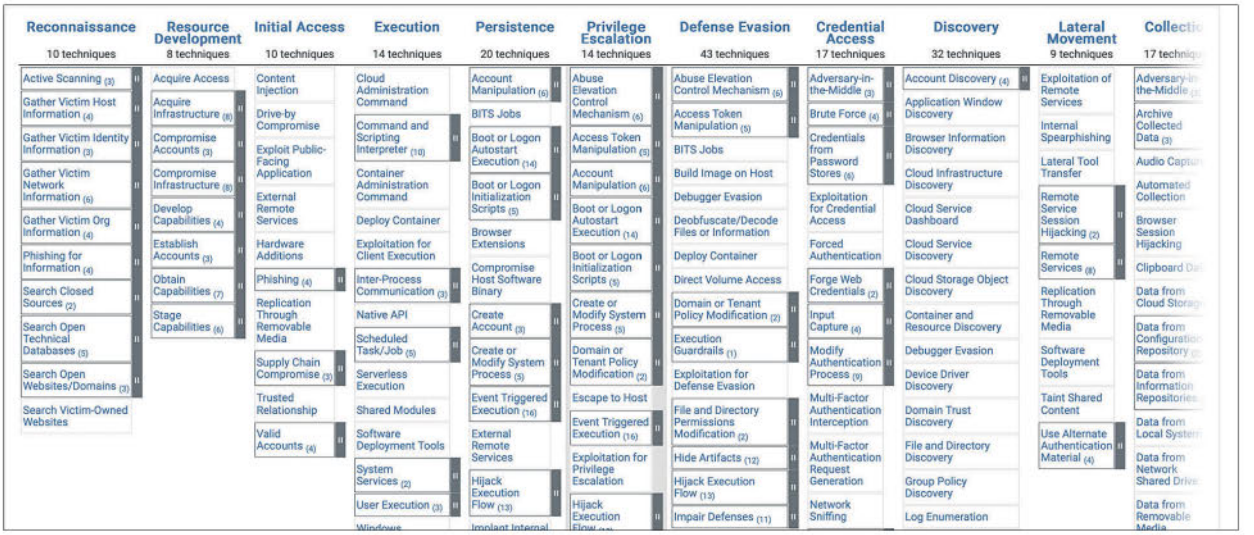
La vostra società è stata chiamata a **capire di cosa si tratta e a porre rimedio**.
Dopo aver analizzato lo scenario dell'attacco, decidete di **utilizzare le categorie e gli identificatori della "matrice delle tattiche" di MITRE ATT&CK** per:

- identificare le **tattiche** corrispondenti alle azioni degli attaccanti (ad esempio, Initial Access, Execution, Persistence, ecc.);
- specificare le **tecniche** utilizzate (ad esempio, Spear Phishing, Data Exfiltration, ecc.);
- suggerire **misure di mitigazione** e strategie di difesa per ciascuna tattica e tecnica identificata.

Svolgimento

Passo 1

Accedere al sito web MITRE ATT&CK (`https://attack.mitre.org/matrices/enterprise/`) e familiarizzare con la matrice delle tecniche e delle tattiche, studiandone le diverse voci presenti nelle colonne.



Passo 2

Lo studio dello scenario porta alle seguenti considerazioni:

FASE	TECNICA/TATTICA	ID MITRE ATT&ACK
Fase di Preparazione	Gli attaccanti creano un documento malevolo. Scrivono anche uno script Python che, una volta eseguito, scarica un file che potrebbe essere pericoloso.	
Fase di Attacco	• Gli attaccanti utilizzano tecniche di spear phishing per ottenere le credenziali di accesso di un amministratore di sistema. • Inviano un'e-mail di phishing con l'allegato malevolo a un elenco di destinatari selezionati. • Attendono che un destinatario apra l'allegato per eseguire il codice.	• T1566.001 • T1059.006

Fase di Post-Attacco	Lo script è offuscato con **codifica Code 64**. Si attua la decodifica (`https://www.base64decode.org/`) e si scopre che si tratta di uno **script Python**:
	`import wget`
	`url = 'https://proof.ovh.net/files/1Mb.dat'`
	`local _ path = '/root/1Mb.dat'`
	`try:`
	`# Download the file`
	`filename = wget.download(url, out=local _ path)`
	`print(f"File downloaded: {filename}")`
	`except Exception as e:`
	`print(f"An error occurred: {e}")`
	
	Questo script scarica il file specificato dall'URL e lo salva nella directory:
	
	`C:\root>python3 wgwtload.py`
		T1071

FASE	TECNICA/TATTICA	ID MITRE ATT&ACK
Fase di Post-Attacco	100% [.....] 1048576 / 1048576File downloaded: /root/1Mb.dat C:\root>dir 20/05/2024 09:10 <DIR> . 19/05/2024 12:21 1.048.576 1Mb.dat C:\root>type 1Mb.dat ┘)ú╗U┴Ó¯þñ$fáKzQª¥úñ7S}Pé©■╝õù³Éss,ÏÝ}È±Ì«Û?øÈÚéÃã¼h└5/╗V" ±ıÀ■cÆÒÃ├Ý¬Y,ùÏ£m7Ù`1Ù╦d'îS╠fì[ð╦╝[Û&┬ÈÈV╔¹t╝ÚuÊ°ý§i#╔§~bÿ ╬ë&}?¥-¼Ùì"»üØ╨┤`9wWqÇQ╠W©ËGÏ©ØtsÉ³v±Á]Å╦Év54ÅFX© ▒îFG┐┘n Ä┬ä▓t±k9u9&ñÖ╣yıÂklå3`$├■S¶¤Mí▓¾│\├▄ zûÑ »§¹ð¤ Testiamo il file scaricato (1Mb.dat) con Virustotal: risulta **innocuo**. "**No security vendors and no sandboxes flagged this file as malicious** 788d1a44b1633c8594def083d1b650e4842ea3e38d88c90228e7d581c6425c68 downloads%2F1Mb.dat" **Conclusione** Probabilmente si è trattato di un attacco effettuato solo per sondare le capacità di difesa della vittima, senza provocare danni. **Nota operativa** Python non è il linguaggio di programmazione più comune utilizzato per gli attacchi informatici, principalmente perché per eseguire i programmi scritti in questo linguaggio è necessario installare l'interprete Python sul computer della vittima. Inoltre, la funzione `wget`, che abbiamo utilizzato per comodità espositiva, deve essere installata nell'ambiente prima di poter essere utilizzata. Tuttavia, nonostante il file caricato in questo caso sia innocuo, le stesse tecniche possono essere utilizzate per caricare file malevoli, come quelli scritti in JavaScript o Visual Basic for Applications (VBA), che spesso sono utilizzati per gli attacchi, a causa della loro universale diffusione.	T1071
Misure di Mitigazione	• Formazione del personale aziendale a riconoscere e segnalare tentativi di phishing. • Autenticazione a più fattori per ridurre il rischio di compromissione delle credenziali. • Principio del minimo privilegio per limitare l'accesso alle cartelle solo agli utenti interessati • Segmentazione della rete per limitare lo spostamento degli attaccanti nelle cartelle del disco e nella rete ("movimento laterale").	• M1017 • M1032 • M1015 • M1030

ATTIVITÀ 5

Scanner delle vulnerabilità: Nmap, Kali Linux e YARA

Scenario

Per difenderci dobbiamo conoscere il nostro territorio, affidandoci alla mappatura della rete per identificare quali sistemi sono presenti, quali servizi sono ospitati e quali risorse presentano delle vulnerabilità. Questo ci permette di intervenire prima che lo faccia un attaccante. Ci metteremo nella posizione di un hacker etico che utilizza strumenti di difesa e di monitoraggio che, in alcuni casi, possono essere gli stessi utilizzati dagli hacker malevoli. Ciò che li distingue è la finalità che, nel nostro caso, è la difesa dagli attacchi. Tuttavia, occorre tenere presente che l'uso di strumenti come **Nmap** per accedere senza autorizzazione ai sistemi non è consentito dalla legge. Pertanto, prima di intervenire sui sistemi, è necessario ottenere le autorizzazioni necessarie ed esplicitare quello che intendiamo fare. Noi utilizzeremo dei server di prova dedicati appositamente al test (sandbox).

Consegna

Nmap, o meglio **Zenmap**, che è la sua interfaccia grafica, è lo strumento che utilizzeremo in questa esercitazione per determinare lo stato della rete. Faremo inviare a Nmap una serie di pacchetti ai sistemi che vogliamo analizzare per provocare una risposta. Ad esempio, faremo richieste con il protocollo ICMP, invieremo pacchetti-sonda (Figura 1) sulle porte che utilizzano i protocolli TCP e UDP, ed effettueremo una scansione ARP. Utilizzeremo alcuni dei comandi di Nmap elencati di seguito.

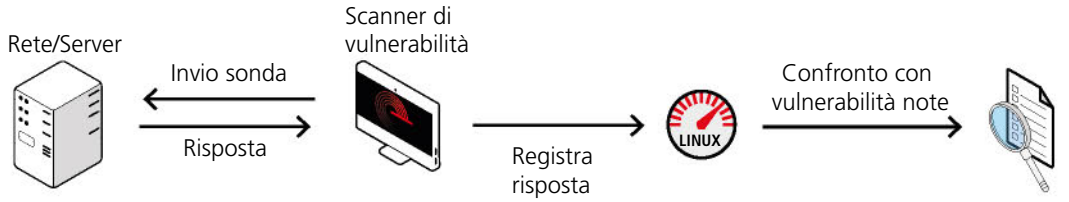


Fig. 1 Invio di pacchetti sonda, risposte, registrazione dei risultati, ricerca nel DB delle vulnerabilità.

Rete di prova 192.168.1.0/24

- **Richiesta echo ICMP**
- **Host e reti**
  - Scansione di più host contemporaneamente:
    `nmap 192.168.1.1 192.168.1.2 192.168.1.3`
  - Scansione di un'intera subnet:
    `nmap 192.168.1.0/24` (`nmap -vv rete/netmask`)
  - Esclusione di host durante la scansione:
    `nmap 192.168.1.0/24 --exclude 192.168.1.5`
  - Scansione di un intervallo di indirizzi IP: `nmap 192.168.1.1-254`
  - Scansione di un dominio: `nmap scanme.nmap.org`
  - Esclusione di host elencati durante la scansione: `nmap -exclude 192.168.1.1`
  - Scansione di host senza scoperta di host (utile se l'host non risponde ai ping):
    `nmap -Pn 192.168.1.1`
- **Scansione porte**
  - Scansione di porte specifiche: `nmap -p 80,443 192.168.1.1`
    (pacchetto TCP SYN inviato alla porta 443)
  - Scansione di un intervallo di porte: `nmap -p 1-100 192.168.1.1`
  - Scansione di tutte le porte: `nmap -p- 192.168.1.1`
  - Scansione di porte multiple (T = TCP, U = UDP):
    `nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.1`

notabene

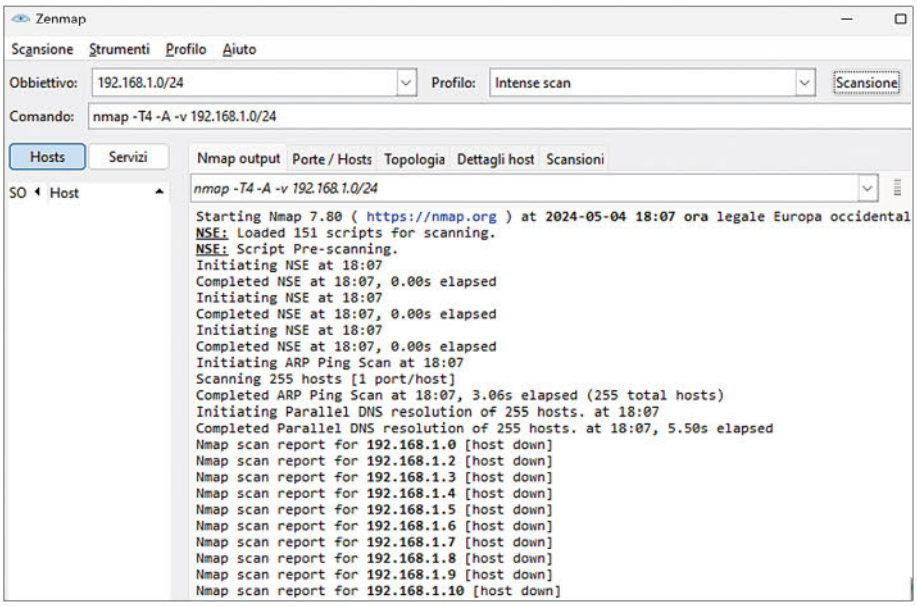
L'invio di un pacchetto TCP ACK alla porta 80 non è conforme alle regole dello standard TCP. Nmap lo fa specificatamente per provare a far sì che il sistema di destinazione fornisca una risposta.

- **Livello di tempo di scansione**: `nmap -T<0-5>`. Il valore numerico può variare da 0 a 5, dove 0 è il più lento e 5 è il più veloce. Ad esempio: `nmap -T0`: scansione molto lenta. `nmap -T5`: scansione estremamente veloce. Un valore più alto aumenta la velocità, ma potrebbe essere meno accurato. Al contrario, un valore più basso rallenta la scansione, ma fornisce risultati più affidabili.
  - **Versione dell'applicazione** in ascolto dietro una porta: `nmap -sV <target>`
  - **Scanner degli script**: `nmap -sC <target>`
  - **Rilevamento del sistema operativo**: `nmap -O <target>`
  - **Scansione indirizzi IPv6**: `nmap -6 <target>`

Svolgimento

Passo 1: sonda la rete locale

`nmap -T4 -A -v`: comando che esegue una scansione veloce (T4) sulla rete `192.168.1.0/24` con opzione aggressiva (`-A`): fornisce la versione del sistema operativo, scandisce gli script, fa il traceroute e produce un output dettagliato (`v`).



notabene

La modalità "aggressiva" (`-A`) di Nmap abilita più flag contemporaneamente. Lo scanner eseguirà il rilevamento della versione e del sistema operativo, abiliterà lo scanner degli script ed effettuerà la scansione delle 1000 porte più comuni `nmap -A <target>`.
Per il manuale di Nmap consultare il sito ufficiale `https://nmap.org/man/it/index.html` con i numerosi esempi.

Passo 2: registra la risposta

Alcune osservazioni:

- NSE: Loaded 151 scripts for scanning.
- Initiating ARP Ping Scan at 18:07
- Initiating Parallel DNS resolution of 255 hosts. at 18:07
- Nmap scan report for 192.168.1.0 [host down]
- Initiating SYN Stealth Scan at 18:07 ... Scanning 11 hosts [1000 ports/host] ...
  ... Discovered open port 443/tcp on 192.168.1.243

Passo 3: sonda un server in Internet

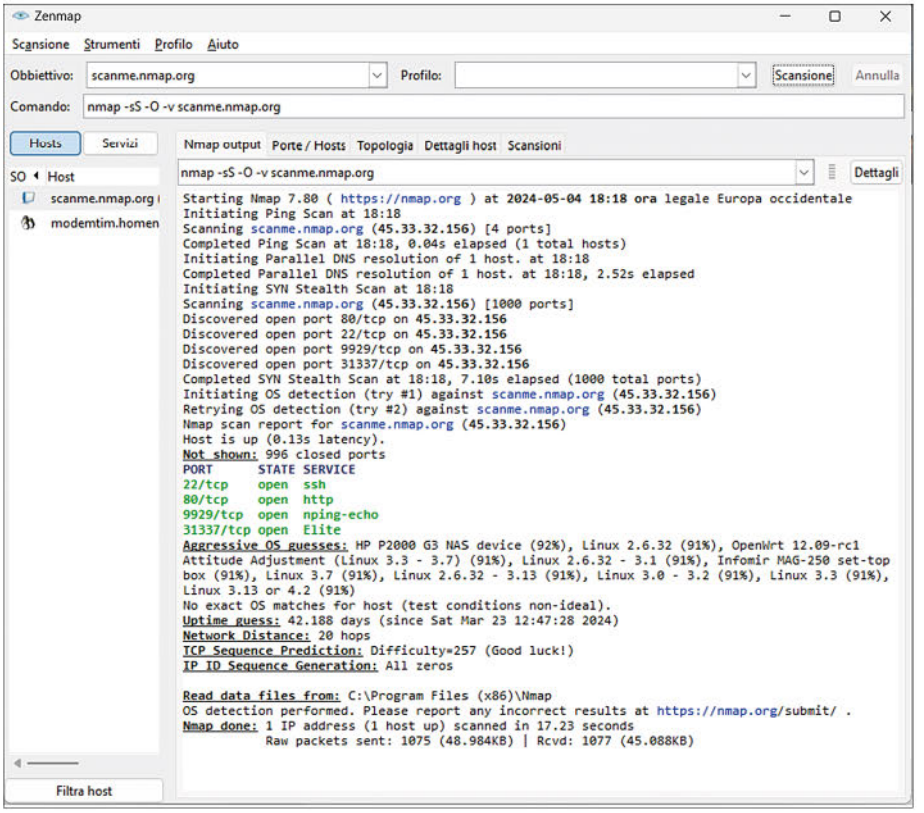
Per fare un esempio concreto, basiamoci su una scena del famoso film *Matrix Reloaded* e precisamente ci riferiamo alla scena in cui Trinity, una hacker molto abile, utilizza Nmap per trovare una porta aperta nel sistema, attraverso la quale infiltrarsi e sfruttare la vulnerabilità associata per guadagnare l'accesso non autorizzato utilizzando il seguente comando:

```
nmap -v -sS -O 10.2.2.2
```

che esegue una scansione SYN con opzioni di rilevamento del sistema operativo:

- `v`: output dettagliato della scansione.
- `sS`: scansione SYN-half-open, che invia pacchetti SYN senza completare la connessione TCP per determinare quali porte sono aperte.
- `O`: Tentativo di rilevare il sistema operativo dell'host di destinazione.

Proviamo a simulare il comando di Matrix utilizzando il server (`scanme.nmap.org`) che Nmap mette a disposizione per le prove in Internet:



notabene

È importante sottolineare che l'uso di strumenti come Nmap per accedere illegalmente ai sistemi è un reato, punito ai sensi dall'articolo 615 del Codice Penale.

ARTICOLO 615 ter, Codice Penale
Sezione IV – Dei delitti contro la inviolabilità del domicilio

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

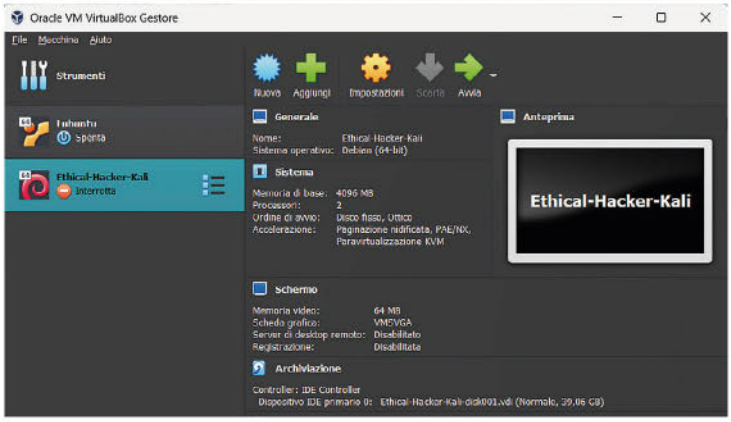
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Notiamo, in particolare, la risposta *Aggressive OS guesses*: In base a come il server ha risposto a una serie di sonde inviate da Nmap si ricava che:

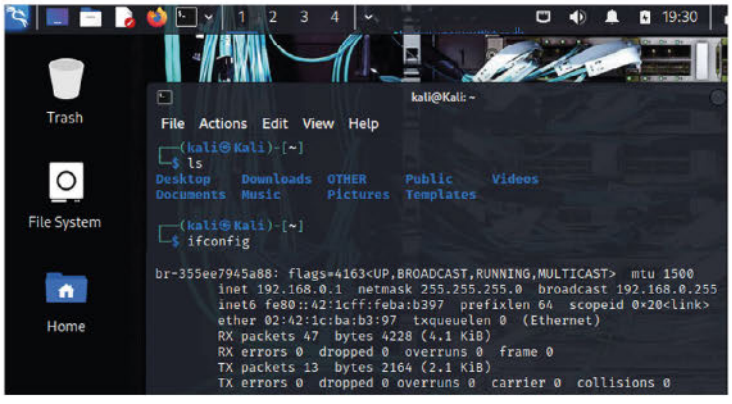
- "HP P2000 G3 NAS device (92%)": c'è il 92% di probabilità che il dispositivo sia un dispositivo di archiviazione di rete HP P2000 G3.
- "Linux 2.6.32 (91%)": c'è il 91% di probabilità che il server stia eseguendo la versione del kernel Linux 2.6.32.
- "No exact OS matches for host (test conditions non-ideal)": Nmap non ha trovato una corrispondenza esatta per il sistema operativo del server, probabilmente per le limitazioni di un firewall, o della configurazione di rete.

Passo 4: utilizzo di Nmap in Kali Linux

Kali Linux è un sistema operativo open-source basato su Debian. Progettato per test di sicurezza, fornisce centinaia di strumenti specifici per il penetration testing. Ci sono diverse modalità di installazione di Kali, tra cui quella di scaricare l'immagine ISO e installarla su una macchina virtuale in VirtualBox (Figura 2 e Figura 3).



➜ Fig. 2



➜ Fig. 3

- Rilevazione del sistema operativo e porte del server Nmap (`scanme.nmap.org`)

```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -v -sS -O scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-04 20:17 UTC
Initiating Ping Scan at 20:17
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 20:17, 0.02s elapsed (1 total hosts)
```

```
Initiating Parallel DNS resolution of 1 host. at 20:17
Completed Parallel DNS resolution of 1 host. at 20:17, 0.02s elapsed
Initiating SYN Stealth Scan at 20:17
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
…
```

- Scansione per valutare la sicurezza dell'host all'indirizzo `192.168.0.1` e identificare potenziali punti deboli:

```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -sV -script vulners --script-args mincvss=4 192.168.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-04 20:37 UTC
Nmap scan report for 192.168.0.1
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p2 Debian 1 (protocol 2.0)
| vulners:
|  cpe:/a:openbsd:openssh:9.3p2:
|    SSV:92579 7.5 https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|    PRION:CVE-2023-38408      7.5      https://vulners.com/prion/PRION:CVE-2023-38408
…
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Parametri di `nmap` utilizzati (il comando `sudo`: segue il comando successivo con i privilegi di superuser):

- `-sV`: scansione delle versioni dei servizi, per determinare quali versioni di servizi sono in esecuzione sugli host aperti;
- `--script vulners`: utilizza lo script `vulners` che confronta le versioni dei servizi rilevati con un database di vulnerabilità note;
- `--script-args mincvss=4`: rileva solo le vulnerabilità con un punteggio CVSS di minimo 4.

L'host in esame è afflitto da una vulnerabilità (CVE-2023-38408) grave (CVSS di 9.8) che colpisce una funzione per la gestione remota in `ssh-agent` di OpenSSH nelle versioni precedenti alla 9.3p2. Se sfruttata permette a un attaccante di eseguire codice arbitrario sul sistema attaccato. Per mitigare questa vulnerabilità va aggiornato il software di OpenSSH alla versione successiva a 9.3p2.

notabene

OpenSSH è un'applicazione che fornisce diverse funzionalità per l'accesso remoto sicuro con il protocollo SSH-2, come ad esempio l'esecuzione di comandi e la copia di file

Passo 5: YARA

YARA (*Yet Another Recursive Acronym*, `https://yara.readthedocs.io/`) è un importante strumento, distribuito anche all'interno di Kali Linux, che permette di cercare sequenze di codice dannoso (pattern malevoli) all'interno di file sospetti. Con YARA possiamo definire delle regole personalizzate ("YARA rules") che identificano queste sequenze. Ad esempio, possiamo cercare URL del tipo `dominiomalevolo.com`, o parole chiave che identificano delle richieste di denaro ("pay", "money") o sequenze di numeri di una firma (`{ 25 55 54 46 }`). Una panoramica delle potenzialità di YARA è mostrata nell'esempio seguente per la ricerca, all'interno di un file o di un flusso di dati, della stringa «malware» o dell'indirizzo `192.168.1.1`. La ricerca dell'indirizzo IP, nel formato decimale puntato, non sempre è efficace, poiché gli indirizzi nei file binari potrebbero essere rappresentati in un formato diverso (ad esempio, in esadecimale). Trasformiamo perciò l'indirizzo `192.168.1.1` nel formato esadecimale `C0 A8 01 01` e scriviamo il codice:

```
rule detect _ multiple _ conditions {
    strings:
        $malware _ str = "malware"  // Cerca la parola "malware"
        $ip _ address _ hex = { C0 A8 01 01 }
    condition:
        $malware _ str or $ip _ address _ hex // Rileva la presenza
                                              // della stringa
                                              // "malware" o
                                              // dell'indirizzo IP
}
```

ATTIVITÀ 6

Convalida dell'input e SQL Injection

Disponibile nell'eBook.

SINTESI

SICUREZZA INFORMATICA
Riguarda i processi e le tecniche utilizzate per proteggere le reti, i sistemi e i programmi dagli attacchi digitali.

C.I.A.
Obiettivi della sicurezza sono:
- C – **Confidentiality** (Riservatezza)
- I – **Integrity** (Integrità)
- A – **Availability** (Disponibilità)

C – Confidentiality (Riservatezza): i dati devono essere accessibili solo a chi ha l'autorizzazione.

I – Integrity (Integrità): i dati non devono essere modificati e devono rappresentare la realtà per condurre a informazioni certe.

A – Availability (Disponibilità): i dati devono sempre essere disponibili e in un formato leggibile.

DIFESA E GESTIONE DEGLI ATTACCHI
Sulle tecniche di difesa e di gestione degli attacchi, Il Cybersecurity Framework (CSF) 2.0 del NIST offre delle linee guida che comprendono:
- l'analisi degli attacchi;
- le procedure per la preparazione e la risposta a situazioni critiche;
- il ripristino della normalità.

TECNICHE DI DIFESA
Richiedono un notevole impegno in termini di tempo e costi; non sempre sono sostenibili e riguardano, per esempio, la progettazione della rete:
- organizzare la propria rete con firewall, server AAA, DMZ;
- variare la topologia della rete e dei dispositivi per rendere difficile il lavoro di ricognizione dell'attaccante;
- predisporre delle trappole.

GESTIONE DI UN ATTACCO
Utilizzo del modello "Incident Response LifeCycle" proposto dal NIST. Si articola nelle seguenti fasi:
- Preparazione (governo, identificazione, protezione);
- Risposta agli incidenti (rilevamento, risposta);
- Recupero (recupero dei dati, analisi post incidente).

VULNERABILITÀ – MINACCE – ATTACCHI

- **Vulnerabilità**: è una debolezza specifica in un sistema informatico che può essere sfruttata per compromettere la sicurezza del sistema.
- **Minaccia**: evento esterno che tende a violare uno o più obiettivi di sicurezza.
- **Attacco**: atto volontario che sfrutta una minaccia per compromettere un sistema.

ATTACCHI E ATTACCANTI

L'attacco informatico è un processo che si articola in varie fasi.
Gli attaccanti sono chiamati *hacker*.
Ci sono diversi tipi di hacker:

- **white hat**: operano nell'interesse pubblico;
- **black hat**: agiscono con intenzioni criminali, violando i sistemi per rubare dati;
- **grey hat**: possono oscillare tra la legalità e l'illegalità, a seconda delle circostanze.

CYBER KILL CHAIN

È un modello che descrive le fasi in cui si articola un attacco:

- Ricognizione
- Armamento
- Distribuzione
- Sfruttamento
- Installazione
- Controllo
- Azioni sui bersagli ed esfiltrazione

MINACCE

Minacce più comuni:

- **Malware**: software malevoli, come virus e worm, trojan e backdoor, ransomware, spyware, rootkit, adware;
- **Social Engineering**: capacità di spacciarsi per quello che non si è;
- **APT**: tecniche di hacking sofisticate per il sabotaggio e lo spionaggio;
- **SYN Flood**: sovraccarica di richieste SYN il server, fino a farlo collassare;
- **Spoofing IP**: Inganna il sistema facendo credere che il traffico provenga da una fonte fidata. Altera l'indirizzo IP sorgente nei pacchetti di rete;
- **Man in the Middle** (**MitM**): gli hacker si inseriscono in una comunicazione fra due parti;
- **Teardrop**: vengono inviati frammenti parziali di pacchetti IP che il sistema di destinazione non riesce a riassemblare;
- **Botnet**: rete di dispositivi infettati da software malevolo;
- **DDoS**: sovraccarico di richieste a un server.

VULNERABILITÀ

Sono classificate nello standard CVE. Possono essere:

- **intrinseche**: sfruttano la natura aperta della rete e degli elementi che ne fanno parte;
- **tecnologiche**: problemi relativi ad Hardware e software;
- **umane**: legate all'imprevedibilità del comportamento umano.

Verifica delle CONOSCENZE

Vero o Falso?

1 Obiettivo della sicurezza informatica è rendere inattaccabile un sistema. V F

2 Integrità dei dati significa che i dati non sono modificati e sono significativi. V F

3 Per rendere sicuri i dati basta crittografarli. V F

4 I keylogger sono programmi malevoli che comprendono svariate funzioni pericolose. V F

5 L'ingegneria sociale è la capacità di spacciarsi per quello che non si è. V F

6 Un hacker è sempre un delinquente che tenta di rubare informazioni. V F

7 Zero-day exploit è un attacco veloce. V F

8 Man in the Middle è un tipo di attacco basato sullo spionaggio. V F

9 APT è un tipo di attacco mirato il cui scopo è introdursi nei sistemi per rubare i dati. V F

10 La confidenzialità permette di comunicare le password in modo sicuro. V F

11 Un attacco SYN Flood modifica le intestazioni di IP e TCP. V F

12 Una minaccia è un evento dannoso che potrebbe accadere. V F

13 Il backup di un database è un esempio di politica di sicurezza. V F

14 ISO 27001: è uno standard che definisce le linee guida per la gestione del sistema di sicurezza. V F

15 SIEM, SOC, CERT sono elementi per la difesa di un sistema informatico. V F

16 Incident Response LifeCycle è una vulnerabilità hardware di un sistema informatico. V F

17 Ricognizione e Armamento sono due fasi in cui si articola un attacco informatico. V F

18 Una minaccia è un evento esterno che tende a violare uno o più obiettivi di sicurezza. V F

19 Confidentiality significa che i dati devono essere accessibili solo a chi ha l'autorizzazione. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

20 Errori o guasti sulla rete e sull'hardware possono avere impatto:

a su riservatezza, integrità e disponibilità dei dati
b solo sulla disponibilità dei dati
c solo sull'hardware
d Non hanno conseguenze perché ci sono le copie di backup

21 Denial of Service:

a è una minaccia all'integrità dei dati
b è un attacco di tipo attivo
c è il miglior modo per difendersi
d si mette in atto per chiudere un sistema insicuro

22 L'attività di recovery serve per:

a recuperare gli errori
b ripristinare le normali attività del sistema
c definire una politica di sicurezza
d fare una copia di sicurezza dei dati

23 La Cyber Kill Chain

a è un modello che descrive le fasi in cui si articola la difesa da attacco informatico
b è una minaccia ad un sistema informatico
c è un modello che descrive le fasi in cui si articola un attacco informatico
d È un malware

24 Relativamente ad un malware, il vettore

a è il mezzo attraverso il quale il malware si diffonde
b contiene le istruzioni che il malware deve eseguire
c è il computer a cui è destinato l'attacco
d è una backdoor

Domande per la prova orale

25 Esponi le principali tipologie di attacchi in rete.

26 Esponi il significato di attacco APT e le fasi in cui si articola il ciclo di vita.

27 Fai degli esempi di politiche di sicurezza.

28 Descrivi le fasi in cui si articola un attacco informatico.

29 Descrivi le fasi del modello Incident Response LifeCycle

30 Quali sono i principali compiti del "difensore" di un sistema informatico?

31 Come possono essere classificati gli hacker?

Verifica delle ABILITÀ

32 Esponi la differenza tra dato e informazione. Fornisci anche un esempio.

33 Completa la tabella

	Significato	Possibile minaccia
Confidentiality	.....	.....
Integrity	.....	.....
Availability	.....	.....

34 Completa la tabella

	Significato	Possibile minaccia
Vulnerabilità	.....	.....
Minaccia	.....	.....
Attacco	.....	.....

Esercizi in più

Computer system security

Abstract

The security of a computer system within a company is extremely important and has a significant impact on our daily lives.
Though absolute security is unattainable, as the probability that a harmful event will occur is always there, the aim of a security process is to minimize this probability, i.e. to reduce the risk of such an event happening. Of course, prevention costs and recovery costs must be balanced, also taking into account damage to the customers and to the company's image. Attacks can be of various types and are more likely to occur if LAN or WAN are being used. Particular relevance in this context is given to the protection of data, to which confidentiality, integrity and availability must be guaranteed.

Questions

Answer all questions

1 What is the difference between threat and cyber attack?

2 What are the goals of data security?

3 What is an APT?

4 What is the Cyber Kill Chain?

Choose the correct answer

5 The acronym CIA is used:
- a to identify special espionage attacks
- b as part of data security
- c to indicate a particular cyber attack
- d to indicate a network virus

6 By DoS we mean:
- a a threat due to human negligence
- b a malware
- c an attack that makes a service unavailable
- d an Internet security service

7 By data integrity we mean that the data:
- a are available
- b are unmodified, usable and reliable
- c are not partial
- d are protected

8 SQL injection:
- a is a vulnerable Internet service
- b is an application layer attack
- c is an APT
- d is a DoS

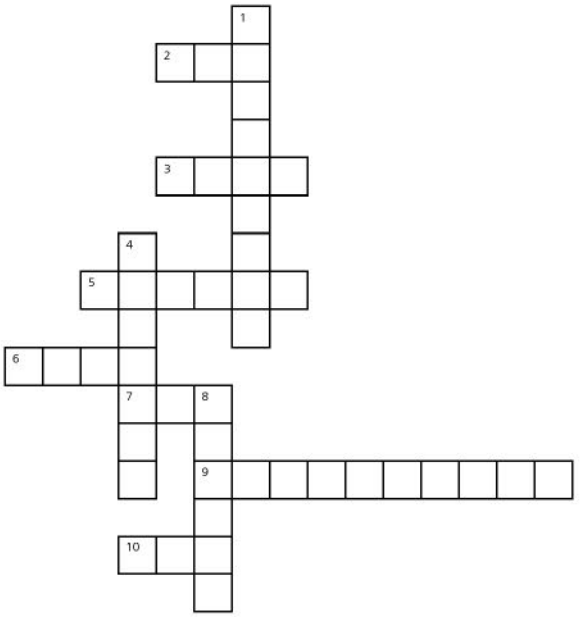
Crosswords

Across

2 Classification of vulnerabilities
3 Attack attempting to disable a server
5 Entity launching an attack
6 Model linking data to knowledge
7 Sophisticated hacking techniques
9 Act of extortion requiring a ransom
10 Goals of cybersecurity

Down

1 They record what is typed on the keyboard
4 Malicious software
8 Event intending to violate a security target

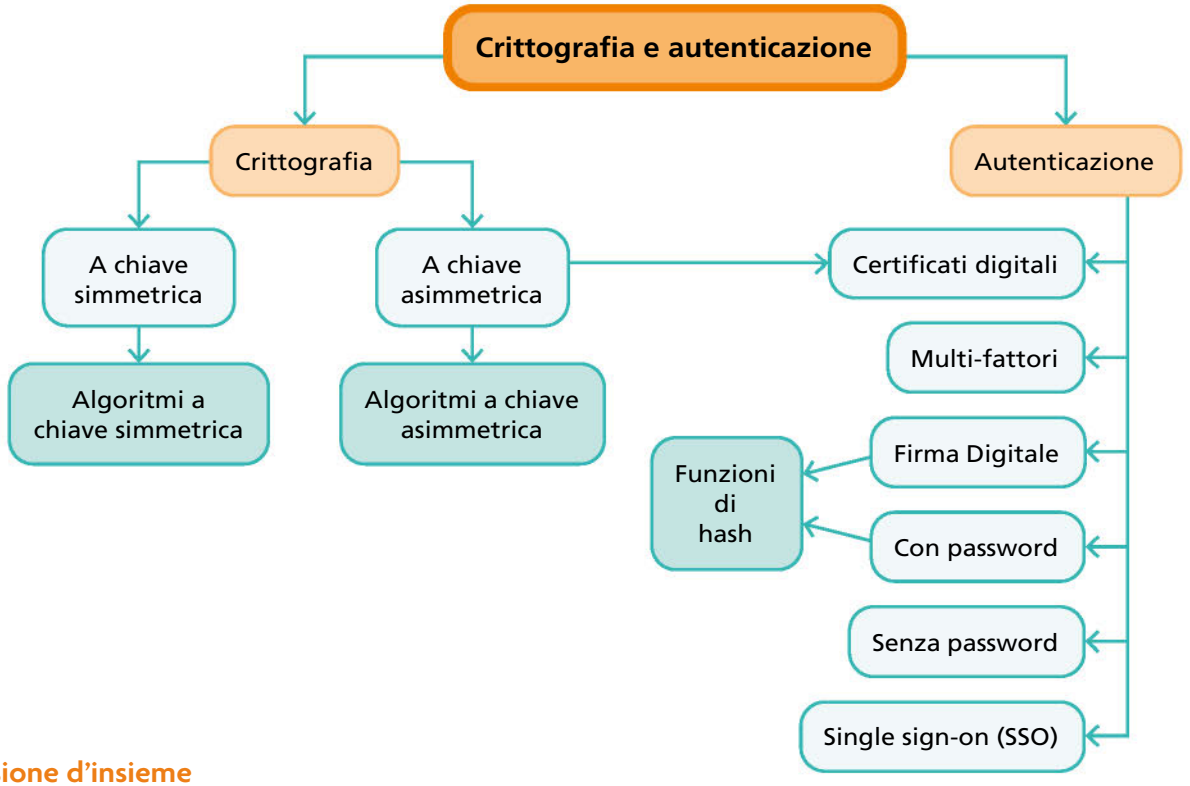




Unità

4

Crittografia e autenticazione



Visione d'insieme

- Metodi per garantire la riservatezza e l'integrità dei dati.
- Crittografia a chiave simmetrica e a chiave asimmetrica (algoritmo RSA).
- Metodi di autenticazione: a più fattori, con e senza password, Firma Digitale.

1 Introduzione

Nel romanzo di Ken Follet *Il codice Rebecca*, ambientato durante la Seconda guerra mondiale, la spia tedesca Alex Wolff deve inviare un messaggio cifrato al comando delle truppe tedesche in Nord Africa. Per mettere in cifra la frase "ARRIVATO. LAVORO AVVIATO. ATTENDO RISPOSTA", Wolff apre una copia del romanzo *Rebecca* di Daphne di Maurier alla pagina 70 (un numero ottenuto sommando l'anno, quarantadue, al giorno del mese, il ventotto di maggio). Poiché maggio è il quinto mese dell'anno, Wolff conta le lettere dalla prima riga, saltando una lettera ogni cinque, fino a incontrare una "A". Contando in questo modo, la prima "A" è la decima lettera della riga. Nel codice con cui sarebbe stato crittato il messaggio, la "A" sarebbe quindi stata rappresentata dalla decima lettera dell'alfabeto, la "R". La lettera successiva del messaggio, una "R", è la numero tre dopo la "A": nel codice sarebbe diventata una "C", la terza lettera dell'alfabeto. Wolff sa che il metodo di crittazione che utilizza, un variante del metodo della griglia, è indecifrabile, a meno che il destinatario del messaggio crittato non possieda sia la chiave utilizzata sia una copia dello stesso libro usato per la codifica.
Il personaggio di KF utilizza un algoritmo di crittografia simmetrica usato durante la Seconda guerra mondiale per trasmettere messaggi segreti. Tuttavia, la sicurezza di questo metodo dipende dal mantenimento del segreto sia del libro sia della regola. Come stabilito dal linguista e crittografo olandese Auguste Kerckhoffs (1835-1903) un sistema di crittografia è invece considerato sicuro solo se è inviolabile anche se l'avversario conosce l'algoritmo di cifratura, purché la chiave rimanga segreta.

2 La crittografia

notabene

Il termine "crittografia" deriva dal greco kryptós, che significa "nascosto", e graphía, che significa "scrittura".

La crittografia è una tecnica utilizzata per garantire, innanzitutto, la **riservatezza** dei dati (*Confidentiality*), sia durante la loro trasmissione, sia quando sono salvati su memoria di massa.
Crittografare un messaggio (o dei dati) significa codificarlo utilizzando un algoritmo e una chiave. **L'algoritmo è pubblico e noto a chiunque, ma solo chi conosce la chiave è in grado di decodificare il messaggio**. Il messaggio criptato, quindi, può essere intercettato o accessibile a chiunque, ma solo le persone (o le applicazioni) autorizzate, in possesso della chiave, saranno in grado di comprenderne il significato. Il messaggio originale è detto "messaggio in chiaro", il messaggio codificato è detto "messaggio criptato".
Per comprendere il problema, vediamo uno dei più semplici algoritmi di crittografia: l'**algoritmo a trasposizione**, in cui ogni lettera di un messaggio è sostituita con un'altra lettera che nell'alfabeto è k posti avanti. In questo caso, "k" costituisce la chiave.
Per esempio, utilizzando l'algoritmo a trasposizione con chiave 3, ogni lettera del messaggio è sostituita dalla lettera che nell'alfabeto è 3 posti avanti.

Esempio 1

messaggio in chiaro: `CIAO`
messaggio criptato (con chiave = 3): `FNDR`
Evidenziamo che l'algoritmo è noto, ma la chiave è segreta. Solo conoscendo la chiave si è in grado di decriptare il messaggio. Questo algoritmo, noto come Cifrario di Cesare, è ovviamente molto semplice e anche se non è nota la chiave, non è particolarmente difficile risalire a essa e decodificare il messaggio.

Pit Stop

1. Cosa significa crittografare un messaggio?
2. Che cos'è l'algoritmo a trasposizione?

I moderni algoritmi di crittografia si suddividono in due categorie:

- algoritmi a chiave **simmetrica**;
- algoritmi a chiave **asimmetrica**.

Crittografia simmetrica

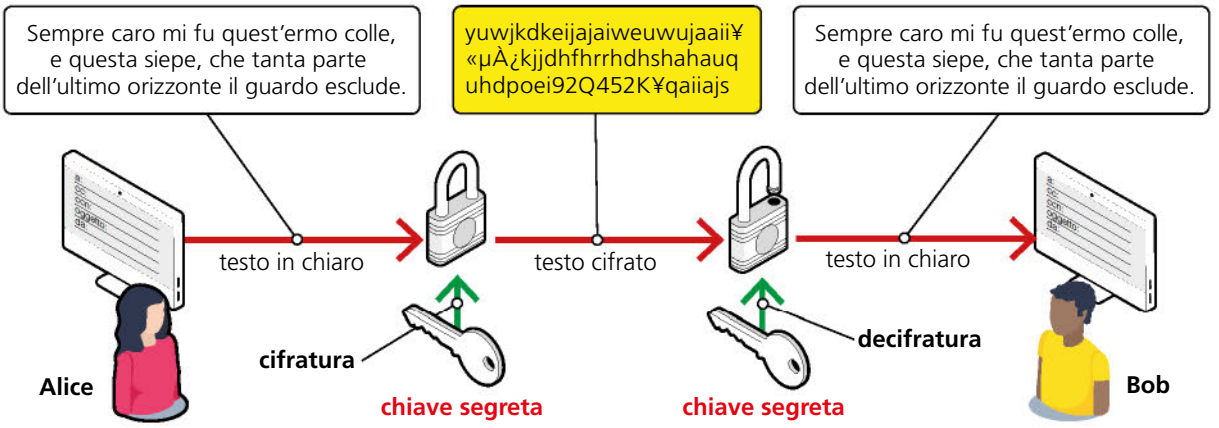
Gli algoritmi a chiave simmetrica utilizzano la stessa chiave per criptare e per decriptare il messaggio.

$$D_k(C_k(m)) = m$$

Dato un messaggio m, questo viene crittografato (C), usando un algoritmo con una chiave k, ottenendo il messaggio crittografato $C_k(m)$ che poi è decriptato (D) usando lo stesso algoritmo con la stessa chiave k, ottenendo il messaggio originale.
Supponiamo che Alice debba inviare un messaggio segreto a Bob (Figura 1):

- Alice cifra il messaggio utilizzando una chiave segreta.
- Alice invia il messaggio cifrato a Bob.
- Bob riceve il messaggio cifrato.
- Bob decripta il messaggio utilizzando la stessa chiave usata da Alice, e ottiene il messaggio originale.

Fig. 1



La criticità degli algoritmi a chiave simmetrica consiste nello **scambio della chiave** tra gli interlocutori senza che questa venga intercettata. La crittografia, infatti, è usata proprio per inviare dati in rete senza che questi possano essere intercettati, ma se la decifratura richiede l'invio della chiave, il problema della trasmissione di dati sicuri si ripropone relativamente alla chiave.

Algoritmi di crittografia a chiave simmetrica

Un messaggio può essere cifrato con chiave simmetrica in due modi:

- **Cifratura a flusso** (*Stream Ciphers*): ogni bit o byte del messaggio in chiaro è cifrato. Questo metodo è utile quando non si conosce la quantità di dati da inviare, è molto veloce e può essere cablato nel firmware. Però è difficile da implementare ed è poco usato.
- **Cifratura a blocco** (*Block Ciphers*): opera su un blocco di dati alla volta. Questo metodo è più lento, ma è utile quando si conosce in anticipo la quantità di dati da inviare.

Pit Stop

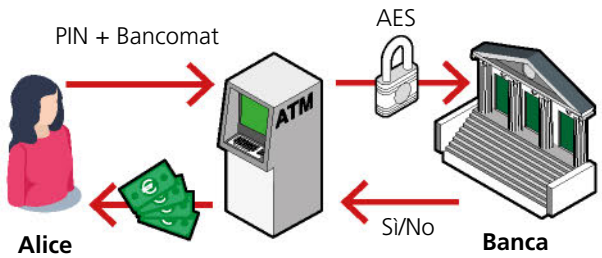
3 Che cosa significa "chiave simmetrica"?

4 Quali sono i metodi di cifratura a chiave simmetrica?

Di seguito vediamo alcuni algoritmi a chiave simmetrica tra i più noti.

- **DES** (**D***ata* **E***ncryption* **S***tandard*): è uno dei primi algoritmi diffusi. Utilizza una chiave a 64 bit (di cui 8 sono di controllo). Suddivide il messaggio in blocchi di 64 bit e cifra ogni blocco, ottenendo un altro blocco di 64 bit. È considerato poco sicuro.
- **3DES** (*Triple DES*): proposto per risolvere le criticità di DES, utilizza tre chiavi e tre successive esecuzioni di DES. La lunghezza effettiva della chiave è di 168 bit (3 × 56). Opera in modalità "Cipher block chaining" (cifratura a blocchi concatenati), effettuando una serie di XOR logici tra l'ultimo blocco di testo e il precedente cifrato.
- **AES** (**A***dvanced* **E***ncryption* **S***tandard*, o *algoritmo di Rijndael*): Nel 2001 è stato scelto dal NIST come sostituto di 3DES per la sua efficienza e sicurezza. Opera con blocchi a 128 bit e chiavi a 128, 192 e 256 bit.

Da evidenziare che la sicurezza degli algoritmi è legata alla **lunghezza della chiave** perché una chiave troppo corta può essere più facilmente trovata con un attacco a forza bruta.
Un esempio di applicazione di algoritmo di cifratura a chiave simmetrica è costituito dai Bancomat o ATM, che utilizzano il protocollo di crittografia 3DES. Tuttavia, a causa delle vulnerabilità scoperte nel 3DES, molti ATM stanno passando all'uso del protocollo AES (Figura 2).



➜ **Fig. 2** Prelievo allo sportello ATM (Automated Teller Machine), o Bancomat, che usa crittografia AES.

Crittografia asimmetrica

Il problema dello scambio delle chiavi su un canale che per sua natura non è sicuro è stato affrontato intorno alla metà del secolo scorso; il 1976 è stato un anno importante nella storia della crittografia moderna, perché ha visto l'introduzione, da parte di Diffie e Hellman, della crittografia asimmetrica a chiave pubblica, che ha avuto un impatto enorme e ha cambiato radicalmente il modo di comunicare in sicurezza.
Gli algoritmi a chiave pubblica sono tali per cui le chiavi usate per cifrare e decifrare il messaggio sono diverse. Ogni utente ha una **coppia di chiavi**: una **Chiave pubblica** che può e deve essere diffusa, e una **Chiave privata**.
La coppia di chiavi è calcolata con un opportuno algoritmo e il fondamento della sicurezza del metodo è che sia difficilissimo ricavare la chiave privata dalla chiave pubblica.
Per garantire la segretezza del messaggio:

- il mittente cripta il messaggio con la chiave pubblica (nota) del destinatario (*kpubdest*);
- il destinatario decripta con la propria chiave privata (segreta) (*kprdest*).

$$D_{kprdest}(C_{kpubdest}(m)) = m$$

Pit Stop

5 Cosa determina la lunghezza di una chiave di cifratura?

6 Qual è la caratteristica di un algoritmo di crifratura a chiave pubblica?

Chiunque potrebbe intercettare il messaggio, ma solo il destinatario, utilizzando la chiave privata associata alla chiave pubblica usata per criptarlo, sarà in grado di comprenderne il significato.
Gli algoritmi sono pubblici. Si noti che ogni chiave privata è associata a una determinata chiave pubblica, per cui solo chi è in possesso della chiave privata è in grado di comprendere un messaggio crittografato con la chiave pubblica associata.
Supponiamo che Alice debba inviare un messaggio segreto a Bob (**Figura 3**):

- Alice cifra il messaggio utilizzando la chiave pubblica di Bob.
- Alice invia il messaggio cifrato a Bob.
- Bob riceve il messaggio cifrato.
- Bob decripta il messaggio utilizzando la sua chiave privata, e ottiene il messaggio originale.

Pit Stop

7 Qual è l'algoritmo a chiave asimmetrica più diffuso?

8 Su quale teoria matematica si basa?

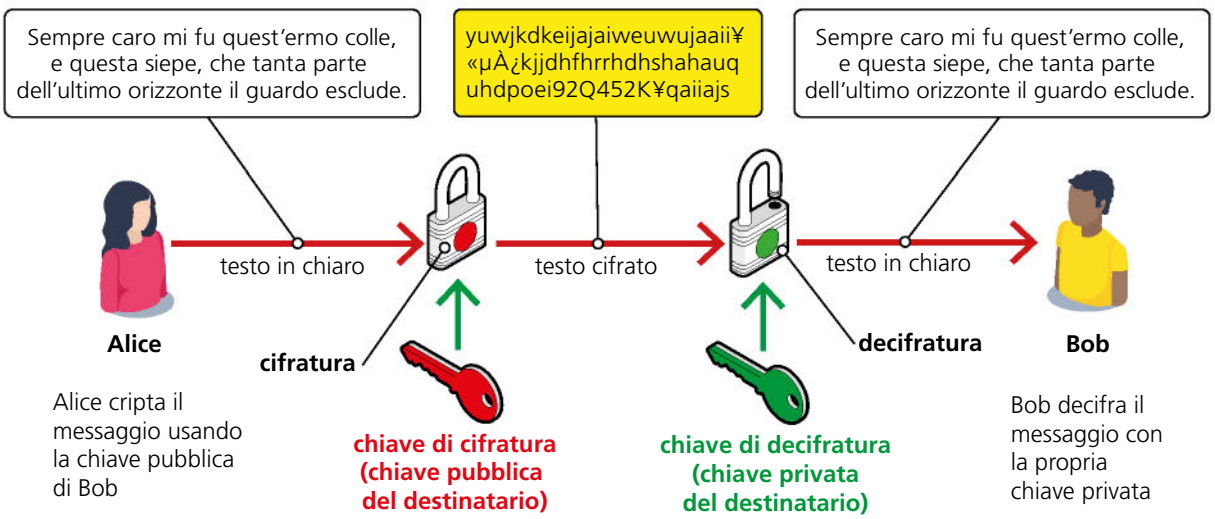


Fig. 3 Algoritmo di crittografia a chiave asimmetrica.

Rispetto agli algoritmi a chiave simmetrica, gli algoritmi a chiave asimmetrica sono molto più complessi e onerosi, e richiedono più risorse di calcolo per essere processati. È per questo motivo che molte applicazioni utilizzano un algoritmo a chiave pubblica per scambiare una chiave simmetrica segreta da utilizzare durante la sessione (**chiave di sessione**). In questo modo si ha l'ulteriore vantaggio che la chiave cambia a ogni sessione.

L'algoritmo a chiave asimmetrica RSA

RSA è l'algoritmo a chiave asimmetrica più diffuso. Prende il nome dalle iniziali dei suoi inventori, Rivest, Shamir e Adleman, ed è fondato su alcune proprietà dei numeri primi, in particolare sulla scomposizione di un numero in fattori primi. Questo algoritmo ha la caratteristica di usare una coppia di chiavi correlate, una privata e una pubblica, generate in modo tale che sia impossibile ricavare una chiave dall'altra. La chiave pubblica è distribuita a chiunque ne sia interessato. Quella privata è posseduta solo dal proprietario delle chiavi. Chiunque voglia comunicare in modo sicuro e garantire la segretezza del messaggio deve cifrare il messaggio con la chiave pubblica del destinatario il quale, una volta ricevuto il messaggio cifrato, applicando la propria chiave privata sarà in grado di decifrarlo. Di seguito presentiamo i passi elementari dell'algoritmo RSA, pubblicato nel 1978 e basato sul teorema di Fermat-Eulero.

Determinazione della chiave pubblica e della chiave privata
Scegliere due numeri p, q primi molto grandi (almeno 300 cifre); la dimensione dei numeri è fondamentale perché l'algoritmo è fondato sul fatto che, una volta moltiplicati tra loro, è praticamente impossibile dal prodotto ricavare i fattori.

- Determinare $n = p \cdot q$
- Determinare $m = (p - 1) \cdot (q - 1)$
- Determinare un numero, e, che sia primo rispetto a m (che cioè non abbia divisori in comune con m).
- Determinare k tale che $[(e \cdot k) \bmod m] = 1$ $\quad k = (m \cdot h + 1)/e$ con h intero positivo.
- La chiave pubblica (kpb) è data dalla coppia (e, n).
- La chiave privata (kpv) è data dalla coppia (k, n).

Cifratura del messaggio
Il messaggio viene cifrato usando la chiave pubblica del destinatario.
Per evitare attacchi basati sull'analisi delle frequenze, il messaggio, convertito in binario, è diviso in blocchi di g bit, con g tale che $2g < m$.
Ogni blocco è cifrato applicando la chiave pubblica. Se M è il blocco di messaggio, il blocco cifrato C è:

$$C = (M_e \bmod n)$$

Decifratura del messaggio
Il messaggio ricevuto viene decifrato dal destinatario applicando la sua chiave privata.
Ogni blocco è decifrato applicando la chiave privata. Se C è il blocco cifrato, il blocco decifrato M è:

$$M = (C_k \bmod n)$$

Esempio 2

Esempio semplificato di applicazione dell'algoritmo RSA
Alice deve inviare a Bob il proprio indirizzo, ma deve fare in modo che Eve (che controlla il canale di comunicazione) non ne venga a conoscenza. A questo proposito Alice e Bob decidono di utilizzare l'algoritmo RSA per proteggere la loro comunicazione.

Mittente: Alice

Destinatario: Bob

1. Generazione delle chiavi
Bob deve generare le chiavi di cifratura (k_{pb}) e decifratura (k_{pr}).
Scegliamo $p = 3$ e $q = 11$ (per semplicità prendiamo dei numeri piccoli)
$n = p \cdot q = 3 \cdot 11 = 33$
$m = (p - 1) \cdot (q - 1) = 2 \cdot 10 = 20$
Determiniamo e primo rispetto a 20. Per esempio $e = 3$
Determiniamo k tale che $[(3 \cdot k) \bmod 20] = 1$, ossia $20 \cdot n + 1 = 3 \cdot k$, cioè $k = (20 \cdot n + 1)/3$, dove n è un qualunque numero intero positivo). Se fissiamo $n = 1$, allora $k = 7$.
La chiave pubblica (k_{pb}) è la coppia (3, 33), la chiave privata (k_{pr}) è la coppia (7, 33).
Bob può distribuire la sua chiave pubblica e tiene la sua chiave privata.

2. Cifratura del messaggio
Alice deve inviare il suo indirizzo a Bob; il messaggio è quindi: «via Roma».
Ogni lettera è tradotta in binario (per esempio in codice ASCII).

v	01110110
i	01101001
a	01100001
	00100000
R	01010010
o	01101111
m	01101101
a	01100001

Messaggio in chiaro:
`01110110011010010110000100100000010100100110111101101101100001`

La sequenza di bit è divisa in blocchi di g bit, in modo che g sia il più grande numero tale che $2^g < 33$; in questo caso $g = 5$.

Divisione in blocchi di 5 bit:
`01110 11001 10100 10110 00010 01000 00010 10010 01101 11101 10110 10110 00001`

L'ultimo blocco è completato con degli zeri (in questo caso `00001`).

Blocco	In decimale	Cifratura del blocco con chiave (3,33)	Blocco cifrato in decimale	Blocco cifrato in binario
01110	14	$(14^3 \bmod 33) = 05$	05	00101
11001	25	$(25^3 \bmod 33) = 16$	16	10000
10100	20	$(20^3 \bmod 33) = 14$	14	01110
10110	22	$(22^3 \bmod 33) = 22$	22	10110
00010	2	$(02^3 \bmod 33) = 08$	8	01000
01000	8	$(08^3 \bmod 33) = 17$	17	10001
00010	2	$(02^3 \bmod 33) = 08$	8	01000
10010	18	$(18^3 \bmod 33) = 24$	24	11000
01101	13	$(13^3 \bmod 33) = 19$	19	10011
11101	29	$(29^3 \bmod 33) = 02$	2	00010
10110	22	$(22^3 \bmod 33) = 22$	22	10110
10110	22	$(22^3 \bmod 33) = 22$	22	10110
00001	1	$(01^3 \bmod 33) = 1$	1	00001

Messaggio cifrato:
`00101100000111010110000101000100010110001001100010101101011000001`

3. Decifratura del messaggio

Blocco cifrato in binario	Blocco cifrato in decimale	Decifratura del blocco con chiave (7, 33)	Blocco decifrato in decimale	Blocco decifrato in binario
00101	5	$(5^7 \bmod 33) = 14$	14	01110
10000	16	$(16^7 \bmod 33) = 25$	25	11001
01110	14	$(14^7 \bmod 33) = 20$	20	10100
10110	22	$(22^7 \bmod 33) = 22$	22	10110
10000	8	$(8^7 \bmod 33) = 2$	2	00010
10001	17	$(17^7 \bmod 33) = 8$	8	01000
10000	8	$(8^7 \bmod 33) = 2$	2	00010
11000	24	$(24^7 \bmod 33) = 18$	18	10010
10011	19	$(19^7 \bmod 33) = 13$	13	01101
00010	2	$(2^7 \bmod 33) = 29$	29	11101
10110	22	$(22^7 \bmod 33) = 22$	22	10110
10110	22	$(22^7 \bmod 33) = 22$	22	10110
00001	1	$(1^7 \bmod 33) = 1$	1	00001

Blocco decifrato (messaggio originale):

01110110	01101001	01100001	00100000	01010010	01101111	01101101	01100001
v	i	a		R	o	m	a

3 L'autenticazione

Tra le misure utili a garantire la riservatezza dei dati (*Confidentiality*), è necessario utilizzare dei metodi di **identificazione** di un soggetto che vuole entrare in un sistema informatico per accedere alle sue risorse. Questo problema è legato al controllo degli accessi che stabilisce chi può accedere alle risorse e cosa gli è consentito fare ("chi può fare cosa").
L'**autenticazione** è il processo di verifica e controllo che un soggetto identificato sia veramente chi dice di essere. Nell'ambito informatico è necessario autenticare gli utenti che devono accedere a un sistema, ma anche le applicazioni client/server che comunicano tra loro in rete.
Occorre distinguere quindi le operazioni di identificazione, autenticazione e autorizzazione:

- **identificazione**: presa d'atto della dichiarazione d'identità di un utente (o di una applicazione utente);
- **autenticazione**: verifica che l'utente sia chi dice di essere;
- **autorizzazione**: permesso di effettuare determinate operazioni su una risorsa come, per esempio, lettura, scrittura, modifica, ...).

Per esempio, un insegnante che passa in un corridoio di una scuola è identificato dal cartellino di riconoscimento, con nome (ID) e foto. Quando accede alla fotocopiatrice l'insegnante deve inserire nome e password: il sistema verifica l'identità, lo autentica, confermandone la validità, e autorizza la richiesta.
In generale il processo di autenticazione riguarda tutti gli attori coinvolti. Per esempio, quando un utente si connette a un server per effettuare un'operazione di home banking, deve essere sicuro che il server a cui si è collegato sia effettivamente la società di credito; ma anche la banca deve essere sicura che l'utente sia chi dice di essere.

Pit Stop

9 Che differenza c'è tra identificazione e autenticazione di un utente?

La password

Il modo più comune per identificare e autenticare un utente è tramite **userid** e **password**:

- lo userid è un codice che identifica un utente a cui è consentito l'accesso a un sistema. Non è segreto. In genere è definito dall'amministratore del sistema con un formato uguale per tutti gli utenti (per esempio *nome.cognome*);
- la password serve per verificare che l'utente sia chi dice di essere. È rigorosamente segreta.

Utilizzare una password sicura è di fondamentale importanza. Esistono delle regole di base che sono raccomandazioni, alcune anche imposte dai sistemi, per la scelta di una password:

- utilizzare password con una lunghezza minima di 8 caratteri e una massima di 64 caratteri;
- utilizzare una combinazione di caratteri minuscoli e maiuscoli, numeri e caratteri speciali;
- utilizzare le iniziali di una poesia o di una canzone, facili da ricordare per l'utente ma impossibili da indovinare per un hacker;
- evitare ripetizioni o sequenze di caratteri;
- evitare l'utilizzo di password di uso comune o scontate (come ad esempio P@ssw0rd, admin, user);
- non includere nella password il proprio nome, il nome del proprio animale domestico, dei figli, del marito/moglie/compagno/compagna o, in generale, riferimenti personali.

Per quanto riguarda la gestione, si raccomanda di:

- modificare periodicamente la password;
- non utilizzare la stessa password per accedere a servizi diversi;
- non trascrivere la password su foglietti;
- non memorizzare la password sul browser;
- non trasmettere mai la password in rete (via mail, via chat, al telefono...);
- non guardare mai un altro utente mentre digita una password (regola di buon comportamento!);
- assicurarsi che la password sia e rimanga segreta;
- non usare un account (username e password) aziendale per scopi personali;
- non accedere alla posta personale da client aziendali.

La Tabella 1 sintetizza le principali **tecniche di hacking** utilizzate per il furto delle password.

Tecnica di hacking	Descrizione	Contromisura
Attacco a dizionario	Tentativi ripetuti e sistematici di inserimento di password ritenute più probabili (dizionario)	Bloccare il sistema dopo un numero limitato di tentativi non andati a buon fine
Credential Stuffing	Utilizzo di password deboli oppure rubate da precedenti data breach basandosi sulla negligenza degli utenti che utilizzano la stessa password per contesti, sistemi e servizi web diversi	Usare password diverse e sicure. Modificare la password frequentemente
Brute Force	Tentativi ripetuti e casuali (automatici). Si provano tutte le varie combinazioni di caratteri alfanumerici finché non si trova la giusta combinazione	
Phishing	L'hacker si finge un'organizzazione nota (banca, posta,..) e chiede l'inserimento via web delle credenziali	Mai inserire le proprie credenziali in rete

↑ Tab. 1 Tecniche di hacking per il furto delle password.

Autenticazione debole e autenticazione forte

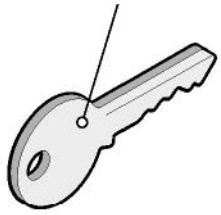
Il livello di sicurezza aumenta combinando tra loro diverse tecniche di autenticazione, che usano tecnologie differenti che rientrano in tre categorie:

ARE (Inherence-based)
qualcosa che sei
something the user is



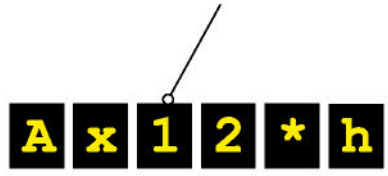
Tecnologie biometriche come l'impronta digitale, la mappatura della retina, il timbro vocale, la propria firma, la velocità di battitura dei tasti.

HAVE (Possession-based)
qualcosa che hai
something the user has



Schede magnetiche, smart card, chiavi, smart phone,…

KNOW (Knowledge-based)
qualcosa che sai
something the user knows



Password, PIN, risposta alla domanda sicura, codici vari

notabene

Spesso il livello a due o tre fattori è opzionale e la sua attivazione è decisa dall'utente.

Ciascuna di queste tre modalità, da sola, costituisce una forma di autenticazione debole. Per ottenere un'autenticazione forte, occorre usare in contemporanea *almeno due* dei tre fattori di autenticazione.
In questo caso si parla di autenticazione a più fattori (**MFA**, **M***ulti*-**F***actor* **A***uthentication*, Figura 4).

Autenticazione a due fattori (2FA)	Autenticazione a tre fattori (3FA)
Dopo aver inserito la password (primo fattore), il sistema chiede il secondo fattore, che può essere: • un numero inviato all'utente con un sms al suo smart phone (metodo poco sicuro) o tramite applicazioni dedicate. Ha una durata limitata ed è chiamato OTP (One Time Password); • un elemento biometrico, come un'impronta o il riconoscimento facciale.	Esempio di utilizzo: lo SPID (Sistema Pubblico di Identità Digitale) di livello 3. In questo caso i tre fattori usati sono: • la password • l'App PosteID (o altro ente certificatore) • il PIN SPID 3

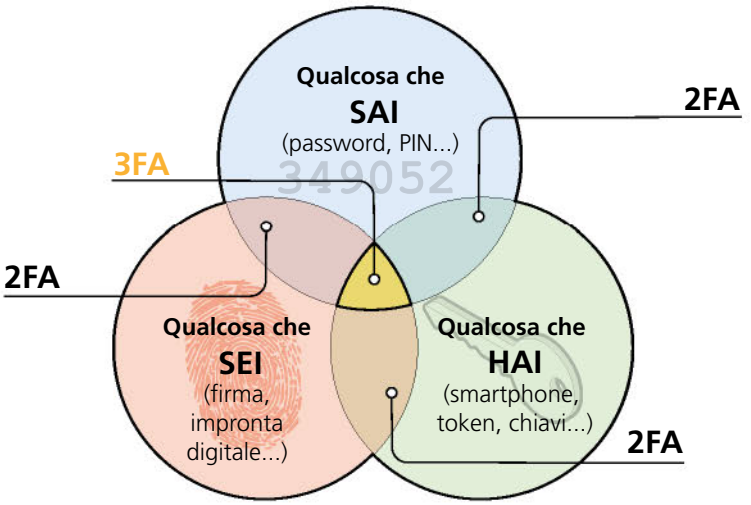


Fig. 4 Autenticazione a più fattori.

Approfondimento
Lo SPID

Autenticazione passwordless

La **Passwordless Authentication** (autenticazione senza password) è un metodo di autenticazione che non utilizza password, evitando così tutti i rischi e le debolezze legate a un uso scorretto.
L'Alliance e il W3C (*World Wide Web Consortium*), nel 2018, hanno lanciato **Fido2 Project** (*Fast Identity Online*) con l'obiettivo di sviluppare standard per un mondo digitale sicuro e passwordless.
FIDO2 funziona nel seguente modo (Figura 5):

1. quando un utente si registra a un servizio online, è generata una coppia di chiavi (pubblica e privata) sul dispositivo utilizzato. La chiave pubblica è la chiave FIDO2;
2. la chiave privata è memorizzata sul dispositivo ed è nota solo al client;
3. la chiave pubblica (chiave FIDO2) è memorizzata nel database delle chiavi del servizio web;
4. i successivi accessi al servizio sono effettuati tramite una prova della chiave privata, che deve essere sbloccata dall'utente con un pin, un comando vocale, un token FIDO2.

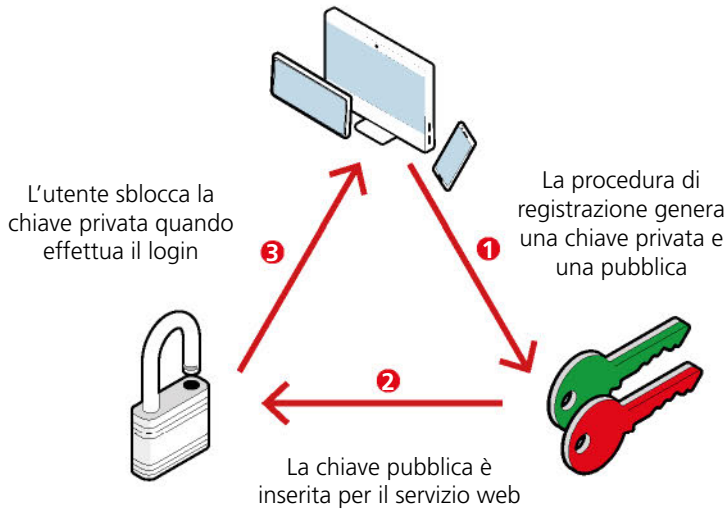


Fig. 5 Schema di funzionamento di FIDO2.

Pit Stop

10 Che cos'è l'autenticazione forte?

11 Che cos'è la Passwordless Authentication?

notabene

Per l'autenticazione FIDO2 è necessario utilizzare lo standard WebAuthn, integrando le relative API (scritte in javascript) nelle applicazioni.

Questo metodo di autenticazione senza password presenta i seguenti vantaggi:

- evita attacchi come Man in the Middle o il phishing;
- offre una superficie di attacco più limitata;
- è uno standard aperto e questo consente agli sviluppatori di utilizzarlo e integrarlo nei propri prodotti;
- agevola l'utente che non deve più preoccuparsi della gestione delle password.

Single Sign-On

SSO (***S**ingle **S**ign-**O**n*) consente di accedere a più servizi in rete, autenticandosi una sola volta.
Il sistema richiede l'autenticazione all'accesso al primo servizio e successivamente utilizza un processo per mantenere memoria dell'avvenuta autenticazione senza la necessità di richiederla nuovamente.
L'autenticazione con SSO è basata su una relazione di fiducia tra domini e siti web.
Quando un utente cerca di accedere a un servizio:

- il servizio verifica che l'utente sia già stato autenticato. In caso affermativo l'accesso è consentito;
- se invece l'utente non è ancora autenticato, è reindirizzato a un fornitore di servizi SSO;
- a questo punto l'utente inserisce nome utente e password;
- il fornitore di servizi SSO determina quale provider di identità (IdP) affidabile utilizzare e reindirizza l'utente a quel provider;
- quando l'utente è autenticato può accedere a tutti i servizi che utilizzano lo stesso sistema SSO senza più reinserire le proprie credenziali.

notabene

Il meccanismo è simile alla tecnica utilizzata con cookie e session per risolvere il problema dell'HTTP stateless ed evitare che a un utente che si autentica per accedere a un'area riservata, sia richiesto nuovamente di autenticarsi quando cambia pagina all'interno della stessa area riservata.

Un **provider di identità** (**IdP** - **I***dentity* **P***rovider*) è un sistema usato per l'autenticazione di utenti o di applicazioni. Per esempio, come spesso accade, è possibile utilizzare il proprio account Google per accedere a un servizio web. In questo caso Google è l'IdP (Figura 6).

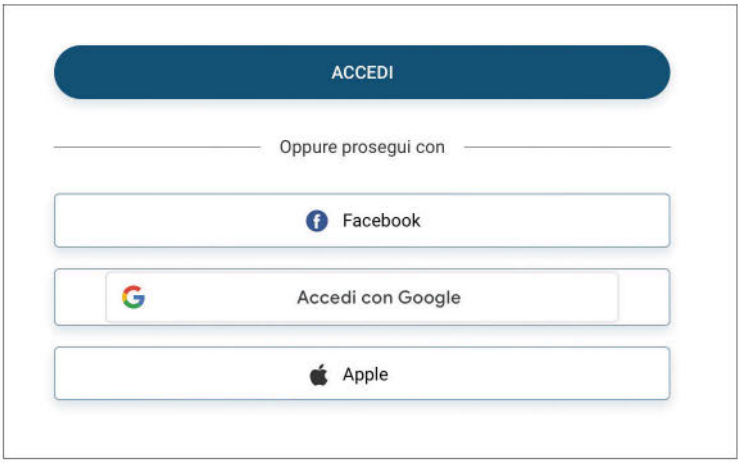
Tra gli standard utilizzati per implementare l'autenticazione SSO troviamo:

- SAML (*Security Assertion Markup Language* del 2005) basato su **xml**.
- OAuth (RFC 5849 del 2010 e RFC 6749 del 2012) basato su **json**.

Pit Stop

12 Qual è il vantaggio del processo di autenticazione con SSO?

13 Che cos'è un provider di identità?



➜ Fig. 6 Accesso ad un servizio utilizzando un account di Google.

L'utilizzo di un sistema di autenticazione SSO presenta i seguenti vantaggi:

- agevola l'utente;
- riduce il lavoro del personale tecnico di un'azienda soprattutto in presenza di un elevato turnover;
- aumenta il livello di sicurezza.

Il protocollo SAML

SAML (**S***ecurity* **A***ssertion* **M***arkup* **L***anguage*) è uno **standard** open source basato su XML, utilizzato per il Single Sign-On. Definisce il modo in cui i provider possono offrire servizi di autenticazione e autorizzazione. Permette, con un unico accesso, di accedere a più applicazioni o risorse web, senza dover inserire le credenziali ogni volta.
È come se SAML ci desse la possibilità di ottenere un passaporto per entrare in nazioni diverse senza chiedere ogni volta una nuova autorizzazione.
Lo scambio di informazioni di autenticazione e autorizzazione avviene tra tre attori principali:

- un provider di identità (IdP - *Identity Provider*) che autentica gli utenti, cioè verifica l'identità quando, ad esempio, vengono inseriti nome utente e password. È simile a una banca dati personale.
- Il provider di servizi (SP - *Service Provider*) che offre servizi e risorse. Sia gli SP che gli IdP fanno parte della gestione federata dell'identità (FIM), in cui gli utenti possono utilizzare lo stesso metodo di verifica per accedere a risorse diverse.
- L'utente che richiede un servizio. Dal punto di vista dell'IdP, un utente è il "richiedente" che può essere un umano o una macchina. Un IdP recupera le identità e determina se una persona o un dispositivo può accedere ai dati richiesti.

Il processo con cui SAML consente a un IdP di autenticare gli utenti e trasferire le credenziali di autenticazione ai provider di servizi è il seguente: per accedere a un sito web o a una risorsa, l'SP chiede all'IdP di confermare l'identità dell'utente. L'IdP invia un "certificato" (chiamato *token*) all'SP per dimostrare l'identità dell'utente.
Il flusso di autenticazione prevede alcuni passaggi chiave (**Figura 7**):

1. l'utente si collega alla pagina web del fornitore di servizi richiedendo una risorsa e dichiarando la sua identità inserendo, ad esempio, nome utente e password o l'autenticazione biometrica;

notabene

SAML è definito in diverse RFC, tra cui RFC 6595 e RFC 7522.

Pit Stop

14 Quali sono gli "attori" nel processo di autenticazione e autorizzazione del protocollo SAML?

La parola a... Hedy Lamarr



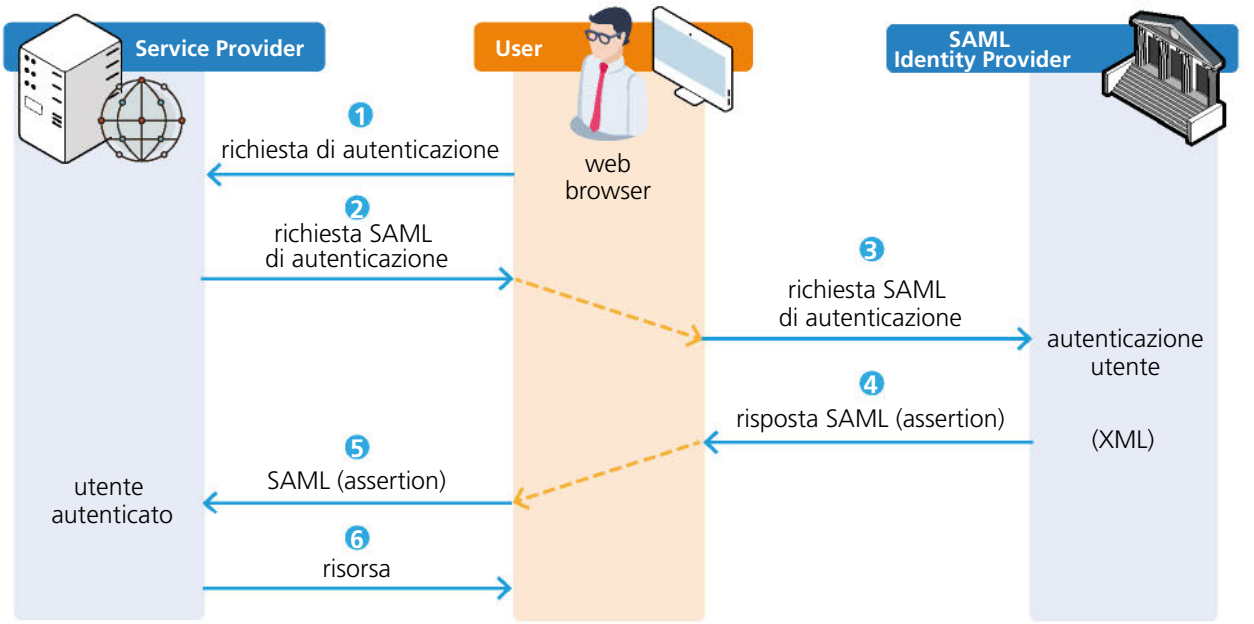
Dagli anni Trenta agli anni Cinquanta del secolo scorso, Hedy Lamarr (pseudonimo di Hedwig Eva Maria Kiesler) fu «la donna più bella del mondo». Nata a Vienna nel 1914, dotata di una memoria prodigiosa, recitò fin da giovanissima e negli Stati Uniti divenne una delle dive più popolari di Hollywood. Ma non fu solo un'attrice: durante la Seconda guerra mondiale, Hedy ideò e brevettò la famosa tecnologia del "salto di frequenza" (FHSS). Poi perfezionato e conosciuto come Code-Division Multiple Access (CDMA), il metodo sta alla base di molti sistemi wireless come Bluetooth, Wi-Fi e telefoni cellulari. Permette a più utenti di condividere la stessa banda assegnando a ciascuno un codice unico. Si tratta di una forma di crittografia analogica: cambiando continuamente le frequenze di trasmissione, il segnale diventa molto difficile da intercettare e interpretare. In una delle ultime interviste (morì all'età di 85 anni), Hedy Lamarr disse: «*L'esperienza e la curiosità per il futuro mi sembravano migliori della conoscenza del presente. L'ignoto è sempre stato attraente per me... e lo è ancora.*»

notabene

Il "token" è una "asserzione SAML", cioè un messaggio in formato XML, che fornisce una prova dell'identità di un utente e i diritti di accesso.

2. il fornitore di servizi crea una richiesta SAML per il provider di identità e la invia al browser dell'utente;
3. il browser dell'utente inoltra automaticamente la richiesta SAML al provider di identità;
4. il provider di identità autentica l'utente e fornisce un "token" al browser contenente le informazioni e i privilegi dell'utente;
5. il browser dell'utente inoltra l'asserzione SAML al fornitore di servizi per autenticare e autorizzare l'utente;
6. il fornitore di servizi risponde con la risorsa originariamente richiesta.

Durante il processo, i certificati vengono utilizzati per autenticare il provider di identità. Il certificato pubblico del provider di identità è necessario per garantire che l'asserzione SAML sia autentica.



↑ **Fig. 7** Il flusso di autenticazione SAML. L'IdP stabilisce una relazione di fiducia con uno SP autenticando l'utente e dichiarando che l'utente dispone dell'autorizzazione per accedere al servizio.

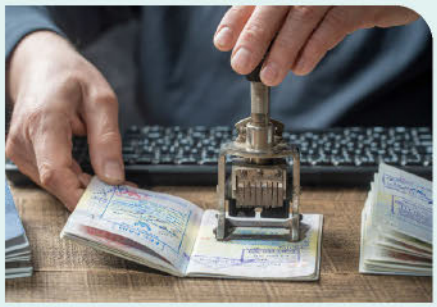
4 La Firma Digitale

La Firma Digitale è l'equivalente informatico della firma autografa che consente di sottoscrivere digitalmente, con il proprio dispositivo, documenti con valore legale.
È una **firma elettronica qualificata** (si veda approfondimento "Tipi di firme elettroniche") basata sulla crittografia a chiave asimmetrica. In Italia l'utilizzo della Firma Digitale è regolamentato dal Codice dell'Amministrazione Digitale (CAD) e dalla Agenzia per Italia Digitale (AgID).
Grazie all'utilizzo dell'algoritmo RSA e all'impego di funzioni di hash, la Firma Digitale garantisce:

- l'autenticazione del documento;
- l'integrità del documento;
- la non ripudiabilità del documento.

Comprendi con l'analogia

Il passaporto rilasciato dal governo è come un token rilasciato da un provider d'identità



Marco sogna la sua destinazione: un'isola tropicale con spiagge di sabbia bianca e acque cristalline. Ma prima di poter salire a bordo dell'aereo, deve ottenere un passaporto.
Per ottenere il passaporto, Marco deve dimostrare la propria identità a un ufficio governativo, fornendo i suoi dati personali (nome, cognome, data di nascita ecc.). L'ufficio, che rappresenta il provider di identità (IdP), verifica questi dati e, se sono corretti, rilascia un passaporto, che corrisponde a un token. All'arrivo sull'isola, un impiegato della dogana lo accoglie dandogli il benvenuto. «Per favore, mi mostra il passaporto?» Con questo passaporto, Marco può realizzare il suo sogno (accedere all'isola, la risorsa desiderata). Questa procedura di identificazione è simile al modo in cui un Service Provider in SAML utilizza l'asserzione SAML (il passaporto) per concedere all'utente l'accesso alla risorsa richiesta.

Il funzionamento si basa sul fatto che, con l'algoritmo RSA, la decodifica che usa la chiave privata di un messaggio codificato con chiave pubblica riproduce il messaggio originale:

$$D_{kprivdest}\,(C_{kpubdest}\,(m)) = m$$

Ma è vero anche l'**inverso**: la decodifica con la chiave pubblica di un messaggio codificato con chiave privata riproduce il messaggio di partenza:

$$D_{kpubmittente}\,(C_{kprivmittente}\,(m)) = m$$

Di seguito vediamo il funzionamento della Firma Digitale:

1. al documento originale è applicata una funzione di hash per ottenere una stringa di caratteri di dimensione ridotta (*digest*). Questa costituisce il "riassunto" del documento;
2. il digest è criptato con la chiave privata del mittente;
3. il mittente invia al destinatario il digest criptato (firma) e il documento originale in chiaro;
4. il destinatario applica al documento ricevuto la stessa funzione di hash usata dal mittente e ottiene il digest del documento ricevuto;
5. decripta il digest ricevuto con la chiave pubblica del mittente;
6. confronta il digest decriptato e quello calcolato.

Se i digest sono uguali, si ha la certezza della provenienza del documento (autenticazione e non ripudio) e dell'integrità del documento, in quanto se fossero state apportate modifiche, il digest ricalcolato sarebbe diverso.
La Firma Digitale non garantisce la segretezza del messaggio perché chiunque abbia la chiave pubblica del mittente può leggerlo. Nel caso fosse necessario garantire **sia la segretezza sia l'autenticazione**, il mittente dovrebbe:

- crittare il digest con la propria chiave privata (per l'autenticità) e successivamente criptare con la chiave pubblica del destinatario (per la segretezza);

e il destinatario dovrebbe:

- decrittare il digest ricevuto con la propria chiave privata (per la segretezza) e successivamente decrittare con la chiave pubblica del mittente (per l'autenticità).

notabene

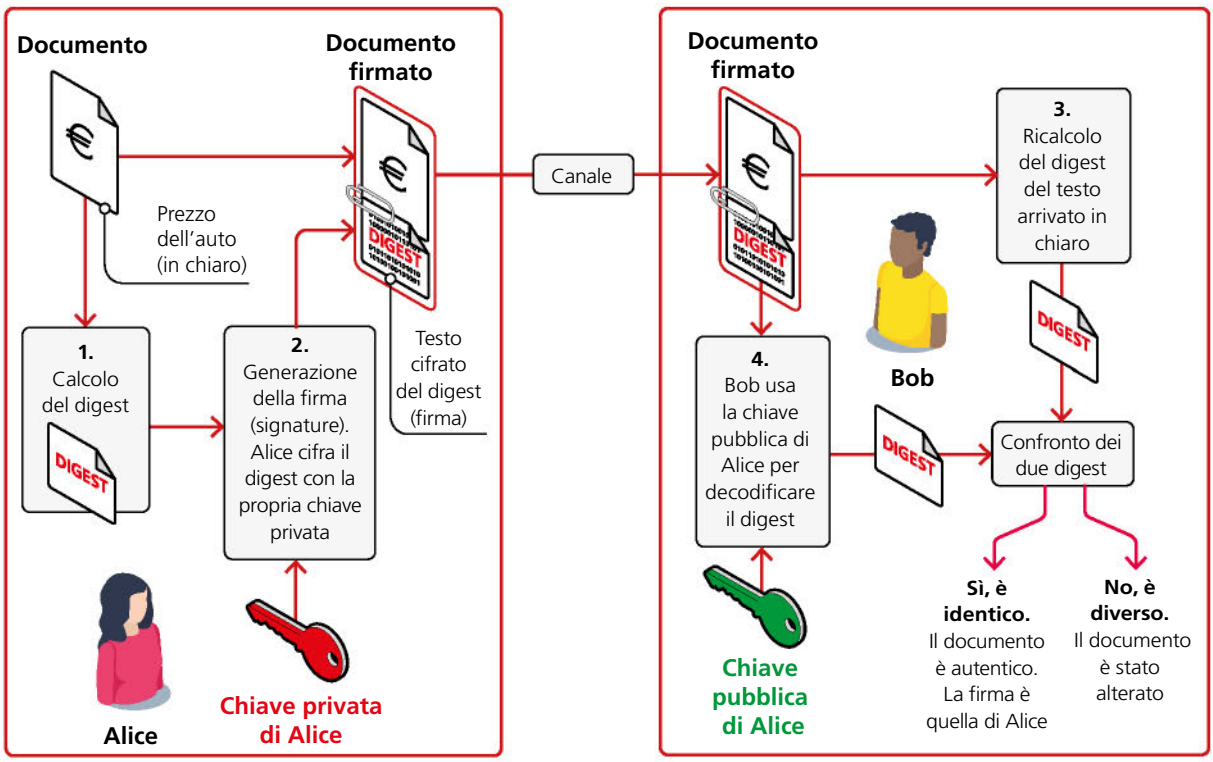
Le funzioni di hash trasformano una stringa di lunghezza qualunque in una di lunghezza fissa (*digest*); vedi il Paragrafo 6 di questa Unità.

Pit Stop

15 Che cos'è la Firma Digitale?

16 Quali sono i vantaggi della Firma Digitale?

Supponiamo che Alice debba inviare un documento con valore legale a Bob. Per esempio, un documento con l'offerta del prezzo dell'auto che desidera vendere. È necessario che Bob sia certo che l'offerta provenga da Alice e che Alice non disconosca di avere inviato l'offerta (Figura 8).
Il documento viene firmato a garanzia della propria identità. In questo modo Alice certifica la provenienza del messaggio permettendone l'autenticazione e il non ripudio.



↑ **Fig. 8** La Firma Digitale è utilizzata per autenticare un documento che deve avere valore legale. Oltre all'autenticazione garantisce il non ripudio e l'integrità del documento.

La Firma Digitale può essere apposta a qualunque documento proprio come una firma autografa. Esempi di documenti a cui apporre una Firma Digitale sono: documenti notarili, documenti commerciali, ordini di acquisto e vendita, comunicazioni con la pubblica amministrazione, atti ufficiali,.... Oltre al riconoscimento del valore legale, la Firma Digitale favorisce la **dematerializzazione** e velocizza lo scambio di documenti favorendo l'efficienza dei sistemi informativi.
La Firma Digitale può essere utilizzata in due modalità:

1. **in "locale"**: generata utilizzando uno strumento del proprietario.
   Per firmare digitalmente un documento occorre:
   – richiedere l'attivazione a uno dei gestori accreditati dall'AgID, fornendo i documenti e quanto richiesto per il controllo dell'identità (come per lo SPID). Il servizio è a pagamento. I gestori emettono dei certificati autentici. Esempi di gestori sono: Aruba, Poste Italiane, InfoCert, ... ;
   – Il gestore fornisce un kit (chiavetta, o altro strumento) e un software che il cliente deve utilizzare sul proprio dispositvo. Il kit contiene il certificato;
   – convertire il file in un formato non modificabile (per esempio PDF);
   – avviare il software fornito dal gestore (spesso su chiavetta USB o altro strumento);
   – e selezionare il file da firmare.

2. **da "remoto"**: è una soluzione molto più comoda perché evita l'utilizzo del kit. Il funzionamento è simile alla Firma Digitale in locale, ma il certificato non è fornito con il kit, ma è su un server del fornitore.
   È possibile firmare utilizzando il servizio via web, previa autenticazione a più fattori (per esempio USERID + PASSWORD + OTP)

5 I certificati digitali

La Firma Digitale autentica un documento, ma chi garantisce che una chiave pubblica è effettivamente associata a un certo utente? È necessario un garante. Il **certificato digitale** (Digital ID) è il documento che assicura l'**autenticazione della chiave pubblica**, cioè conferma che una chiave appartiene veramente al suo proprietario. I certificati digitali sono emessi da autorità di certificazione (CA - *Certification Authority*), strutture incaricate del rilascio dei certificati e testimoni credibili della veridicità dei dati contenuti. A fronte di una richiesta da parte di una persona, ente o sito web, le autorità di certificazione ne controllano l'identità ed emettono il certificato che verrà conservato in un registro pubblico con tutti i certificati digitali emessi e con quelli revocati. Un certificato, quindi, conferma l'identità di un utente e contiene informazioni usate per proteggere i dati o per stabilire connessioni di rete sicure.
Tra le maggiori società al mondo che si occupano della Firma Digitale, delle chiavi pubbliche e del rilascio dei certificati ci sono Verisign (Symantec), AT&T, American Express. In Italia gli enti certificatori sono quelli collegati a organizzazioni statali, grossi gruppi bancari e qualche provider (Figura 9).

Pit Stop

17 Quali sono le due modalità d'uso della Firma Digitale?

18 In che cosa si differenziano?

19 Che cos'è il certificato digitale?

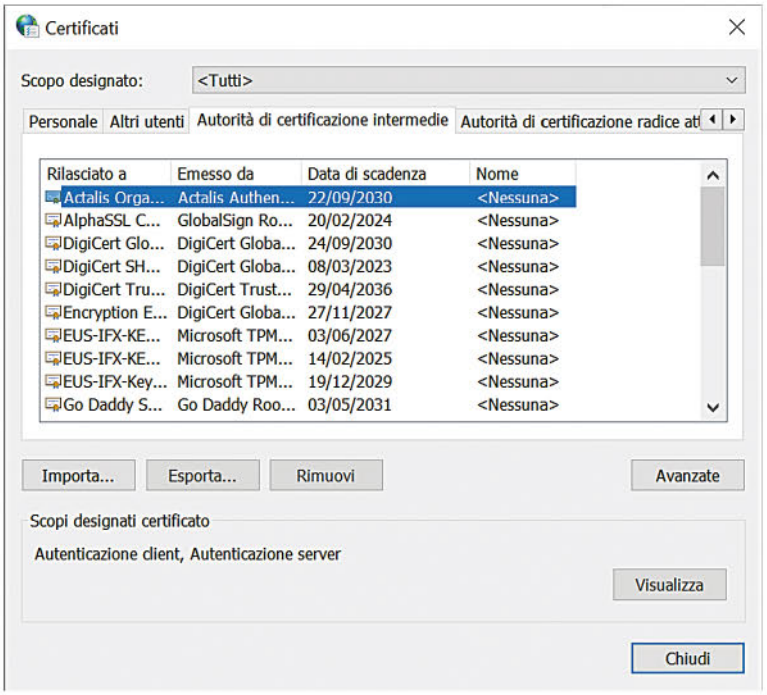


Fig. 9 Dalle impostazioni del browser o del sistema operativo è possibile risalire alle autorità di certificazione presenti nel sistema.

I certificati legano il nome del titolare (una persona, una società, un dispositivo) alla sua chiave pubblica utilizzata per le funzioni di cifratura/decifratura e autenticazione, e sono analoghi alla carta di identità che il Comune (ente certificatore) rilascia al cittadino, garantendone l'identità.

Pit Stop

20 Chi emette i certificati digitali?

Un certificato è firmato con la chiave privata dell'autorità di certificazione e la sua struttura, conforme allo standard X.509, include, tra l'altro, le seguenti informazioni:

- il numero di serie;
- informazioni sul titolare della chiave pubblica (nome, cognome, ragione sociale...);
- la chiave pubblica del titolare (*public key*);
- il periodo di validità;
- il nome CA che ha firmato il certificato;
- la Firma Digitale della CA.

Per esempio, se Bob vuole fornire ad Alice una prova della sua identità, richiede un certificato alla Certification Authority. La CA emette un certificato, firmato con la propria chiave privata, che contiene la chiave pubblica di Bob (**Figura 10**).

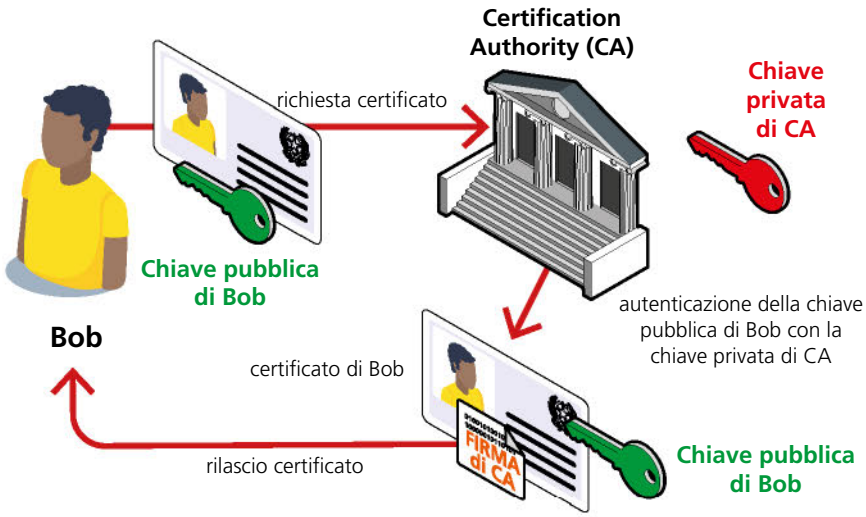


Fig. 10 Il processo di certificazione. Il soggetto che vuole essere certificato invia a CA i propri dati personali e la sua chiave pubblica, CA autentica la chiave pubblica del soggetto con la propria chiave privata ed emette il certificato firmato.

Quando Alice ottiene il certificato di Bob, si accerta dell'autenticità della chiave pubblica di Bob, applicando la chiave pubblica della CA che lo ha firmato e della cui autenticità si fida (**Figura 11**).

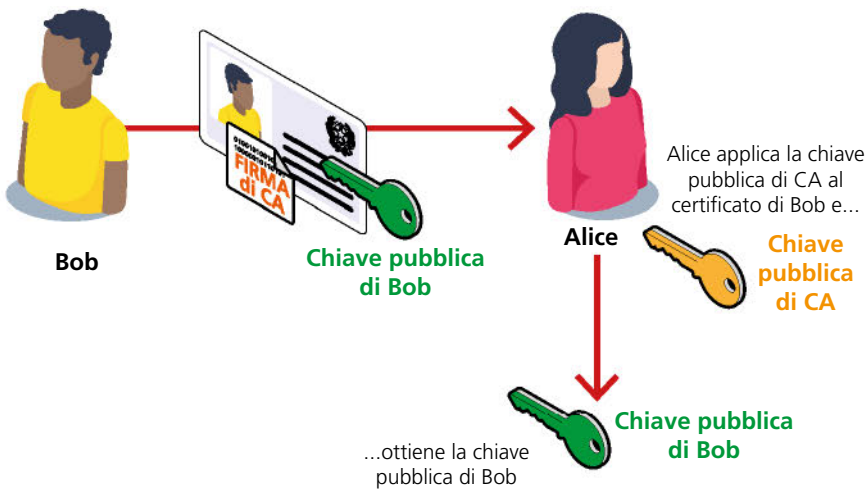


Fig. 11 Bob fornisce ad Alice una prova della sua identità tramite il proprio certificato firmato (e garantito) da CA. Alice applica la chiave pubblica della CA, di cui si fida, al certificato di Bob e ottiene la chiave pubblica di Bob.

6 Le funzioni di hash

Le funzioni di hash sono funzioni che trasformano una stringa di lunghezza arbitraria in una stringa di lunghezza fissa, chiamata **digest**. Le funzioni di hash hanno due proprietà importanti:

- sono **non invertibili**, che significa che dalla stringa ottenuta non è possibile ricostruire la stringa di partenza;
- **ogni stringa di input dà luogo a un'unica stringa di output** che rappresenta una sorta di "impronta digitale" dell'input. Due input diversi non possono avere lo stesso digest.

Le proprietà sono utilizzate per garantire l'integrità del dato di input poiché una modifica (intenzionale o meno) genera un digit diverso.
L'input è una qualsiasi sequenza di caratteri: una password, un documento...
Sono utilizzate in vari ambiti informatici, tra cui:

- la comunicazione client/server cifrata;
- la cifratura delle password;
- la Firma Digitale;
- l'organizzazione di strutture di dati (*hash table*).

Ci sono vari algoritmi utilizzati per implementare le funzioni di hash. Questi si caratterizzano per la lunghezza della stringa di output. Di seguito presentiamo i più comuni.

- MD5 (*Message Digest Algorithm 5*), sviluppato da Ronald Rivest e oggi considerato non del tutto sicuro).
- SHA (*Secure Hash Algorithm*), uno standard adottato dalla NSA (National Security Agency).
  Il termine SHA indica una famiglia di funzioni crittografiche di hash. Alla famiglia SHA appartengono:
  – SHA-1 (160 bit),
  – SHA-2 che comprende: ▸ SHA-256 (256 bit) ▸ SHA-512 (512 bit)
  che producono digest di lunghezza in bit pari al numero indicato nella sigla.

In rete ci sono tante applicazioni per il calcolo dell'hash.
Nella seguente tabella sono riportati degli esempi di applicazione di algoritmi di hash con i corrispondenti output. Come input consideriamo la parola "ciao" per semplicità, ma potrebbe essere un file di qualsiasi dimensione.

Testo originale	ciao codice ascii (in esadecimale): 63 69 61 6f

Algoritmo	Digest (in esadecimale)	Lunghezza digest (in bit)
CRC32	4ddf4306	32
MD5	6e6bc4e49dd477ebc98ef4046c067b5f	128
SHA-1	1e4e888ac66f8dd41e00c5a7ac36a32a9950d271	160
SHA_256	b133a0c0e9bee3be20163d2ad31d6248db292aa6dcb1ee087a2aa50e0fc75ae2	256
SHA_512	a0c299b71a9e59d5ebb07917e70601a3570aa103e99a7bb65a58e780ec9077b 1902d1dedb31b1457beda595fe4d71d779b6ca9cad476266cc07590e31d84b206	512

Pit Stop

21 Che cos'è una funzione di hash?

22 Quali sono i più comuni algoritmi che implementano le funzioni di hash?

7 Server AAA

Con il termine AAA (**Authentication**, **Authorization**, **Accounting**) si intende un insieme di protocolli utilizzati per il controllo degli accessi a una rete informatica. Il controllo è diviso in tre fasi:

- Autenticazione ("chi sei"). Verifica l'identità di un utente che chiede l'accesso alla rete.
- Autorizzazione ("cosa ti è permesso fare"). Definisce le operazioni che il soggetto riconosciuto, può effettuare. Per questo possono essere utilizzati l'elenco delle operazioni ammesse (ACL) insieme ai privilegi di cui l'utente dispone. Un conto è essere riconosciuto dal sistema, un altro è poter fare tutte le operazioni possibili. Uno studente, per esempio, può accedere alla rete scolastica ma non leggere o modificare i dati anagrafici di compagni e insegnanti.
- Accounting ("quali operazioni hai svolto realmente"). Tiene traccia dell'utilizzo di una risorsa da parte dell'utente per fini di sicurezza, statistici e di tariffazione. Possono essere controllati e salvati gli accessi, il tempo di permanenza nel sistema, le modifiche apportate, le operazioni fatte ecc.

Un esempio di protocollo AAA è **RADIUS** (**R***emote* **A***uthentication* **D***ial-in* **U***ser* **S***ervice*) definito in RFC 2865 e 2866. È un protocollo client/server che fornisce servizi di autenticazione, autorizzazione e accounting. Il client (per esempio un Access Point) invia le credenziali dell'utente e i parametri di connessione al server RADIUS, che autentica e autorizza la richiesta del client. Lo stesso client invia anche messaggi di accounting per il tracciamento dei collegamenti effettuati e delle risorse utilizzate. I messaggi RADIUS sfruttano la porta 1812 di UDP per l'autenticazione e la porta 1813 per l'accounting.
È spesso utilizzato per i servizi AAA tra un NAS (*Network Access Server*) e un Authentication Server.

Comprendi con l'analogia

AAA e carta di credito

La carta di credito è un classico esempio del concetto AAA. L'autenticazione prevede codice e nome. L'autorizzazione alla spesa fornisce il massimo credito a disposizione. Il report dettagliato degli acquisti, con date, importi e descrizione, costituisce l'accounting.



Approfondimento - Storia

Da Giulio Cesare a Enigma

La storia della crittografia precede di migliaia di anni quella dei calcolatori e si perde nella notte dei tempi. L'uomo, da sempre, ha sentito l'esigenza di creare codici segreti capaci di proteggere da sguardi indiscreti i propri messaggi. Ragioni militari, politiche, commerciali, economiche, religiose, amorose hanno segnato la storia della crittografia. Una transazione economica o un ordine militare non devono essere conosciuti da concorrenti e nemici.
Uno dei più antichi algoritmi di crittografia è il **Cifrario di Cesare** con cui **Giulio Cesare**, secondo lo storico Svetonio, crittava le comunicazioni segrete con le proprie truppe, con le lettere disposte in modo tale che «nessuna parola potesse essere ricostruita: se qualcuno avesse voluto capire il senso e decifrare, avrebbe dovuto cambiare la quarta lettera degli elementi, cioè D per A e così via per le rimanenti». Questo tipo di cifratura fa parte degli algoritmi a trasposizione ed è chiamata "a sostituzione monoalfabetica": ogni lettera è sostituita con un'altra che si trova avanti di un certo numero di posti rispetto all'ordine alfabetico. L'algoritmo è noto, il numero di posti costituisce la chiave e non è conosciuto a priori.

Esempio 1

Sostituzione monoalfabetica con chiave 3

Ogni lettera viene sostituita con quella che la segue di tre posti rispetto all'ordine alfabetico. L'algoritmo consiste nello "spostarsi di *k* posti in avanti" e usa la chiave di cifratura (*k*) con valore 3. La chiave di decifratura è la stessa e deve necessariamente essere conosciuta dal destinatario che applica l'algoritmo inverso.

Testo in chiaro	Testo cifrato
PROVA DI CIFRATURA	SURYD GL FLIUDWXUD

I cifrari monoalfabetici presentano alcuni punti di debolezza:

- l'analisi è relativamente semplice: confrontando le frequenze relative dei simboli nel testo cifrato con la distribuzione nota di frequenza delle lettere della lingua di partenza, si può risalire alle corrispondenze tra le lettere.
- Utilizzano un numero limitato di chiavi: solo 25, tante quante le lettere dell'alfabeto.

Successivamente questi algoritmi sono stati migliorati rendendo più laborioso risalire alla chiave utilizzata. A titolo di esempio, vediamo l'algoritmo di Leon Battista Alberti e l'algoritmo di Vigenère, del XVI secolo.
Nell'opera *De Cifris* (*Sulle cifre*) del 1466, Leon Battista Alberti (1404-1472) propose «una maniera di scrivere inventata da noi (...) in cui nessuna cifra, tra tutte quelle che si possono usare, è più rapida e più facile a leggersi; nessuna, se tu ignori gli indici convenuti tra me e un altro, si può pensare più segreta». Si tratta di due cerchi concentrici: quello esterno, che contiene l'alfabeto, è fisso. Il disco interno, mobile, contiene le lettere dell'alfabeto disposte in modo casuale. Ruotando il disco mobile in modo da posizionarlo su una certa lettera si ottiene una corrispondenza tra la lettera in chiaro del disco esterno e quella cifrata del disco interno (**Figura 1**).



↑ **Fig. 1** L'algoritmo di crittografia di Leon Battista Alberti.

Nel 1586, Blaise de Vigenère (1523-1596) pubblicò un algoritmo polialfabetico in cui la lettera viene spostata di un numero di posti variabile in funzione di una parola chiave, conosciuta da mittente e destinatario.

Esempio 2

Sostituzione polialfabetica

La lettera viene spostata di un numero di posti variabile in funzione della lettera corrispondente della parola "GELATO". Per esempio, la G occupa la settima posizione nell'alfabeto, quindi la B è codificata con la lettera H che è 7 posti avanti rispetto a B.

Messaggio in chiaro	B	E	L	L	A	G	I	O	R	N	A	T	A
Chiave	G	E	L	A	T	O	G	E	L	A	T	O	G
Messaggio cifrato	H	I	W	L	T	U	O	S	C	N	T	H	G

Uno dei vantaggi è che lo stesso carattere viene crittografato con caratteri diversi di volta in volta.



Fig. 2 Enigma, la macchina utilizzata dalle forze armate tedesche per criptare i messaggi durante la Seconda guerra mondiale.

Particolarmente rilevante è stato l'utilizzo della crittografia durante la Seconda guerra mondiale.
Fu la costruzione della macchina tedesca Enigma a segnare un punto di svolta (Figura 2): l'operatore digitava il messaggio usando la tastiera della macchina. I fili della tastiera entravano nell'elemento scambiatore comprendente vari rotori. I caratteri del primo rotore costituivano il nuovo alfabeto per il secondo e così via per tutte le ruote di cui era composta la macchina.
In questo contesto merita particolare attenzione la storia di Alan Turing.
Nato a Londra nel 1912, fin da giovane dimostrò eccellenti doti nel campo della matematica e della logica. Dopo la laurea in matematica mise a frutto queste sue abilità applicandole, in particolare, agli studi sulla crittografia. Allo scoppio della Seconda guerra mondiale, con un gruppo di crittoanalisti, Turing sviluppò un metodo per decrittare i messaggi militari tedeschi codificati con la macchina Enigma. Nel dopoguerra si interessò ai problemi logici legati ai calcolatori e all'intelligenza artificiale e, in particolare, al "modo di pensare" delle macchine.

notabene

Steganografia vs crittografia

La crittografia non deve essere confusa con la steganografia. Steganografia (da due parole greche che significano "nascosto" e "scrivere") indica l'arte di mantenere sconosciuta l'esistenza di informazioni a chi non possiede la chiave per estrarle. La steganografia "nasconde" un documento all'interno di un altro documento (la crittografia, al contrario, mostra il documento che però risulta incomprensibile).
Erodoto racconta la storia di un messaggero che venne rasato e a cui venne tatuato, sulla pelle del cranio, un messaggio segreto: «…allora, rasato il capo al più fidato dei suoi servi, vi tatuò dei segni, attese che ricrescessero i capelli e appena furono ricresciuti lo mandò a Mileto con il solo incarico, una volta giuntovi, di invitare Aristagora a radergli i capelli e a dargli una occhiata sulla testa. Il tatuaggio ordinava la ribellione». Scrivere con inchiostro simpatico fa parte della steganografia, così come cambiare alcuni pixel di un'immagine e sostituirli con un codice, in modo che l'osservatore non si accorga di nulla.





Fig. 3 Il complesso edilizio di Bletchley Park.

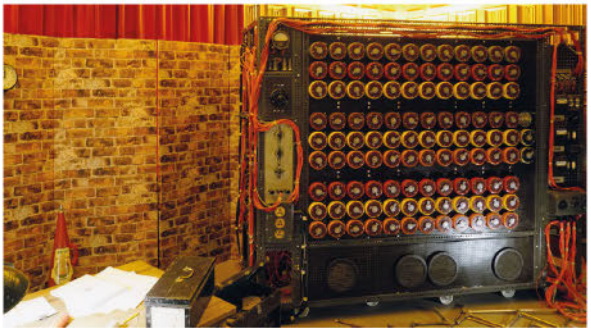


Fig. 4 La macchina progettata da Turing per violare Enigma.

La Figura 3 mostra il complesso edilizio di Bletchley Park, che durante la Seconda guerra mondiale fu sede dell'Unità di Crittoanalisi del Regno Unito, in cui Alan Turing escogitò una serie di tecniche per penetrare i cifrari tedeschi e una macchina elettromeccanica, soprannominata "La Bomba" (Figura 4), in grado di trovare le impostazioni della macchina Enigma.
La vita di Turing ebbe una svolta drammatica quando subì una condanna per "indecency", un reato che alludeva a relazioni omosessuali, all'epoca illegali nel Regno Unito, e gli venne imposta, per evitare il carcere, la castrazione chimica. L'esperienza lo devastò fisicamente e psicologicamente, e si ritiene che lo condusse al suicidio, per avvelenamento da cianuro, a soli quarantuno anni.

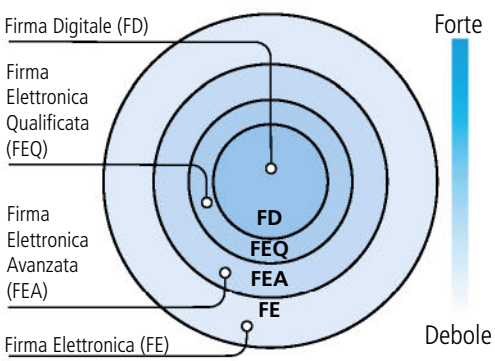
Approfondimento - Tecnologia 1

Tipi di firme elettroniche

La firma elettronica è un processo informatico che permette di identificare il sottoscrittore di un documento.
Ci sono varie tipologie di firma elettronica (definite nel Codice dell'Amministrazione Digitale) che consentono di sottoscrivere un documento in modo più o meno certo, con effetti giuridici diversi.
La normativa vigente individua diverse tipologie di firma elettronica (Figura 5):

1. **Firma elettronica semplice** (FES): è la forma più semplice di firma elettronica, più comune e più debole. Non garantisce autenticità né integrità del documento. Comprende dei dati che identificano il firmatario, per esempio userid e password collegati al firmatario.
2. **Firma elettronica avanzata** (FEA): è più complessa della FES, ma offre maggiore sicurezza e garantisce autenticità e integrità del documento. Per esempio, la firma apposta su un tablet. In questo caso si usano tablet grafometrici che rilevano i dati biometrici di chi firma (velocità, pressione...): È quindi memorizzata una firma biometrica.
3. **Firma elettronica qualificata** (FEQ): è la firma elettronica più complessa e più sicura. È basata su certificati emessi da un'Autorità. Garantisce autenticazione e integrità del documento e ha valore legale. La Firma Digitale è una FEQ.

Fig. 5 Tipi di firme elettroniche.



Approfondimento - Tecnologia 2

La rivoluzione della blockchain

La logica centralizzata (**Centralized Ledger**, libro mastro centralizzato) rappresentata **da un'autorità di controllo**, è caratterizzata da un **rapporto di fiducia basato sull'autorevolezza del sistema centrale** a cui tutti i satelliti fanno riferimento.
L'esatto contrario è la logica distribuita (**Distributed Ledger**) in cui **non esiste alcun centro di controllo** e la **fiducia è quella che si ripone tra i soggetti** (reti **Peer-to-Peer**, **trustless**). Le decisioni vengono prese attraverso un processo di costruzione del consenso in cui nessuno prevale.
La **blockchain è la realizzazione del Distributed Ledger**.
Con la decentralizzazione del libro mastro, la blockchain consente lo scambio peer-to-peer di informazioni diverse in modo crittograficamente sicuro. Blockchain è utilizzata per i pagamenti, lo scambio di servizi e beni e lo scambio di informazioni sui contratti (*Smart Contracts*) ed è soprattutto legata all'importante concetto di avere degli **asset digitali unici**. Un bene digitale (asset) può essere un documento, una canzone, una foto. Quando scattiamo una foto con il cellulare e la inviamo agli amici, non facciamo nient'altro che riprodurre questo file un numero arbitrario di volte. Il bene non appartiene più solo a noi, ma anche a loro e a tutti quelli che ne entreranno in possesso. Se, al contrario, stampiamo la foto e la regaliamo a un amico, diventa di sua proprietà e noi non ne siamo più in possesso.
Possiamo fare lo stesso ragionamento anche con beni di scambio come le monete: ogni volta che compro un caffè devo pagarlo con un euro che passa fisicamente dal mio portafoglio a quello del barista.
La blockchain permette di togliere alle risorse digitali la loro immaterialità e di fare ritornare il nostro asset digitale nel mondo fisico dove esiste il principio di "scarsità dei beni e delle risorse", consentendo di mantenerne il valore. Non a caso il mondo della finanza è stato il primo a comprendere il valore della blockchain nella sua capacità di mantenere l'unicità di un bene digitale (ricordiamo che Blockchain costituisce l'infrastruttura tecnologica della criptovaluta Bitcoin).



➜ **Fig. 6** Ogni nodo della rete peer-to-peer deve mantenere una copia identica di tutti i messaggi inviati. Ogni blocco include l'hash del blocco precedente nella blockchain. I blocchi collegati formano una catena.

Architettura della blockchain

Blockchain è un **database distribuito** sui nodi presenti nella rete. Le informazioni vengono registrate come messaggi, chiamati **blocchi**, che per essere identificati devono contenere delle informazioni, come ad esempio l'autore del messaggio e la data di creazione.
I dati che vengono inviati in rete **non sono più modificabili**, salvo l'approvazione dei nodi che hanno il compito di controllare e approvare tutte le transazioni che avvengono. Ogni nodo è, di fatto, un archivio di tutti i messaggi che vengono memorizzati in una sorta di "catena di blocchi" (Figura 6).
Nel caso più semplice la struttura di un blocco comprende un'intestazione del blocco e un messaggio (Figura 7).

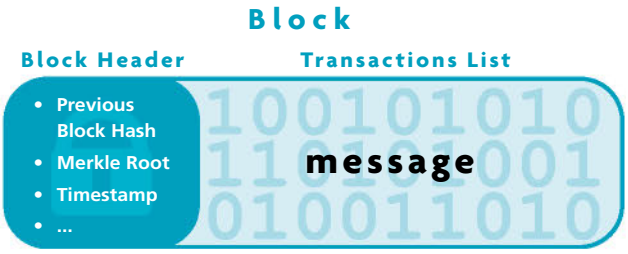


Fig. 7 L'intestazione del blocco contiene diversi campi tra cui: l'*hash* del blocco precedente (256 bit), che costituisce l'identificatore univoco, il *Merkle Root* che contiene il riepilogo di tutte le transazioni (un *Merkle Tree* è un albero in cui ogni foglia contiene l'hash di un blocco), il *Timestamp* dell'ultima transazione, il numero della transazione.

Una blockchain si basa sull'idea che il messaggio successivo contiene anche l'hash che autentica il messaggio precedente. Per garantire l'integrità dei messaggi, infatti, in ogni blocco è salvato l'hash del messaggio precedente. Per controllare l'integrità dei messaggi è sufficiente ricalcolare l'hash del messaggio precedente e confrontarlo con quello memorizzato. Se sono diversi, il messaggio è stato modificato.
In Figura 8 il Blocco0 contiene il Messaggio0. Il Blocco1 contiene, oltre al Messaggio1, l'hash del Blocco0 (H0). Il Blocco2 contiene l'hash del blocco precedente (Blocco1) e così via per i blocchi successivi che si possono aggiungere man mano.



Fig. 8 In ogni blocco della catena è salvato il codice hash del blocco precedente. Nel blocco genesi è contenuto il Messaggio0 senza l'hash. Il Blocco1 contiene, insieme al Messaggio1, l'hash di Messaggio0 (H0). Il Blocco2 contiene anche il codice che autentica Messaggio1 H1) e così via.

Per capire che un blocco è stato modificato è sufficiente calcolare l'hash del blocco e confrontarlo con quello contenuto nel blocco successivo. Ad esempio è facile scoprire se nella catena qualcuno ha modificato il Blocco1: basta calcolarne l'hash e confrontarlo con l'hash contenuto nel Blocco2. Per non farsi scoprire sarebbe necessario modificare anche il Blocco3 e tutti i successivi fino alla fine della catena.
Nel caso in cui dovesse capitare che nodi diversi posseggano copie diverse della catena, si applica il principio di democrazia, assumendo come valida la catena presente nella maggioranza dei nodi in rete.
Naturalmente la sicurezza non esiste mai al 100%, ma la probabilità di un attacco si riduce fortemente se il numero di nodi è molto elevato e il controllo che si pone è ai massimi livelli.



Fig. 9 Ethereum è una moneta virtuale che eredita da Bitcoin molte caratteristiche con l'ambizione di realizzare un sistema contrattuale parallelo a quello tradizionale: offre la possibilità, in maniera decentralizzata, di **eseguire script** (**smart contracts**) tramite i quali eseguire azioni al verificarsi di un particolare evento. Per esempio è possibile attivare, con una assicurazione con blockchain, uno smart contract di una polizza che rimborsi le cancellazioni di un volo.

Permissionless Ledger e Permissioned Ledger

Le reti blockchain "**Permissionless Ledger**", come Bitcoin ed Ethereum (Figura 9), sono aperte, non hanno proprietari e non sono controllate da un'autorità centrale. Questo ha permesso alle reti blockchain di candidarsi a tecnologia sicura e affidabile per lo "scambio di valore" (**Internet of value**) non solo monetario, ma anche di proprietà intellettuale o di diritti civili (per esempio per votare).
Le "**Permissioned Ledger**", al contrario del "libro mastro senza permessi", sono controllate e posseggono dei proprietari. Un nuovo blocco può essere inserito solo dopo l'approvazione di un ente di controllo ("trusted") che non è vincolato alla maggioranza dei partecipanti alla blockchain. Questo tipo di blockchain è utilizzato sempre di più da grandi imprese e organizzazioni come banche, gestori di carte di credito e e-commerce che vedono nel blockchain la base di un sistema innovativo di pagamenti. L'idea è quella di creare una criptovaluta sul modello di Bitcoin, che però sia più stabile e si agganci a monete fisiche, come il dollaro. Il vantaggio è quello di eliminare le intermediazioni fatte di commissioni e spese, ma anche di utilizzare le criptovalute come una sorta di "tessera fedeltà" per ricompensare gli utenti che utilizzino certi servizi o vedano certe pubblicità.

Approfondimento - Tecnologia 3

Crittografia quantistica

In ambito di crittografia classica, una delle soluzioni al problema di distribuzione della chiave è rappresentato dalla *crittografia asimmetrica*, che prevede l'utilizzo di due coppie di chiavi (una per il mittente e l'altra per il destinatario). Ciascuna coppia è costituita da una chiave privata e una pubblica (esempio: algoritmo RSA). Nonostante risolva il problema della distribuzione della chiave, la crittografia asimmetrica non è in grado di stabilire se il messaggio è stato intercettato da un'eventuale spia. Inoltre, anche i più sicuri sistemi crittografici attualmente in uso sarebbero vulnerabili in seguito ad attacchi sferrati da computer quantistici, teoricamente possibili e che potrebbero diventare realtà (esempio: D-Wave primo prototipo di calcolatore "quantistico" funzionante).
Qui interviene la **distribuzione quantistica delle chiavi** (in inglese QKD, *Quantum Key Distribution*), chiamata spesso con il termine più generico di crittografia quantistica. La QKD è in grado di:

- *distribuire in modo sicuro la chiave* così da garantire la segretezza del messaggio
- *scoprire se una spia si è interposta tra mittente e destinatario*, per esempio nel caso di attacco Man in the Middle.

Inoltre, solo sistemi crittografici quantistici potrebbero resistere a un eventuale attacco da parte di un computer quantistico.
Tutto ciò grazie alle proprietà dell'informazione quantistica che si basano sulla **sovrapposizione quantistica degli stati**.

Approfondimento
Crittografia quantistica

Laboratorio

Una delle applicazioni più frequenti degli algoritmi di crittografia riguarda la cifratura delle password.
Di seguito vedremo alcuni esempi di applicazione di algoritmi di crittografia delle password e di utilizzo dell'algoritmo RSA sui router Cisco.
È bene ricordare, però, che la crittografia non può:

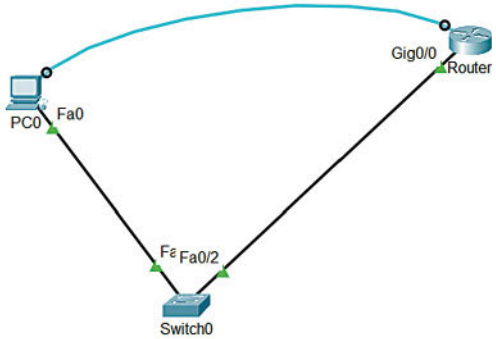
- proteggere un sistema da persone che, non autorizzate, accedono fisicamente alle risorse hardware e software;
- intervenire sui malware impedendo l'alterazione di programmi;
- prevenire e contrastare attacchi DoS che, tramite un bombardamento continuo di richieste, mandano in sovraccarico il sistema;
- impedire un attacco di forza bruta che, provando una moltitudine di chiavi, rilevi quella corretta;
- impedire che un'analisi crittografica del testo sia in grado di interpretare il contenuto del messaggio.

ATTIVITÀ 1

Sicurezza sui router Cisco – Password enable

Scenario

Il corretto funzionamento di un router dipende dalla sua configurazione e dalle sue impostazioni. Tali operazioni sono particolarmente delicate, in quanto un errore, intenzionale o meno, potrebbe compromettere il funzionamento di una rete. Per questo motivo è buona regola impostare una password per accedere alla modalità privilegiata (EXEC MODE) che costituisce il massimo livello di privilegi per fornire le impostazioni del router.
Consideriamo un router a cui è consentito l'accesso via cavo console, o da remoto da PC0.
Sia `10.10.1.1` l'indirizzo IP della porta Gig 0/0 del router, default gateway per PC0.



Consegna

Impostare una password criptata per proteggere l'accesso alla modalità EXEC MODE di un router. La crittografia è effettuata con MD5.

Svolgimento

Passo 1: introduzione
Verifichiamo l'accesso alla modalità exec mode senza password.
Ricordiamo che per entrare in exec mode occorre utilizzare il comando `enable`, dopodiché il prompt appare come #:

```
Router>enable
Router#
```

In questo caso l'accesso alla modalità privilegiata è libero e chiunque potrebbe procedere alla configurazione del router.

Passo 2: impostazione della password in chiaro
Ora impostiamo una password per proteggere l'accesso.
Per fare ciò entriamo in modalità privilegiata, digitiamo il comando `configure terminal`, e impostiamo la password desiderata digitando il comando `enable password`. In questo caso la password è `PswSistemi`.
Successivamente usciamo e rientriamo per verificare che venga richiesta la password.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable password PswSistemi
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#exit
Router>enable
Password: PswSistemi
Router#
```

Con il comando `show run` è possibile vedere le impostazioni di configurazione presenti nella RAM, e notare che la password impostata appare in chiaro.

```
Router#show run
Building configuration...

Current configuration : 715 bytes
...
no service password-encryption
...
enable password PswSistemi
...
```

Passo 3: impostazione della password criptata
Affinché la password sia criptata, rifacciamo tutto il procedimento, ma utilizziamo il comando enable secret; successivamente verifichiamo con il comando `show run`.

```
Router>
Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#enable secret PswSistemi
The enable secret you have chosen is the same as your enable
password.
This is not recommended. Re-enter the enable secret.
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show run
Building configuration...

Current configuration : 762 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
…
enable secret 5 $1$mERr$oEGK6ZZtR2WrnJD5QSJqc/
enable password PswSistemi
!
```

Osserviamo che:

- la password è ora criptata con l'algoritmo di hash MD5 (Cisco IOS type 5) e ciò che viene visualizzato è il digit ottenuto.
- Non avendo rimosso la password precedente, viene visualizzata anche la password in chiaro che, per giunta, è la stessa impostata in modo criptato. In questo modo l'impostazione perde di significato.
- La password criptata avrebbe comunque la precedenza su quella non criptata

Per criptare la password inserita la prima volta, utilizziamo il comando `service password-encryption`, che cripta a posteriori utilizzando un altro algoritmo di cifratura un po' meno sicuro, il cifrario Vigenere (Cisco IOS type 7).

```
Router>
Router>enable
Password: PswSistemi
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show run
..
enable secret 5 $1$mERr$oEGK6ZZtR2WrnJD5QSJqc/
enable password 7 08115F593A101603170605
..
```

ATTIVITÀ 2

Sicurezza sui router Cisco – Protezione delle vie di accesso al router

Scenario

Nell'**Attività 1** abbiamo visto come proteggere l'accesso alla modalità privilegiata di un router. Ora vediamo come proteggere le vie di accesso al router:

- accesso tramite console (accesso fisico tramite un cavo);
- accesso tramite Line VTY 0 15 (accesso da remoto).

Il termine "VTY" sta per Virtual teletype (telescrivente virtuale). VTY è una porta virtuale, a cui non corrisponde un hardware, utilizzata esclusivamente per ottenere l'accesso da un dispositivo esterno al router o switch, tramite i protocolli Telnet o SSH. Le vecchie versioni di IOS supportavano solo 5 linee VTY da 0 a 4, mentre la nuova versione arriva fino a 16 linee VTY (0-15). La configurazione e la gestione delle linee VTY è possibile tramite l'utilizzo dell'interfaccia a riga di comando.

Consegna

Proteggere le via di accesso al router impostando utente e password per accedere sia via console sia dalle linee VTY.

Svolgimento

Passo 1: console
Impostiamo una password per l'accesso via console (`PswConsole`) e impostiamo il tempo massimo di inattività a 5 (espresso in minuti. Il default sarebbe 30).

```
Router(config)#line console 0
Router(config-line)#password PswConsole
Router(config-line)#login
Router(config-line)#exec-timeout 5
```

Proviamo ora l'accesso al router via console da PC1 e entriamo in modalità privilegiata. Ci verrà chiesto di inserire due password: la prima relativa alla linea di console, l'altra relativa al passaggio di stato enable. Le password non sono visibili.

```
User Access Verification

Password: PswConsole

Router>enable
Password: PswSistemi
Router#
```

Passo 2: Line VTY
Passiamo ora a proteggere l'accesso da remoto.
Per accedere in remoto alla CLI di un router (o di uno switch) è necessario utilizzare un terminale (client) che utilizza i protocolli Telnet o SSH.

- **Telnet** è il protocollo TCP/IP standard per eseguire i comandi su un dispositivo remoto. È vulnerabile agli attacchi alla sicurezza perché i dati passano in chiaro.
- **SSH** (***S****ecure* ***S****Hell*) è un protocollo che permette di stabilire una connessione cifrata tramite interfaccia a riga di comando e consente di superare molti problemi relativi alla sicurezza di Telnet.

Iniziamo ad attivare Telnet proteggendo le VTY 0 15 e impostando il tempo di inattività a 30 secondi:

```
Router(config)#line vty 0 15
Router(config-line)#login
% Login disabled on line 132, until 'password' is set
% Login disabled on line 133, until 'password' is set
% Login disabled on line 134, until 'password' is set
% Login disabled on line 135, until 'password' is set
% Login disabled on line 136, until 'password' is set
% Login disabled on line 137, until 'password' is set
% Login disabled on line 138, until 'password' is set
% Login disabled on line 139, until 'password' is set
% Login disabled on line 140, until 'password' is set
% Login disabled on line 141, until 'password' is set
% Login disabled on line 142, until 'password' is set
% Login disabled on line 143, until 'password' is set
% Login disabled on line 144, until 'password' is set
% Login disabled on line 145, until 'password' is set
% Login disabled on line 146, until 'password' is set
% Login disabled on line 147, until 'password' is set
Router(config-line)#password PswVTY
Router(config-line)#exec-timeout 0 30
Router(config-line)#end
```

Proviamo l'accesso da remoto collegandoci da PC0:

```
C:\>telnet 10.10.1.1
Trying 10.10.1.1 ...Open

User Access Verification

Password: PswVTY
Router>
```

Per completare il procedimento di autenticazione da remoto, impostiamo anche uno username per l'accesso alle linee VTY e impostiamo le line affiché sia richiesta l'autenticazione. Infine proviamo il collegamento da PC0:

```
Router(config)#username utente1 secret PswUt1
Router(config)#exit
Router#

Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#no password
Router(config-line)#end

C:\>telnet 10.10.1.1
Trying 10.10.1.1 ...Open
User Access Verification

Username: utente1
Password: PswUt1
Router>
```

ATTIVITÀ 3

Sicurezza sui router Cisco – Abilitare il protocollo SSH

Scenario

In genere l'accesso a un router (o a uno switch) avviene da remoto.
Per accedere in modo sicuro è consigliabile utilizzare un protocollo come SSH (anziché Telnet) che, tramite algoritmo RSA, stabilisce una connessione cifrata.

Consegna

Abilitare il protocollo SSH per l'accesso remoto sicuro a un router.

Svolgimento

Per abilitare SSH su un router Cisco IOS è necessario:

1. Configurare il comando **`hostname`** e un dominio DNS.
2. Generare la chiave SSH.
3. Abilitare il supporto del trasporto SSH per vty.

Passo 1
Per attivare SSH occorre innanzitutto dare al router un nome diverso da quello di default e specificare un dominio DNS.

```
Router(config)#hostname R1
R1(config)#ip domain-name RR
```

Passo 2
Da questi parametri, utilizzando il comando `crypto key generate rsa`, è generata la coppia di chiavi RSA: quella pubblica e quella privata, da usare con SSH. L'esempio seguente mostra i comandi per generare chiavi di lunghezza pari a 2048 bit. Scegliere chiavi più lunghe migliora la sicurezza, perché aumenta esponenzialmente l'insieme dei possibili valori che possono essere generati, nonostante il tempo per crittografare e decrittare un messaggio aumenti.

```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.RR1
Choose the size of the key modulus in the range of 360 to 2048
for your
General Purpose Keys. Choosing a key modulus greater than 512 may
take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
```

Per aumentare il livello di sicurezza impostiamo la versione 2 di SSH:

```
ip ssh version 2
```

Successivamente, possiamo impostare i parametri relativi a SSH, quali:

- l'idle timeout (tempo di inattività trascorso il quale il sistema effettua automaticamente un logout), espresso in secondi è un numero compreso tra 1 e 120.
- Il numero di tentativi di login errati consentiti. È un numero compreso tra 1 e 5.

```
R1(config)#ip ssh time-out 30

R1(config)#ip ssh authentication-retries
```

Proviamo ora l'accesso al router da remoto da PC0 via SSH:

```
C:\>ssh -l utente1 10.10.1.1

Password: PswUt1

R1>
```

Passo 3
Una volta abilitato il protocollo SSH è necessario indicarlo alle interfacce VTY. Il comando `transport input ssh` fa in modo che l'accesso avvenga solo via SSH, impedendo l'accesso via Telnet.

```
R1(config)#line vty 0 15
*Mar 1 7:9:54.316: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config-line)#transport input ssh
R1(config-line)#
```

Passo 4
Utilizzare il comando `show crypto key mypubkey rsa` per visualizzare le chiavi pubbliche generate.

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 7:9:44 UTC marzo 1 1993
Key name: R1.RR1
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00007ac0 00001b0d 00005e58 00004896 00004b6e 0000245c 000042a2 0000444b
000062d3 000031e0 0000453a 0000485b 00000b5a 0000116f 00003569 00007c7d
00004d2a 00006c9d 00001041 00003c07 00005e92 00000790 00001426 6b61
% Key pair was generated at: 7:9:44 UTC marzo 1 1993
Key name: R1.RR1.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
000073aa 00006210 00002d8d 000041ba 00003137 00006ede 00002102 00005afb
000046d0 00005547 00001670 000025f9 0000743f 000070f8 0000699d 000002ef
00007e2a 00000414 000063f4 0000262b 000055f3 00004f84 00004387 1307
R1#
```

Passo 5
Proviamo ora il collegamento da remoto da PC0 prima via Telnet (e non andrà a buon fine) poi via SSH:

```
C:\>telnet 10.10.1.1
Trying 10.10.1.1 ...Open
[Connection to 10.10.1.1 closed by foreign host]

C:\>ssh -l utente1 10.10.1.1
Password: PswUt1
R1>logout

[Connection to 10.10.1.1 closed by foreign host]
C:\>
```

Il procedimento è analogo se fatto con connessione diretta via console.

ATTIVITÀ 4
Cifratura delle password su un database

Scenario

È buona norma aumentare il livello di sicurezza delle nostre applicazioni, evitando di memorizzare le password in chiaro nel database, criptandole utilizzando un algoritmo di hash.

Consegna

Scrivere un frammento di codice PHP per la gestione della password criptata in fase di registrazione e login di un utente tramite form.
Per la registrazione, il server riceve la password, la cripta e poi la scrive nel database.
Per il login il server riceve la password, la cripta e la confronta con quella precedentemente scritta nel database.

Svolgimento

Vediamo ora un frammento di codice PHP per la gestione delle password.

```
$password = 'M1aPassW0rd';
$hash = md5($password); // f998920e95576dedaefd8ec2e6f83661
$hash = sha1($password); // 7f00c6446c9a7aa7cd182060a47ea66bea83984b
```

Per aumentare il livello di sicurezza è possibile combinare tra loro, anche più volte, gli algoritmi MD% e SHA. Per esempio:

```
$password = 'M1aPassW0rd';
$hash = md5(md5($password);
$hash = md5(sha1($password);
```

Oppure combinare un ***salt*** alla password, cioè una stringa di caratteri casuali che aumenta la complessità.

```
$password = 'M1aPassW0rd';
$salt = '1xc5)7#3';
$hash = md5($password . $salt);
```

Passo 1: registrazione
In fase di registrazione il server riceve la password, la cripta e la inserisce nel database.

```
<?php
$password=$ _ POST[‘password’];
$passwordCript=md5(sha1($password));
< inserimento password criptata nella tabella>
?>
```

Passo 2: login
In fase di autenticazione, il server:

- riceve dal client username e password;
- accede al database con username e preleva la password (con l’istruzione `sql select`);
- cripta la password ricevuta e la confronta con quella letta dal database.

```
<?php
$userLogin=$ _ POST['user'];
$passwordLogin=$ _ POST['password'];

< estrai dal db la password relativa allo user ricevuto e assegna
valore letto a $passwordCript
select password from users where users=$userLogin;>

if($passwordCript == md5(sha1($passwordLogin)) ) {
    echo "Accesso effettuato con successo";
} else {
    echo "La password inserita non è corretta";
}
```

SINTESI

CRITTOGRAFIA E AUTENTICAZIONE
Tecniche utilizzate in ambito cybersecurity

CRITTOGRAFIA
Tecnica utilizzata per crittografare dei dati: utilizzando un algoritmo e una chiave i dati sono codificati. L'algoritmo è pubblico e noto a chiunque, ma solo chi conosce la chiave è in grado di decodificare i dati.

A CHIAVE SIMMETRICA
Gli algoritmi a chiave simmetrica utilizzano la stessa chiave per criptare e per decriptare il messaggio.
È garantita la riservatezza dei dati.
Criticità: lo scambio della chiave

A CHIAVE ASIMMETRICA
Ogni soggetto ha una **coppia di chiavi**: una **pubblica** che può e deve essere diffusa, e una **privata**.
La coppia di chiavi è calcolata con un opportuno algoritmo.

ALGORITMI A CHIAVE SIMMETRICA
- DES: Utilizza una chiave a 64 bit (di cui 8 sono di controllo).
- 3DES: Usa tre chiavi e tre successive esecuzioni di DES. La lunghezza della chiave è di 168 bit.
- AES sostituto di 3DES per la sua efficienza. Opera con blocchi a 128 bit e chiavi a 128, 192 e 256 bit

ALGORITMI A CHIAVE ASIMMETRICA
RSA è il più diffuso.
È basato sulle proprietà dei numeri primi.
Garantisce riservatezza e autenticazione.

AUTENTICAZIONE
Il processo di verifica e controllo che un soggetto identificato sia veramente chi dice di essere.

CERTIFICATI DIGITALI
Documenti emessi da un'affidabile autorità di certificazione (CA) che assicura l'autenticazione della chiave pubblica. Confermano che una chiave appartiene veramente al suo proprietario.

MULTI-FATTORI
I fattori utilizzati per l'autenticazione rientrano nelle categorie: "sei", "hai", "sai".
- Autenticazione debole: utilizza uno solo dei fattori.
- Autenticazione forte: è multi-fattore (MFA) e combina due (2FA) o tre (3FA) fattori.

FUNZIONI DI HASH
Trasformano una stringa di lunghezza arbitraria in una stringa di lunghezza fissa chiamata digest. Hanno due proprietà:
- sono **non invertibili**, che significa che dalla stringa ottenuta non è possibile ricostruire la stringa di partenza;
- **ogni stringa di input dà luogo a un'unica stringa di output** che rappresenta una sorta di "impronta digitale" dell'input. Due input diversi non possono avere lo stesso digest.

Sono utilizzate per garantire l'integrità del dato di input. Algoritmi utilizzati: MD5, SHA (SHA-1, SHA-2 e le sue varianti SHA-256 e SHA-512) e altri.

FIRMA DIGITALE
Consente di sottoscrivere digitalmente documenti con valore legale. È una firma elettronica qualificata basata sulla crittografia a chiave asimmetrica. Utilizzando l'algoritmo RSA e le funzioni di hash, garantisce l'autenticazione, l'integrità e la non ripudiabilità del documento.

CON PASSWORD
Metodo più comune di autenticazione, utilizzato con USERID.
- Lo userid identifica un utente
- La password verifica che l'utente sia chi dice di essere.

SENZA PASSWORD
Passwordless Authentication è un metodo di autenticazione che non utilizza la password, evitando così tutti i rischi e le debolezze legate a un uso scorretto delle password.

SINGLE SIGN-ON (SSO)
Consente di accedere a più servizi in rete, autenticandosi una sola volta

Verifica delle CONOSCENZE

Vero o Falso?

1 La crittografia garantisce la segretezza ma non l'affidabilità dei dati. V F

2 Un algoritmo di crittografia a chiave pubblica garantisce la segretezza e l'integrità dei dati, mentre quello a chiave privata no. V F

3 RSA è un algoritmo di crittografia a chiave pubblica. V F

4 Un certificato digitale serve a certificare una firma. V F

5 La Firma Digitale è un'immagine digitale di una firma. V F

6 La crittografia a chiave simmetrica è meno complessa di una crittografia a chiave asimmetrica. V F

7 La chiave di sessione è scambiata tramite una chiave simmetrica. V F

8 Per garantire la segretezza il mittente cripta con la sua chiave privata. V F

9 Per garantire l'integrità il mittente cripta con la sua chiave privata. V F

10 Il digest è un riassunto del messaggio. V F

11 Il nome utente serve per l'identificazione, la password per l'autenticazione. V F

12 L'impronta digitale è considerata autenticazione forte. V F

13 SHA-256 deve avere un input di lunghezza massima 256 byte. V F

14 SHA produce un message digest di lunghezza fissa, partendo da un messaggio di lunghezza variabile. V F

15 AAA significa: Authentication, Authorization, Accounting. V F

16 SAML è utilizzato per il Single Sign-On. V F

17 L'autenticazione a più fattori non può utilizzare la password come uno dei fattori. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

18 Per garantire la riservatezza:

a si cripta con la chiave privata e si decripta con la chiave pubblica
b si cripta con la chiave pubblica e si decripta con la chiave privata
c si cripta con la chiave pubblica e si decripta con la chiave di sessione
d si utilizza un certificato digitale

19 La crittografia a chiave simmetrica:

a è più veloce della crittografia a chiave asimmetrica, ma meno sicura
b è più sicura della crittografia a chiave asimmetrica, ma meno veloce
c è usata per la Firma Digitale
d garantisce il non ripudio

20 Nella crittografia:

a l'algoritmo è noto, la chiave è segreta
b la chiave è nota, l'algoritmo è segreto
c sia la chiave sia l'algoritmo sono noti
d sia la chiave sia l'algoritmo sono segreti

21 RSA è un:

a algoritmo di crittografia a chiave simmetrica
b algoritmo di crittografia a chiave asimmetrica
c protocollo di comunicazione
d standard di rete

22 La Firma Digitale:

a usa la crittografia a chiave asimmetrica
b è comoda perché evita all'utente di scrivere
c è una fotografia della firma dell'utente
d garantisce la segretezza del messaggio

Domande per la prova orale

23 Cos'è la crittografia? In che contesti si utilizza la crittografia asimmetrica a chiave pubblica?

24 Quali sono le tecniche di autenticazione degli utenti?

25 Che cosa significa "crittografare"?

26 Esponi il funzionamento della crittografia a chiave simmetrica.

27 Esponi il funzionamento della crittografia a chiave pubblica.

28 Che cosa significa "autenticazione" nell'ambito della sicurezza informatica?

29 Quali sono i tre fattori di un'autenticazione forte?

30 Che cos'è la Firma Digitale?

31 Come è fatto 'algoritmo alla base della Firma Digitale?

32 Che cosa sono e a che cosa servono le funzioni di hash?

33 Completa la tabella.

	Che cos'è	Quali problemi risolve	Algoritmi usati
Firma Digitale	.....	.....	.....
Certificato digitale	.....	.....	.....

34 Quando ci registriamo a un servizio web, ci viene chiesto di inserire una password e in genere il servizio ci indica il livello di sicurezza della password che stiamo scegliendo. Crea una password per un servizio web a tua scelta ottenendo un livello di sicurezza debole, medio, sicuro. Confronta le password tra loro argomentando i risultati ottenuti. Sintetizza i risultati in una tabella

Livello	Password	Motivazioni
Debole	.....	.....
Medio	.....	.....
Sicuro	.....	.....

Conclusioni: .....

35 Dopo aver generato una password di livello di sicurezza alto, utilizza gli algoritmi di hash MD5, SHA-256 e SHA-512 per ottenere il digit. Riporta i dati ottenuti in una tabella
Password in chiaro: .....

	Digit
MD5	.....
SHA-256	.....
SHA-512	.....

37 Esponi un caso, tratto dalla tua esperienza, di utilizzo dei seguenti metodi di autenticazione. Sintetizza i risultati ottenuti nella tabella.

Metodo di autenticazione	Descrizione	Servizio utilizzato
Debole (1 fattore)	.....	.....
A due fattori	.....	.....
Senza password	.....	.....
Single Sign-on	.....	.....

38 Effettua una ricerca sul Web per trovare organizzazioni in grado di fornire il servizio di Firma Digitale. Riassumi in tabella i risultati della ricerca.

Organizzazione	Servizio offerto (descrizione)	Modalità di fruizione	Costo
.....	.....	.....	.....
.....	.....	.....	.....



Esercizi in più

Encryption and Authentication

Abstract

Transmission of data over a network sets specific issues related to confidentiality, integrity and authentication. Encryption solves these problems. There are two encryption techniques: public key and private key. In both cases, the encryption algorithm is public and what varies is the management of the key used for encryption/decryption. A private key encryption algorithm requires that the sender and receiver use the same secret key with which the sender encrypts the message and the recipient decrypts it. This, however, raises the issue of exchanging the key through a secure channel. Public key algorithms solve this problem: the key is formed by a pair constituted by a public key (known to everybody), and a private key (known only to the owner). The sender encrypts with the public key of the recipient, the recipient decrypts with its private key. Given that even by encrypting with private key and decrypting with public key one can get the original message, this method is also used for the realization of the digital signature, in which the sender encrypts with its private key and the recipient decrypts with its public key. This method ensures the sender's authentication, data integrity (as only a digest of the message obtained using hash functions is encrypted) and non-repudiation. Network protocols are typically based on these techniques and generally use a session key: a private key is securely exchanged using an asymmetric key, and then the symmetric key is used for the entire session.

Questions

Answer all questions

1 What is the problem with symmetric key algorithms?

2 What do we mean by public key and private key?

3 What is the use of a digital signature?

4 What is a session key?

Choose the correct answer

5 Digital signature
- a is a type of authentication
- b requires a tablet
- c has no legal value
- d must always be accompanied by a paper document

6 The private key:
- a is known to the recipient of a message
- b is known to the sender of a message
- c is known to both recipient and sender
- d is not known to either of them

7 A digest is used
- a to authenticate a session key
- b to guarantee the message integrity
- c in symmetric-key algorithms
- d to shorten the message

8 The SSO authentication method
- a is used to authenticate a document
- b is used to authenticate once to access multiple services
- c is an encryption algorithm
- d does not use passwords

Crosswords

Across

1 Utilizes multiple authentication factors

4 Protocol for Single Sign On

6 Symmetric key encryption algorithm

7 Temporary code used in multi-factor authentication

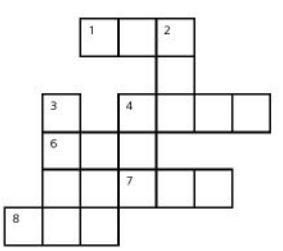
8 Hash algorithm

Down

2 Set of protocols used to control access to a network

3 Family of functions used to ensure data integrity

4 Authentication method for multiple services

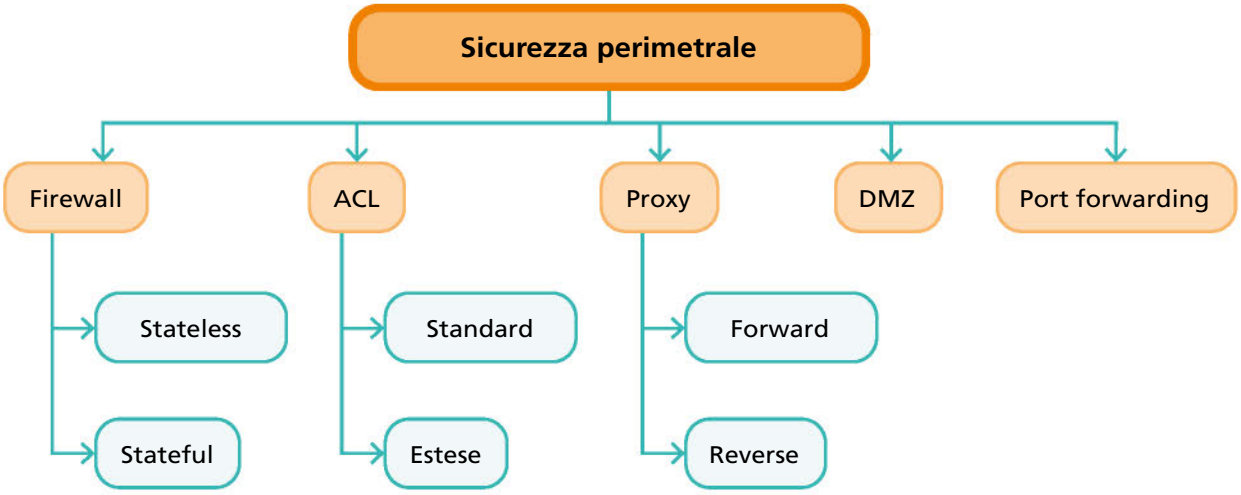




Unità

5

La sicurezza perimetrale



Visione d'insieme

- Come difendere una LAN e controllare gli accessi.
- Elementi base della sicurezza perimetrale.
- Firewall, ACL, Proxy e DMZ.

1 Introduzione



«Come ci inerpicavamo per il sentiero scosceso che si snodava intorno al monte, vidi l'abbazia. Era questa una costruzione ottagonale i cui lati meridionali si ergevano sul pianoro dell'abbazia, mentre quelli settentrionali sembravano crescere dalle falde stesse del monte, su cui si innervavano a strapiombo. Dico che in certi punti, dal basso, sembrava che la roccia si prolungasse verso il cielo, senza soluzione di tinte e di materia, e diventasse a un certo punto mastio e torrione. Per la posizione inaccessibile era capace di generare timore nel viaggiatore che vi si avvicinasse a poco a poco. E fortuna che, essendo una limpidissima mattinata invernale, la costruzione non mi apparve quale la si vede nei giorni di tempesta.»

Umberto Eco, *Il nome della Rosa*, Bompiani

↑ **Fig. 1** le misure di sicurezza moderne sono simili alle strategie difensive del passato, dove il "perimetro" era protetto da mura robuste per prevenire intrusioni e attacchi.

Le mura che circondano l'abbazia medievale (Figura 1) offrono un'ottima rappresentazione di ciò che si intende per **difesa perimetrale di una rete**: un insieme di misure di protezione messe in atto per difendere il "perimetro" di una rete aziendale da potenziali attacchi informatici.
La **sicurezza perimetrale protegge il confine tra una rete privata e la rete pubblica**, con l'obiettivo principale di prevenire l'accesso non autorizzato ai dati della rete privata. Questo tipo di sicurezza implementa misure preventive per contrastare sia minacce "fisiche", come catastrofi naturali o danneggiamenti volontari a sistemi (ambienti, reti, dispositivi), sia minacce "logiche", legate ad attività software quali attacchi informatici, malware, virus e interruzioni del servizio.
Per le **minacce fisiche** si ricorre a soluzioni come porte blindate, sistemi di videosorveglianza, controllo degli accessi e sistemi di ridondanza.
Per le **minacce logiche** si risponde con strategie e politiche che includono l'uso di **firewall**, software **antimalware**, sistemi di **rilevamento delle intrusioni**, con l'obiettivo principale di proteggere i dispositivi e le risorse di rete. In particolare i firewall sono dispositivi che analizzano i pacchetti in transito, li aprono ed esaminano il loro contenuto. Se il contenuto è ritenuto sospetto, i pacchetti sono respinti. Questo è un aspetto fondamentale della sicurezza perimetrale che esamineremo in questa unità.

Pit Stop

1 Che cosa si intende per sicurezza perimetrale?

2 Proteggere la rete

Per mitigare gli attacchi di rete, è fondamentale adottare una strategia di sicurezza che protegga i dispositivi, tra cui router, switch, server. Spesso ci si basa su un approccio noto come "defense-in-depth", che utilizza diversi strati di protezione. Questi strati coinvolgono dispositivi di rete (Figura 2) e servizi che lavorano insieme per difendersi dagli attacchi.

- **Firewall**: lavorano al livello di sicurezza della rete. Sono dispositivi che separano le reti interne da quelle esterne. In particolare, i firewall **stateful** analizzano il traffico in base allo stato delle connessioni, permettono di bloccare pacchetti indesiderati e riconoscono attacchi come il Denial of Service (DoS).
- **Intrusion Prevention System** (**IPS**): è un dispositivo che a livello di rete monitora il traffico per:

  - **rilevare** attività dannose o sospette, utilizzando diversi metodi, tra cui la firma dell'attacco, l'analisi del comportamento e l'ispezione approfondita dei pacchetti di rete;
  - **prevenire** l'attacco adottando contromisure come il blocco del traffico;
  - **registrare** le informazioni sugli eventi di sicurezza rilevati che possono essere utilizzate per analizzare l'attacco e studiarne le conseguenze;
- – **segmentare**, la rete per separare aree diverse della rete. Questo può essere realizzato suddividendo la rete in più segmenti che separano, ad esempio, i server dai client e da altri dispositivi (come stampanti, telefoni VoIP e dispositivi wireless). Questo può essere realizzato introducendo le Virtual LAN e aree pubbliche separate dalla rete interna (DMZ - *DeMilitarized Zone*).
- **Protezione delle e-mail e delle applicazioni Web**: lavora a livello di sicurezza delle applicazioni. È realizzata con dispositivi hardware e software come **WAF** (**W***eb* **A***pplication* **F***irewall*), per proteggere i servizi web "interni" dalle minacce esterne come malware, phishing, spam e accesso a contenuti dannosi.
- **Autenticazione**, **Autorizzazione** e **Contabilità** (**AAA**). Un server AAA è utilizzato a livello utente per applicare le politiche di sicurezza che gestiscono l'accesso.

I servizi di sicurezza comprendono:

- software antivirus e antimalware per proteggere i dispositivi;
- configurazione attenta di router e switch con password robuste;
- aggiornamenti regolari e backup dei dati.

Nelle sezioni successive, esploreremo in dettaglio alcuni degli elementi chiave che abbiamo introdotto.

notabene

La sicurezza perimetrale rappresenta solo uno degli aspetti della sicurezza complessiva di una rete. Gli utenti possono essere il punto debole nella catena di sicurezza, è quindi necessario sensibilizzarli riguardo alle minacce informatiche per ridurre il rischio di attacchi di tipo social engineering o phishing.

Pit Stop

2 Elenca le principali soluzioni utilizzate per far fronte al problema della sicurezza perimetrale.

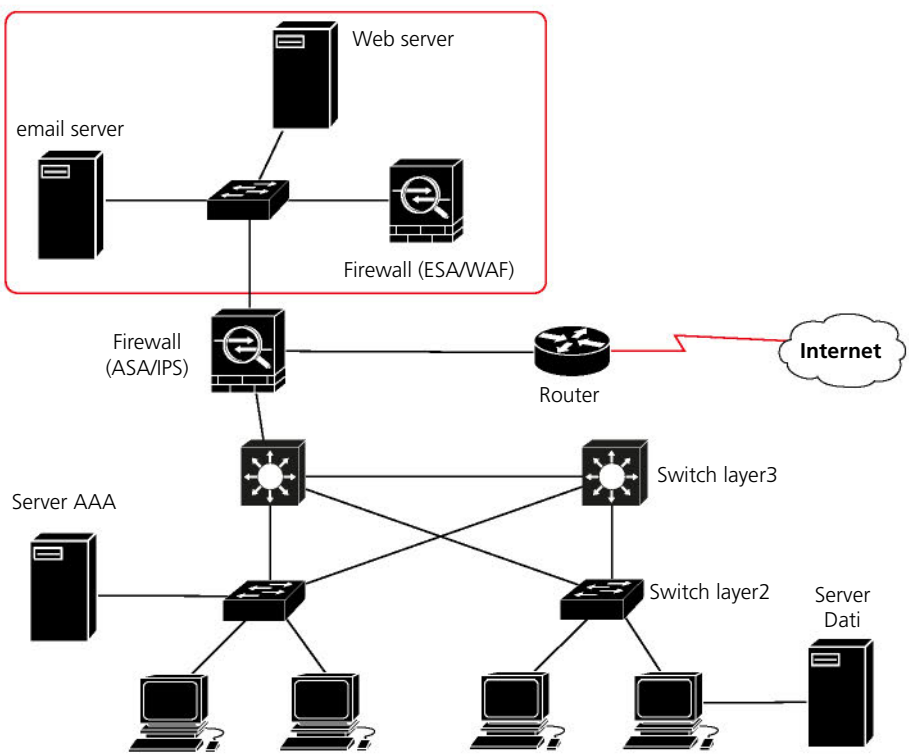


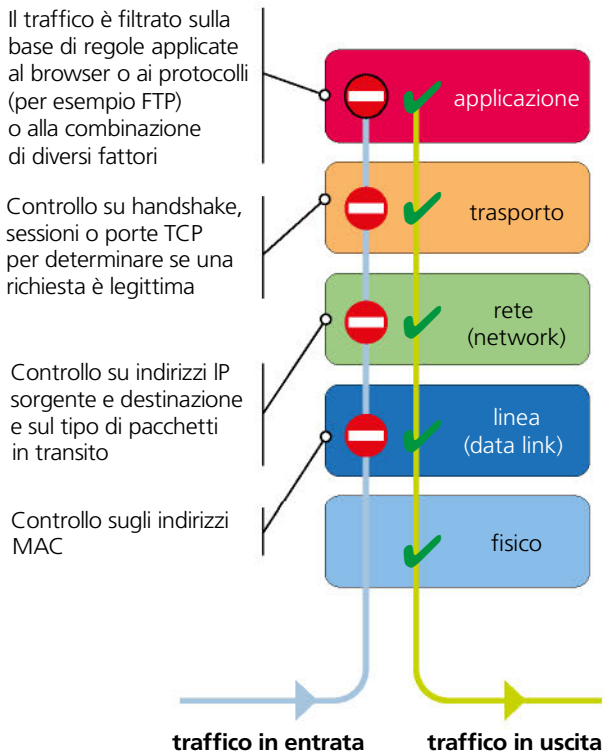
Fig. 2 Uno schema di principio con i componenti principali della sicurezza: Firewall (ASA, *Adaptive Security Appliance* e IPS, *Intrusion Prevention System*), ESA (*Email Security Appliance*) e WAF (*Web Application Firewall*) per proteggere e-mail e navigazione nel Web. La rete prevede anche switch di ridondanza per aumentare l'affidabilità.

Comprendi con l'analogia

Il varco (il controllo degli accessi)



È arrivato il giorno del colloquio presso la grande azienda a cui aspiravo. Mi dirigo verso l'ingresso e raggiungo l'area riservata ai controlli di sicurezza. Vengo fermato dal personale della security che mi chiede la carta di identità e il motivo della visita. Digita il mio nome sul terminale e controlla se il mio nome è nella lista delle persone attese. Mi chiede se sono in possesso di un tablet o di un laptop e verifica che io abbia l'autorizzazione necessaria a portarlo con me. Infine mi informa che potrò accedere al solo settore "Risorse Umane" e non avrò la possibilità di scattare fotografie. Mi fa firmare la policy di sicurezza interna e mi consegna un badge con cui passare il varco.
Il compito della guardia è quello di controllare l'accesso all'edificio, sia in entrata sia in uscita, permettendo l'ingresso solo alle persone i cui nomi compaiono nella lista.



↑ **Fig. 3** Il filtro del traffico può avvenire a livello di Rete, Trasporto o Applicazione.

3 I firewall

Un firewall, "**muro tagliafuoco**", è un dispositivo che costituisce la prima linea di difesa per la sicurezza della rete. Come un muro tagliafuoco impedisce la diffusione di un incendio, un firewall impedisce la diffusione di attività dannose su una rete. Agisce da barriera tra le reti interne, sicure e controllate, e le reti esterne che possono essere inaffidabili. Permette di applicare regole di sicurezza per monitorare il traffico in entrata e in uscita o bloccare minacce e attacchi.
Un aspetto fondamentale dei firewall è la loro capacità di operare a diversi livelli del modello TCP/IP (Figura 3):

- **Livello data-link**: controllo degli indirizzi delle trame, in particolare gli indirizzi MAC.
- **Livello rete e trasporto**: verifica dei campi di intestazione dei protocolli, tra cui indirizzi IP, porte di TCP e UDP.
- **Livello applicazione**: analisi e interventi su protocolli e dati, utilizzando "black list" per impedire l'accesso a siti indesiderati.

Un **firewall** può essere:

- Un **apparato autonomo**: un dispositivo dedicato che filtra il traffico di rete.
- Una **funzionalità di un router**: possono controllare il passaggio dei pacchetti attraverso le loro interfacce.
- Un **computer con software dedicato**: viene configurato come firewall con un software specifico per gestire il filtraggio del traffico. Deve avere almeno due schede di rete: una per la rete interna e una per quella esterna.
- Un **firewall personale** realizzato con applicazioni installate sui dispositivi degli utenti. Filtrano i pacchetti in entrata e in uscita, basandosi su politiche di sicurezza. A differenza dei firewall convenzionali, non proteggono l'intera rete (Figura 4).

Pit Stop

3 Dove si colloca un firewall?



↑ **Fig. 4** Windows Defender Firewall filtra il traffico di rete in entrata e in uscita dal dispositivo (in questo caso un PC) bloccando pacchetti indesiderati.

È importante ricordare che i router e i firewall hanno obiettivi diversi: i router gestiscono il traffico di rete, mentre i firewall si concentrano sulla sicurezza, filtrando e proteggendo la rete da minacce esterne, come specificato nella **Tabella 1**.

	Router	Firewall
obiettivo	• Nascono per **consentire il traffico** tra le reti ("facilitatori") e applicano semplici regole di sicurezza. • Dispositivi di sicurezza di rete.	• Nascono per **impedire il traffico dannoso** tra le reti ("controllori"). • Offrono soluzioni di sicurezza più completa e avanzata rispetto ai router.
livelli del modello TCP/IP	• Operano **a livello Rete** e l'ispezione è fatta sui pacchetti IP (e al massimo sulle porte).	• Operano a **diversi livelli** (dal Data Link all'Applicazione).
Principi di funzionamento	• **Stateless**: esaminano i valori in ogni pacchetto individualmente, senza "ricordarsi" dei pacchetti precedenti.	• **Stateful**: controllano il flusso in transito "ricordandosi" dei dati che erano presenti nei pacchetti precedenti.

← **Tab. 1** Compiti di router e firewall.

Firewall che filtrano i pacchetti

I firewall appartengono a due categorie:

- **Packet filtering – stateless**: sono i firewall di prima generazione che agiscono applicando le regole di filtraggio su indirizzi di rete e porte per bloccare o accettare i pacchetti. Il filtro agisce a due livelli:
  – **Livello rete**: il controllo è effettuato sugli indirizzi mittente/destinatario presenti nell'intestazione dei pacchetti. Per esempio, è possibile controllare l'indirizzo IP del mittente per far passare solo i pacchetti che provengono da uno specifico nodo.

Pit Stop

4 Che cosa sono i firewall packet filtering?

5 Che cosa sono i firewall Stateful Packet Inspection?

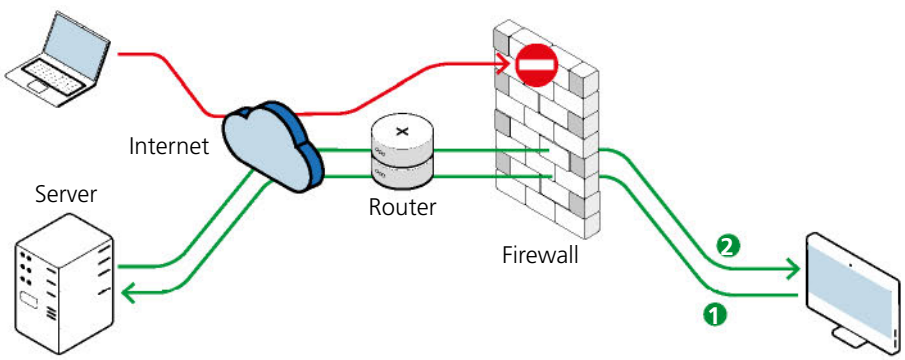
– **Livello trasporto**: il controllo è effettuato sulle porte presenti nell'intestazione di un segmento TCP/UDP. In base alle regole possono, per esempio, entrare solo segmenti che chiedono la connessione (controllo sul flag SYN e ACK) a una determinata porta o possono essere bloccate richieste di connessione a una porta in uscita. Questi filtri sono semplici da applicare, ma sono poco sicuri, perché non tengono conto dello stato della comunicazione e, per questo, sono vulnerabili ad attacchi di spoofing.

- **Stateful Packet Inspection** (**Circuit-Level Gateway**): sono firewall di seconda generazione che operano come i precedenti, ma **mantengono memoria delle sessioni aperte** tra due dispositivi, ricordando l'indirizzo IP e il numero di porta utilizzati per lo scambio dei dati. Inoltre, prendono in considerazione i valori del sequence number e dell'acknowledgement number, e i flag (ACK, SYN, FIN) di TCP per determinare lo stato della connessione. Vengono accettate solo le combinazioni di indirizzi IP e numeri di porta relativi alle connessioni esplicitamente iniziate e volute da sistemi interni alla rete, rifiutando tutte le altre. In questo modo, i soli pacchetti accettati dall'esterno sono quelli che rispondono a richieste fatte da host interni; tutti gli altri vengono bloccati. Ad esempio, se un client interno alla LAN apre una connessione Telnet verso un server su Internet, viene consentito il transito solo della risposta generata dal server, mentre tutto il resto del traffico proveniente dall'esterno viene bloccato (vedi **Figura 5**). Questi tipi di firewall operano fino al livello di trasporto e possono essere vulnerabili ad attacchi DoS che tentano di sovraccaricare il firewall con richieste false, riempiendo la sua memoria.

Firewall di ultima generazione e apparati per la gestione unificata delle minacce

I firewall di ultima generazione (**NGFW - N***ext* **G***eneration* **F***irewall*) rappresentano l'evoluzione dei sistemi di sicurezza di rete, offrendo protezione avanzata contro le minacce informatiche. Questi dispositivi combinano le funzionalità di un firewall tradizionale con strumenti di prevenzione delle intrusioni e altre tecniche di sicurezza per fornire una difesa migliore. In particolare, un firewall di questo tipo ha almeno le seguenti caratteristiche.

- **Prevenzione delle intrusioni**. Includono sistemi **IPS** (**I***ntrusion* **P***revention* **S***ystem*) che analizzano il traffico di rete per rilevare e bloccare gli attacchi prima che raggiungano i dispositivi interni.
- **Controllo delle applicazioni**. Identificano e bloccano il traffico di applicazioni potenzialmente pericolose o non autorizzate.
- **Gestione delle identità**. Integrano la gestione delle identità degli utenti, associando il traffico di rete agli indirizzi IP o MAC specifici.



➜ **Fig. 5** Stateful Packet Inspection Firewall: il traffico è consentito ai soli datagrammi Telnet che fanno parte della stessa sessione iniziata dall'host interno (1 e 2). Qualsiasi altro tentativo di accesso è bloccato.

- **Firewall per applicazioni Web** (**WAF**). Proteggono le applicazioni web da attacchi come SQL injection e XSS.
- **Analisi intelligente del traffico**. Utilizzano la correlazione degli eventi e l'analisi del contesto per una risposta tempestiva agli attacchi.
- **Monitoraggio del traffico**. Eseguono un monitoraggio costante per rilevare attività sospette e comportamenti anomali.
- **Aggiornamenti continui**. Ricevono aggiornamenti regolari per contrastare le minacce emergenti e le nuove tecniche di attacco

Un apparato **UTM** (**U***nified* **T***hreat* **M***anagement*, Gestione unificata delle minacce) integra diverse funzioni di sicurezza in un'unica soluzione, offrendo un pannello di controllo (dashboard) per centralizzare e semplificare la gestione delle funzioni.

- **Protezione antivirus**, **antimalware e anti-spam** per proteggere la rete da virus e malware come ransomware, spyware e trojan e rilevare e neutralizzare comunicazioni indesiderate.
- **Prevenzione della Perdita di Dati** (**DLP**), che fornisce strumenti per impedire che informazioni sensibili, come i numeri delle carte di credito, vengano divulgate, sia accidentalmente che intenzionalmente, al di fuori dell'organizzazione. Un sistema DLP sfrutta software antivirus, Intelligenza Artificiale e apprendimento automatico per esaminare i contenuti e identificare comportamenti anomali. In alcuni casi i dati sensibili possono essere criptati per renderli inaccessibili in caso di intercettazione.
- **IPS** (**I***ntrusion* **P***revention* **S***ystem*), che rileva e previene le minacce alla sicurezza in tempo reale.
- **Web Filtering**, che blocca l'accesso a siti web dannosi o inappropriati.
- **Servizi Integrati**, che comprendono servizi di routing, NAT e VPN per consentire connessioni sicure e private su Internet.

La Figura 6a illustra le funzioni principali di un firewall UTM sotto forma di livelli sovrapposti. La Figura 6b illustra, a titolo di esempio, il pannello posteriore di un firewall FortiGate 100E di Fortinet con le varie porte dei diversi servizi. Entrambi i sistemi sono progettati per operare in tempo reale e sono spesso dotati di sistemi operativi dedicati che girano su hardware con processori specializzati.

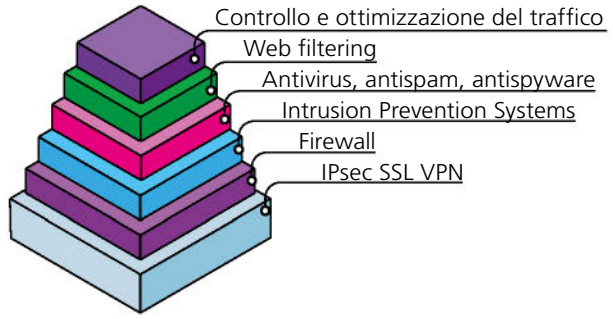
notabene

Cross-site scripting (XSS) è una vulnerabilità che consente a un attaccante di iniettare codice malevolo (spesso un codice JavaScript) all'interno di pagine web per reindirizzare l'utente verso pagine compromesse o eseguire operazioni dannose.

notabene

I firewall di fascia alta come F5 BIG-IP Advanced Firewall Manager utilizzano l'apprendimento automatico (vedi Approfondimento) per rilevare attività anomale, decifrare il traffico TSL, ispezionare tutte le connessioni in entrata e in uscita. Una caratteristica particolare di F5 è la creazione di firme che specificano l'origine della minaccia e che vengono create in tempo reale.

a



b



Porte: **1.** USB port **2.** Console port **3.** DMZ port **4.** WAN port **5.** High availability (HA) port **6.** Gigabit Ethernet (GE) port **7.** GE Shared Media pairs

Fig. 6 a. Lo stack delle funzioni principali di un firewall UTM - Unified Threat Management; **b.** Il pannello di un firewall FortiGate 100E di Fortinet, un sistema di sicurezza che integra diverse funzioni (IPS, Antivirus, Antimalware, Web Filtering, VPN).

notabene

Le ACL non si limitano alla sicurezza perimetrale. Vengono utilizzate anche per controllare una risorsa software, come nei sistemi operativi, per determinare i permessi di lettura e scrittura di file e cartelle.

4 ACL

Che cosa sono le ACL

Una **ACL** (**A***ccess* **C***ontrol* **L***ist*, Lista di controllo degli accessi) è un elenco di autorizzazioni utilizzate per controllare il traffico in ingresso e in uscita da una rete. Queste autorizzazioni determinano chi può accedere a determinati servizi di rete e in che modo. Quando una lista ACL è configurata su un'interfaccia di un firewall o di un router, il dispositivo analizza i dati che passano attraverso l'interfaccia, li confronta con i criteri presenti nell'ACL e ne vieta o consente il passaggio, proprio come il ponte levatoio di un castello medioevale si apriva solo dopo aver controllato che aspettava al di là del fossato.
Esistono due tipi di ACL (Tabella 2 e Figura 7):

- **ACL Standard**. Queste liste contengono le regole per filtrare il traffico solo sulla base dell'indirizzo IP sorgente dei pacchetti in arrivo.
- **ACL Estese**. Queste liste forniscono un controllo più approfondito del traffico di rete. Possono considerare vari criteri, come l'indirizzo IP di origine e di destinazione e il numero di porta.

Pit Stop

6 Che cosa è una ACL?

ACL	Numeriche (numbered)	Con nome (named)
Standard	Numerate da 1 a 99 e da 1330 a 1999.	Identificate da un nome.
	Filtrano il traffico basandosi solo sugli indirizzi IP sorgente. Vengono utilizzate per consentire o impedire il traffico proveniente da un terminale o da una rete.	
Estesa (*extended*)	Numerate da 100 a 199 e da 2000 a 2699.	Identificate da un nome.
	Filtrano il traffico basandosi sugli indirizzi IP sorgente e destinazione. Inoltre filtrano le porte sorgente e destinazione dei protocolli TCP e UDP, i flag e i messaggi del protocollo ICMP.	

→ **Tab. 2** ACL Standard ed Estesa, numeriche e con nome.

Comprendi con l'analogia

Il firewall e le ACL sono come il ponte levatoio di un castello medioevale



In un castello medioevale il fossato separa i "buoni", che stanno all'interno del castello, dai "cattivi" che devono essere lasciati fuori: il ponte levatoio si abbassa solo per lasciare passare gli amici che entrano o escono. I firewall e i router, che applicano le regole per i controlli degli accessi (ACL), controllano il traffico in entrata o in uscita dalla LAN, consentendo il passaggio solo al traffico autorizzato. Esiste però una differenza concettuale. Nel caso del router, per sua natura un "facilitatore" della comunicazione, i soldati che stanno di guardia alla porta sollevano il ponte levatoio solo se all'ingresso è presente un nemico o, in generale, colui che non ha i requisiti richiesti ("stateless inspection"). La natura del firewall è diversa, più somigliante alla porta fortificata di un castello sotto assedio. È tenuta ben chiusa e strettamente sorvegliata. Il ponte levatoio è mantenuto sollevato. È abbassato solo per far passare residenti e alleati. Se un carro attraversa il varco dal castello per uscire a far rifornimento, ne viene accuratamente presa nota in modo tale che, al suo ritorno, possa essere riconosciuto come amico e fatto passare ("stateful inspection").

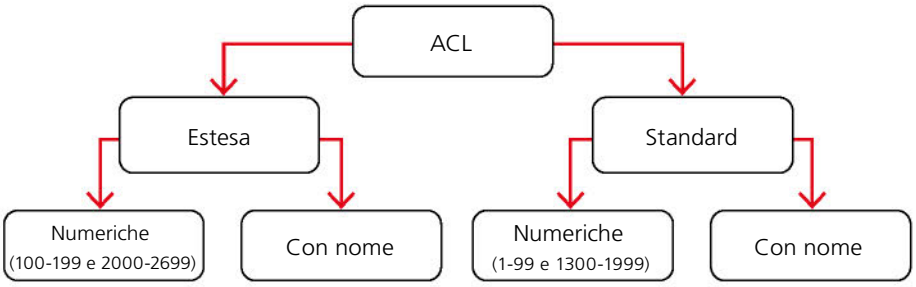


Fig. 7 ACL: standard ed estesa (*extended*). La prima modalità è la meno recente e limitata al controllo dell'indirizzo IP sorgente dei pacchetti. La modalità ACL extended è la più completa. I pacchetti sono filtrati applicando diversi criteri: indirizzo IP sorgente e destinazione, porte TCP/UDP, tipo di protocollo, ecc.

Come funzionano le ACL

Una ACL stabilisce quali pacchetti possono entrare o uscire da una rete. Quando un pacchetto arriva all'interfaccia di un firewall o di un router, viene ispezionato per individuare alcune informazioni, come indirizzi IP e porte, che, se presenti nella lista di controllo, possono determinare il passaggio del pacchetto (**permit**), oppure impedirne l'ingresso (**deny**). Nel controllo delle regole è importante l'ordine, come mostrato in **Figura 8**. Se nessuna regola viene soddisfatta il pacchetto viene automaticamente scartato ("implicit deny").

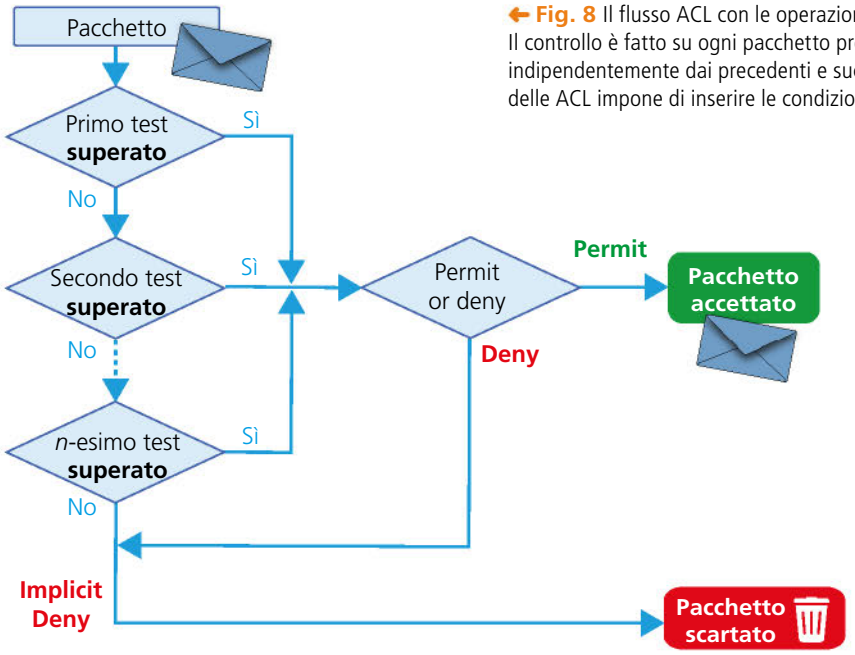


Fig. 8 Il flusso ACL con le operazioni di un pacchetto in entrata. Il controllo è fatto su ogni pacchetto preso singolarmente, indipendentemente dai precedenti e successivi. L'esecuzione sequenziale delle ACL impone di inserire le condizioni più restrittive all'inizio della lista.

Applicazione di una ACL all'interfaccia di un router

La definizione di una ACL prevede alcuni parametri:

- il numero dell'ACL (access-list) con i permessi (permit/deny);
- gli indirizzi IP di rete e le porte del livello di trasporto.

È necessario, inoltre, specificare a quale interfaccia del router si applicano le regole, precisando se si riferiscono al traffico in ingresso (in) oppure in uscita (out) dalla LAN.

notabene

La terminologia relativa alle ACL standard ed estese è specifica di Cisco, ma può essere applicata anche in un contesto generale, con qualche leggera differenza a seconda del produttore del dispositivo di rete.

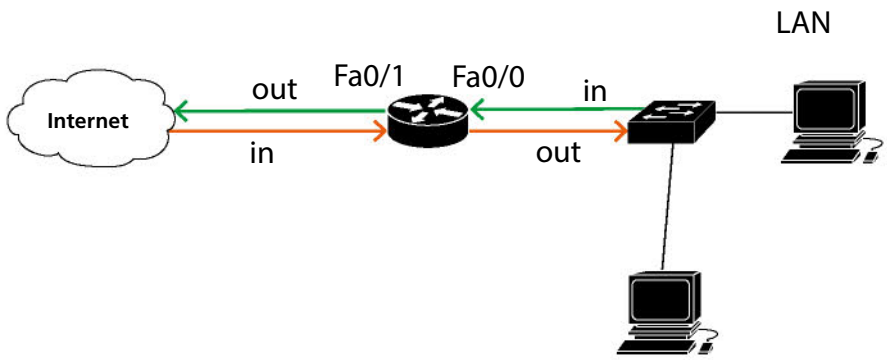


Fig. 9 Traffico in ingresso e uscita dalla LAN.

Nell'esempio di **Figura 9**, il router possiede due interfacce: una interna (Fa0/0) e una esterna (Fa0/1). In genere, l'obiettivo è configurare il router per proteggere la rete affidabile (la LAN) dalla rete non attendibile (Internet). Concettualmente, abbiamo quattro punti logici su cui il router può ispezionare il traffico: in/out sull'interfaccia interna (Fa0/0) e in/out sull'interfaccia esterna (Fa0/1). Possiamo applicare le regole su uno di questi punti in base al flusso del traffico che vogliamo controllare.

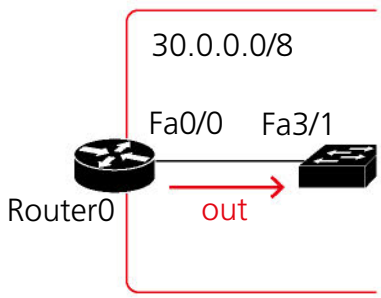


Fig. 10

Ad esempio, per bloccare il traffico proveniente da un host remoto con indirizzo 10.0.0.10 e diretto a un server appartenente alla rete 30.0.0.0/8 (**Figura 10**), e contemporaneamente permettere l'accesso ai pacchetti provenienti dall'host 10.0.0.11, occorre applicare le regole all'interfaccia del router interessata al transito dei pacchetti (interfaccia Fa0/0 di Router0).

Numero regola	Sorgente	Azione
10	IP: 10.0.0.10	Bloccato – Deny
20	IP: 10.0.0.11	Permesso – Permit

Comandi	risultato
`Router0(config)#access-list 1 permit 10.0.0.11`	IP permesso
`Router0(config)#access-list 1 deny 10.0.0.10`	IP negato
`Router0(config)#interface fa0/0`	Interfaccia a cui si applica la regola
`Router0(config-if)#ip access-group 1 out`	L'access list è associata alla porta in uscita
`Router0(config)#access-list 1 permit 10.0.0.11`	IP permesso
`Router0(config)#access-list 1 deny 10.0.0.10`	IP negato

Tab. 3 Regole ACL riferite alla Figura 10. Comandi che implementano la tabella.

La Tabella 4 fornisce la sintassi dei principali comandi e alcuni esempi per le modalità standard ed estesa.

Modalità standard	
access-list *access-list number* {**permit**|**deny**} {*host*|*source source-wildcard*|**any**}	
Parametri	**Descrizione**
Access-list number	Numero univoco che identifica ogni ACL e ne definisce il tipo.
Permit/Deny	Se le condizioni sono soddisfatte: Permette l'accesso/Nega l'accesso.
Source	Indirizzo sorgente del pacchetto Il termine `any` individua tutti gli indirizzi un singolo indirizzo si identifica con il termine host Una wildcard mask può essere applicata all'indirizzo sorgente
Modalità estesa	
access-list *access-list-number* {**permit**|**deny**} *protocol source source-wildcard destination destination-wildcard*	
Parametri	**Descrizione**
Access-list number	Numero univoco compreso tra 100 e 199 o tra 2000 e 2699 che identifica ogni ACL.
Permit/Deny	Se le condizioni sono soddisfatte: Permette l'accesso/Nega l'accesso.
Protocol	IP, ICMP, TCP, UDP, IGRP
Source/Destination Address	Indirizzi IP (sorgente e destinazione) del pacchetto.
Source/Destination Port	Porta sorgente o porta destinazione scelta in funzione del punto in cui il parametro port number è configurato nella ACL (invece del numero di porta si può indicare il servizio: FTP, HTTP, ecc.).
Comandi comuni	
interface *type number* → interfaccia a cui si applica la regola	
ip access-group *access-list number* {**in**|**out**}	
Parametri	**Descrizione**
Access-list-number	il numero della ACL che deve essere legata all'interfaccia
In|Out	Specifica la direzione. Indica se la regola va applicata all'interfaccia in entrata o in uscita. Se ACL è applicata in input, il router applica la regola e poi effettua il routing. Se si privilegia l'output, prima si effettua il routing e poi si applica la regola. Se il parametro non è specificato, si sottointende "out".
show access-lists → Visualizza le regole applicate al router	
no access-list access-list number → Elimina una ACL	
L'attivazione di ACL all'interfaccia avviene tramite il comando ip access-group, specificando la direzione (in/out).	

Pit Stop

7 Perché le ACL devono essere impostate sulle interfacce di un router?

← **Tab. 4** Tabella della sintassi dei principali comandi ACL in modalità standard ed estesa da applicare ai router CISCO nello stato di "Global Configuration Mode".

notabene

Fortinet è un'azienda che offre servizi di sicurezza, tra cui firewall di nuova generazione (NGFW) per la protezione delle reti.

Applicazione di una policy di sicurezza a un firewall

La configurazione delle ACL nei firewall può essere molto dettagliata e complessa. La configurazione può essere applicata sia tramite un'interfaccia **a riga di comando** (CLI), sia tramite un'**interfaccia grafica utente** (GUI). Entrambi i metodi hanno i loro vantaggi e la scelta tra l'uno o l'altro dipende dal contesto e dall'esperienza dell'amministratore della rete.
A titolo di esempio mostriamo due semplici configurazioni . La prima si riferisce a un firewall ASA CISCO, la seconda al firewall Fortinet.

Configurazione di un firewall ASA

L'Adaptive Security Appliance (ASA 5506-X) è un dispositivo di sicurezza prodotto da Cisco che unisce le funzionalità classiche di un firewall con quelle più sofisticate di prevenzione delle intrusioni. Le regole di accesso possono consentire o negare specifici tipi di traffico. Ad esempio, possono consentire il traffico SSH o VPN dalla rete Internet alla rete interna, oppure può bloccarlo.
Per impostazione predefinita, l'ASA di Cisco applica una policy di sicurezza che regola il flusso del traffico tra le interfacce in base ai loro livelli di sicurezza. Questa policy consente il traffico da un'interfaccia con un livello di sicurezza più elevato verso un'interfaccia con un livello di sicurezza inferiore, mentre blocca il traffico in direzione opposta.

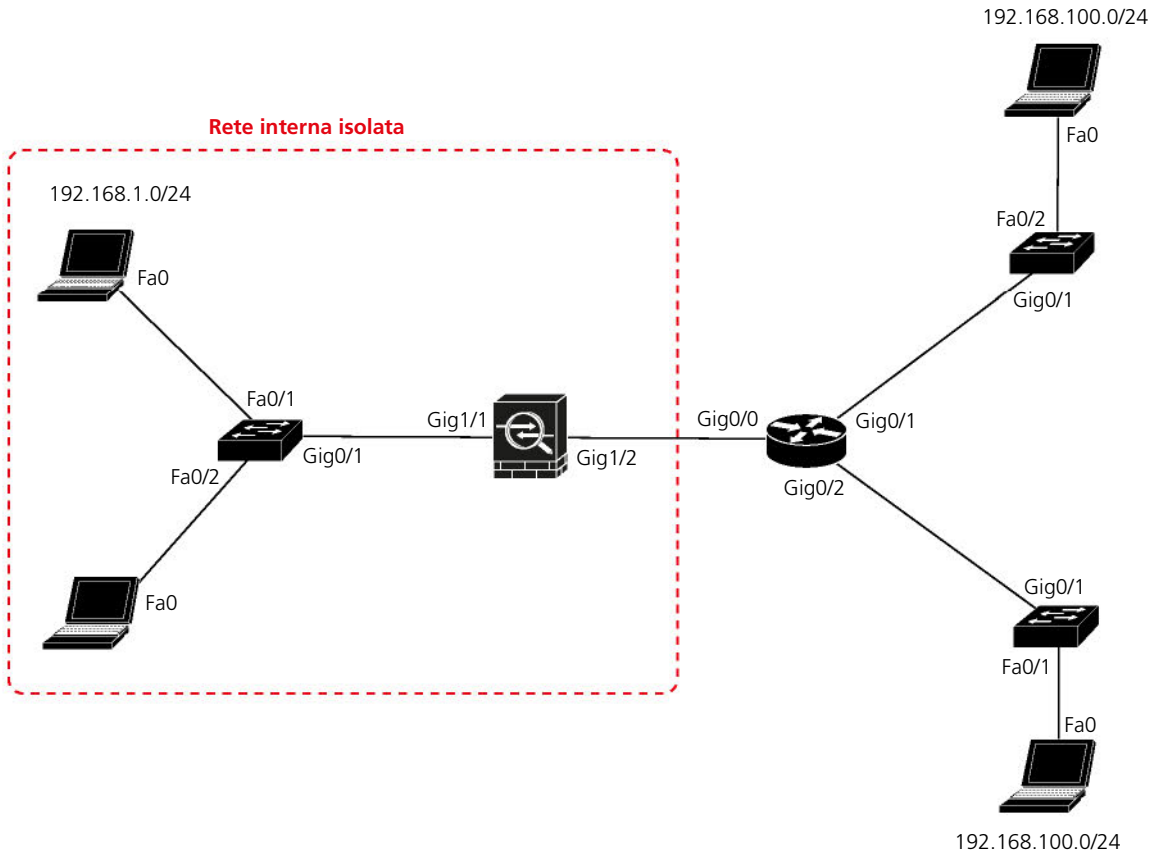


Fig. 11 Una applicazione con firewall Adaptive Security Appliance (ASA 5506-X) di CISCO.

Per valutare, seppure sommariamente, le ACL di ASA 5506-X, possiamo considerare la topologia della rete illustrata nella **Figura 11** e fare un semplice esempio che rende irraggiungibile dall'esterno la rete 192.168.1.0/24 .
Configuriamo l'interfaccia Gig1/1 di ASA che collega la rete interna (192.168.1.0/24). Successivamente, configuriamo l'interfaccia Gig1/2 per la rete esterna (200.0.0.2/24).

Per **impostazione predefinita**, l'ASA consente il traffico da un'interfaccia con un livello di sicurezza più elevato (in questo caso, l'interfaccia "inside", già impostata, nel firewall con livello di sicurezza 100) a un'interfaccia con un livello di sicurezza inferiore (in questo caso, l'interfaccia "outside", già impostata, con livello di sicurezza 0). Questo significa che il traffico può fluire liberamente dalla rete interna alla rete esterna, ma non viceversa.
È comunque possibile impostare i livelli di sicurezza e i nomi delle interfacce, anche se il dispositivo, "sapendo" di essere un firewall, configura già opportunamente "inside" verso la LAN e "outside" verso l'esterno:

```
ciscoasa>enable
ciscoasa#configure terminal
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)#security-level inside 100
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit

ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#ip address 200.0.0.2 255.255.255.0
ciscoasa(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)#security-level outside 0
ciscoasa(config-if)#no shutdown

ciscoasa#show interface ip brief
GigabitEthernet1/1 192.168.1.1 YES unset up up
GigabitEthernet1/2 200.0.0.2 YES unset up up
```

notabene

Molti comandi dell'interfaccia a riga di comando (CLI) dell'ASA sono simili, ma non identici, a quelli utilizzati dalla CLI di Cisco IOS. Il processo di passaggio tra gli stati di configurazione è essenzialmente lo stesso di quello dei router.

Configurazione di un firewall Fortinet

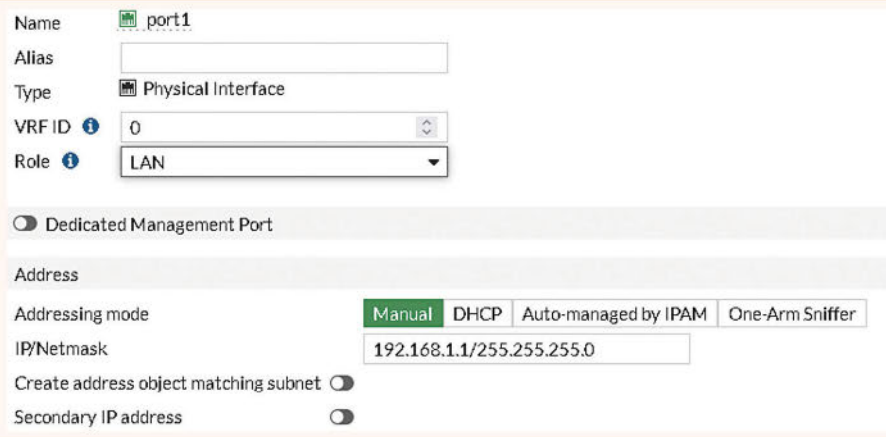
Gli apparati UTM più recenti possono essere configurati sia tramite riga di comando (CLI) sia tramite interfaccia web (GUI). Ogni produttore di dispositivi UTM ha le proprie caratteristiche. Molti di essi utilizzano una configurazione basata su oggetti: per implementare una regola di sicurezza (policy), è necessario creare gli oggetti specifici, come ad esempio indirizzi IP, gruppi di utenti e servizi, che verranno utilizzati nella regola.
Di seguito riportiamo l'esempio della configurazione di un firewall Fortinet, utilizzando i due modi, CLI e GUI, tenendo presente che le configurazioni sono identiche per tutti i modelli, a parità di versione del software.

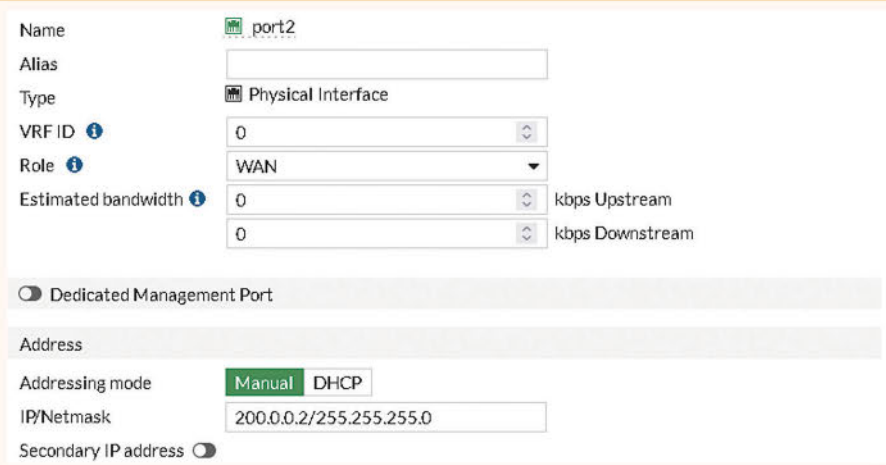
Configurazione delle interfacce

CLI

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.1.1 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set description "inside"
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 200.0.0.2 255.255.255.0
        set type physical
        set description "outside"
        set role wan
        set snmp-index 6
    next
end
```

GUI



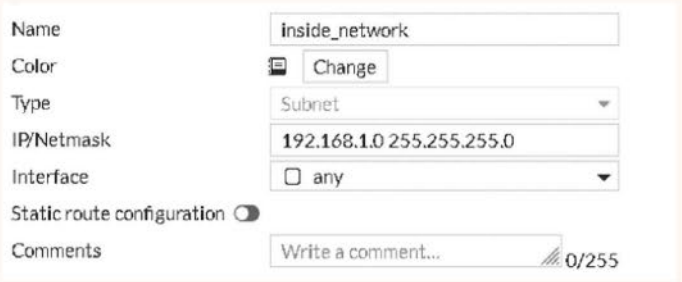


Impostazione dell'oggetto "address" (0.0.0.0/0 è già codificata come "all")

CLI

```
config firewall address
    edit "inside _ network"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

GUI

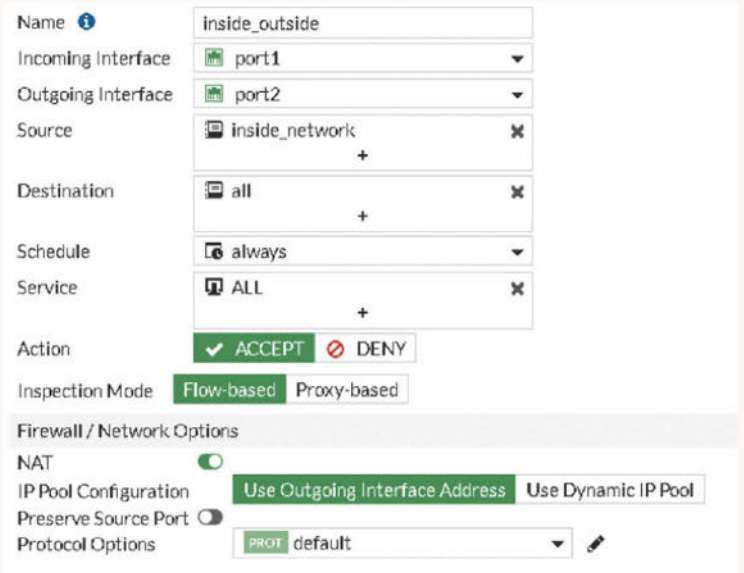


Creazione della policy

CLI

```
config firewall policy
    edit 1
        set name "inside _ outside"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "inside _ network"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

GUI



notabene

Un server proxy può essere installato su diversi tipi di sistemi come computer e server dedicati. I browser web (Figura 12b), possono avere funzionalità di proxy integrate così come alcuni router o firewall.

5 Proxy Server

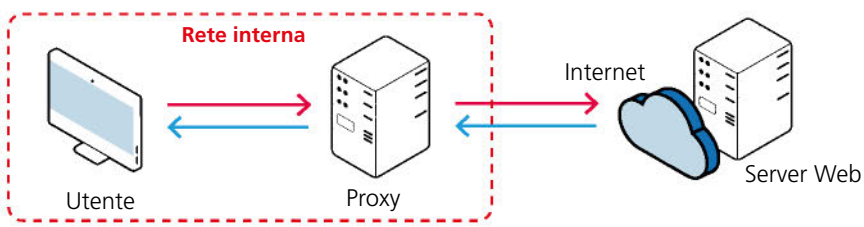
Le funzionalità del server proxy

Un **proxy server** (o **forward proxy**) è un sistema, un computer con il proprio indirizzo IP o un'applicazione software, che agisce **come intermediario tra il computer e i siti Web o le risorse Internet che l'utente vuole raggiungere**, concentrando in un unico punto il passaggio dei pacchetti tra la rete interna ed esterna (Figura 12).

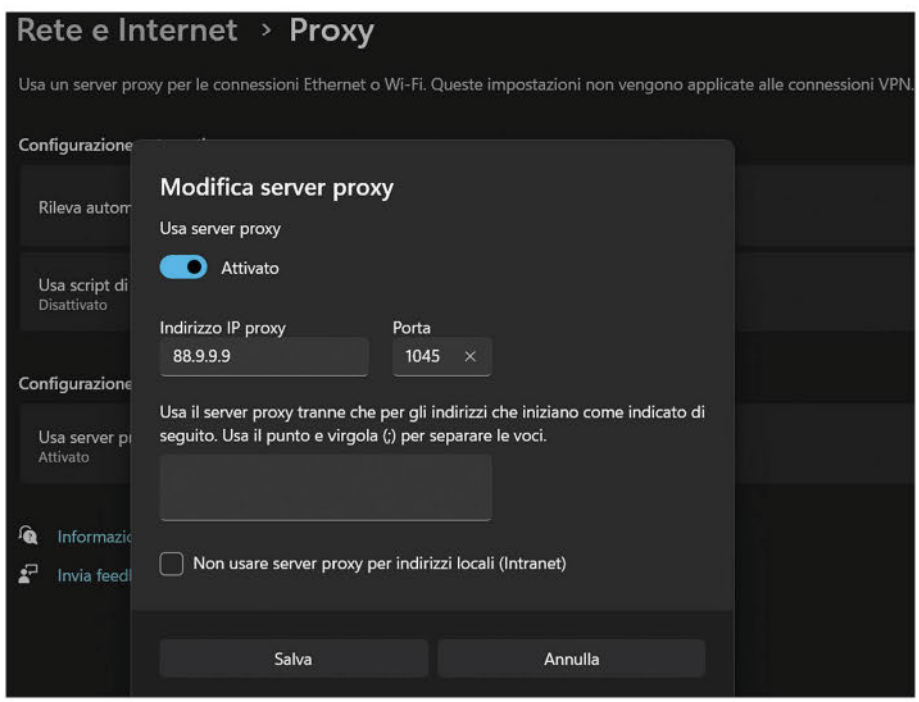
Il proxy svolge diversi compiti.

- Monitora il traffico, con la possibilità di mantenere traccia (log) degli accessi e registrare i pacchetti che violano una certa regola e limitare l'accesso a determinati siti web o servizi.
- Filtra gli accessi in base a parole chiave che riscontra nei dati in transito. Poiché lavora a livello applicazione, un proxy è in grado di analizzare i contenuti dei messaggi che possono riguardare una vasta gamma di argomenti. Ad esempio, una scuola potrebbe scegliere di filtrare parole chiave legate a siti di gioco d'azzardo, droghe, violenza, odio, razzismo, ecc.

a



b

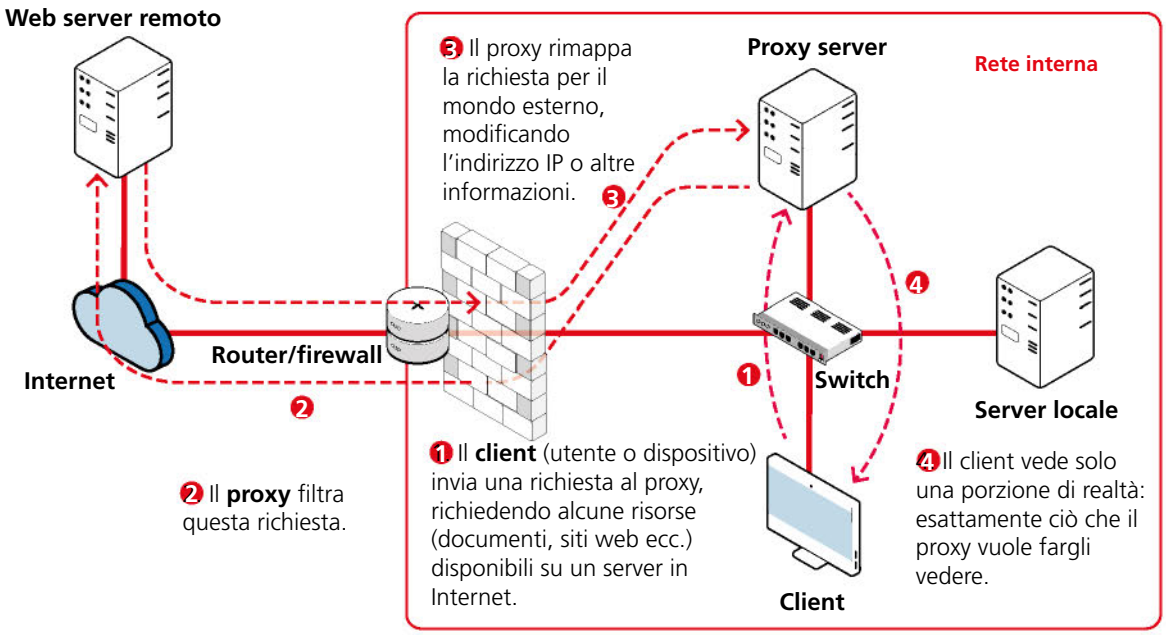


➜ **Fig. 12 a.** Proxy server (forward proxy). **b.** Impostazione manuale di un server proxy in Windows (l'indirizzo IP è puramente di esempio).

- Migliora le prestazioni di navigazione attraverso la memorizzazione delle pagine visitate nella memoria cache delle pagine web. Quando un utente richiede una pagina web a un server esterno, il proxy controlla se è nella sua cache; in tal caso, la invia direttamente al client, invece di recuperarla dal server web originale, riducendo così i tempi di risposta e il traffico di rete.

Nella **Figura 13** è illustrato il funzionamento di un **proxy server**, utilizzato come intermediario tra due reti. Il client si connette al server proxy, richiedendo alcune risorse (collegamento, file, sito Web ecc.) disponibili su un server in Internet.

Fig. 13 Il proxy server utilizzato come Firewall.



Comprendi con l'analogia

La "quarantena" di un file è come l'isolamento di un paziente durante un'epidemia

Dagli scritti di Maurizio Cornaro, mercante veneziano. Venerdì 16 agosto 1630, festa di San Rocco. Ponte della Fortunata

Il sole sorge lentamente all'orizzonte sulle acque agitate del mare. Sono passate più di due settimane da quando, a bordo della galea *Fortunata*, sono partito da Costantinopoli, dove la peste imperversa. Sono dovuto fuggire con il cuore pesante, lasciando dietro di me amici e commerci. Ogni giorno a bordo della *Fortunata* è un misto di speranza e paura. La speranza di rivedere la mia famiglia e il timore della malattia che potrebbe aver contaminato ogni angolo di Venezia.

Salgo sul ponte. Le acque della laguna sono ora più tranquille e la *Fortunata* procede con calma, guidata dalle vele e da rematori esperti. Quante volte ho fatto ritorno impaziente di mettere piede a terra; ma questa volta è diverso: la salute della mia amata città è in pericolo, e anch'io potrei essere un portatore della malattia. All'arrivo so che mi aspetta l'isola del Lazzaretto Nuovo, fuori Venezia, dove trascorrerò i prossimi 40 giorni in isolamento e in condizioni precarie per essere sicuro di non essere infetto.

La Sibilla, scolpita sulla polena della nave, guarda in avanti con determinazione, e anch'io vorrei fare lo stesso. Venezia, la mia casa, mi attende. E io attendo di poter camminare di nuovo per calli e campielli, di sentire lo sciabordio delle gondole che scivolano sui canali e di riabbracciare coloro che amo.

Come i viaggiatori delle navi venivano messi in isolamento per 40 giorni durante le epidemie, un antivirus moderno, quando rileva un file sospetto, lo sposta in "quarantena", un'area di memoria isolata dove i file non possono fare danni né contagiare altri.

Un **server proxy** ha anche la funzione di **mascherare l'indirizzo IP di un utente dietro un altro indirizzo**, permettendo la navigazione anonima su Internet e impedendo al server di destinazione di determinare l'origine della richiesta. Ad esempio, se un utente desidera accedere a un server di social network, ma non può (o non vuole) farlo direttamente, può utilizzare un **server proxy pubblico** ospitato su Internet, seguendo il flusso illustrato in Figura 14. In questo scenario, il client invia la richiesta al server proxy. Dopo aver analizzato la richiesta, il server proxy la inoltra al server di destinazione. Il server risponde al proxy, che a sua volta inoltra la risposta al client.

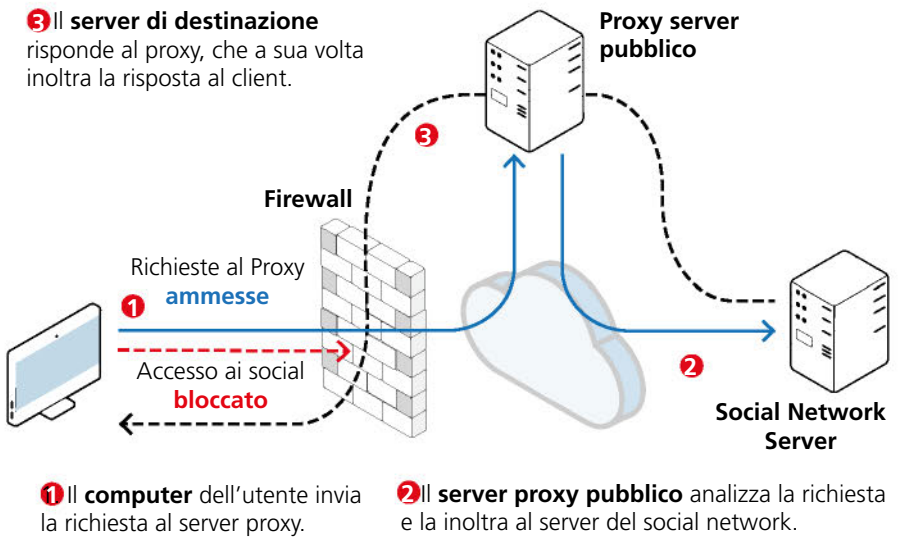


Fig. 14 Un server proxy che fa da gateway per il server di social network.

Pit Stop

8 Quali sono i principali compiti di un proxy server?

Questo meccanismo è simile a quello con cui viene instradata una chiamata telefonica, per esempio quando la segreteria di una scuola effettua una chiamata telefonica esterna: il numero visualizzato dal destinatario della chiamata è quello del centralino della scuola, non quello della segreteria.

Bastion Host

Un server proxy può essere ospitato in un ambiente isolato, noto come "bastion host": un computer che ospita solo i servizi essenziali al funzionamento dell'applicazione proxy, posizionato in modo simile al proxy server mostrato in Figura 14. Il suo obiettivo principale è creare uno scudo protettivo per la rete locale, difendendola dagli attacchi esterni e isolandola da Internet con i metodi seguenti.

- **Filtraggio del traffico**: il bastion host filtra il traffico scambiato tra la rete locale e Internet. Questo aiuta a prevenire l'accesso non autorizzato e a proteggere la rete interna.
- **Blocco dell'accesso alla rete locale in caso di attacco**: se viene rilevata un'attività malevola o un tentativo di intrusione, il bastion host può bloccare l'accesso alla rete locale per proteggerla.
- **Limitazione dei servizi non essenziali**: il bastion host limita tutti gli altri servizi non essenziali, come applicazioni e utenti. Questo riduce al minimo la minaccia di infezioni.
- **Aggiornamenti costanti**: per mantenere l'efficacia, il bastion host deve essere costantemente aggiornato.

Fig. 15 Il rivellino che protegge la Porta di Santo Spirito del Castello Sforzesco di Milano è l'elemento più avanzato della fortificazione, costruito appena fuori dalle mura a salvaguardia della porta.



Il termine "bastion host" deriva dal bastione che nel medioevo indicava un punto particolarmente solido delle fortificazioni di un castello che aveva lo scopo di respingere gli attacchi nemici (Figura 15).

Server Proxy Pubblici e Sicurezza

I server proxy pubblici possono essere **utilizzati in modo malevolo** dagli hacker per nascondere la loro identità durante gli attacchi informatici. Ad esempio, un attaccante potrebbe sfruttare un proxy pubblico per inviare richieste malevole a un server-vittima senza rivelare il proprio indirizzo IP originale, evitando così di essere rintracciato.
Inoltre, alcuni hacker creano una **catena di proxy** per rendere ancora più difficile risalire all'origine dell'attacco. Affittano server proxy per un breve periodo di tempo (ad esempio, alcune ore) e fanno passare il traffico attraverso una serie di proxy diversi. Per proteggersi dagli attacchi tramite server proxy, le organizzazioni adottano diverse contromisure, tra cui:

- **Monitoraggio del traffico**: analizzare attentamente il traffico di rete per individuare eventuali anomalie o attività sospette.
- **Utilizzo di liste di proxy noti come malevoli**: bloccare l'accesso ai server proxy noti per essere utilizzati per scopi malevoli.
- **Analisi di comportamenti anomali**: monitorare i modelli di traffico e identificare eventuali comportamenti fuori dall'ordinario.

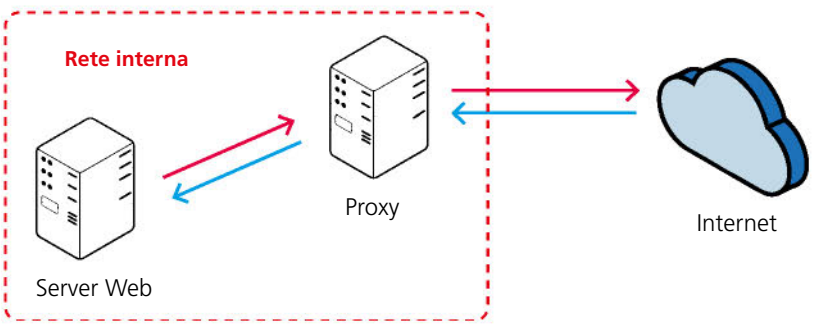
Il reverse proxy

Un **reverse proxy**, come suggerisce il nome, agisce in modo complementare a un forward proxy. Mentre un forward proxy riceve le richieste dai client e le inoltra ai server su Internet, un **reverse proxy si posiziona tra uno o più server web interni alla rete e Internet** (Figura 16). Riceve le richieste da Internet e le inoltra ai server sulla rete interna. Dopo aver inviato la richiesta a uno dei server web, riceve la risposta da quel server e la restituisce al client.
Le principali funzionalità di un reverse proxy includono:

- **Anonimato del server**: nasconde le informazioni dei server interni, rendendo più difficile per un attaccante capire la struttura della rete.
- **Bilanciamento del carico**: ripartisce le richieste, che arrivano dai client in Internet, a più server interni.
- **Sicurezza**: controlla l'accesso alla rete interna e protegge i server da attacchi come quelli DDoS.

Pit Stop

9 Dove si colloca un reverse proxy?



↑ **Fig. 16** Reverse proxy con server web.

notabene

A protezione della DMZ è utile posizionare sul firewall un sistema di rilevamento delle intrusioni (IDS) che, insieme a un sistema di prevenzione delle intrusioni (IPS),possono segnalare agli amministratori di rete traffico anomalo e potenziali intrusioni.

6 DMZ e Port forwarding

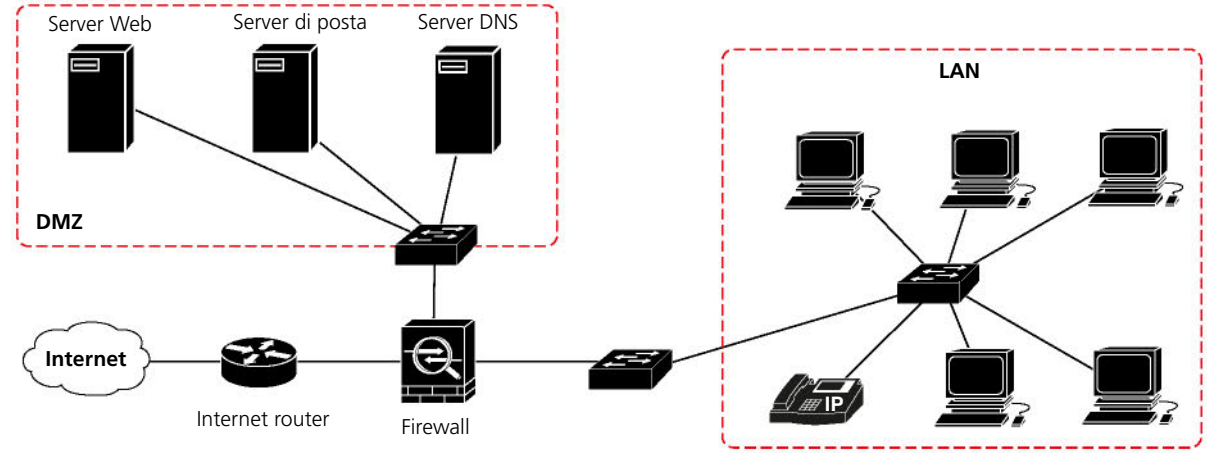
DMZ- DeMilitarized Zone

In gergo militare, la "zona demilitarizzata" è un'area di frontiera che fa da cuscinetto tra due stati in cui non è permessa alcuna operazione militare. Con la stessa finalità, nel mondo della sicurezza informatica si crea una "zona demilitarizzata" o **DMZ - D*e*M*ilitarized* Z*one***. Questa zona funge da cuscinetto tra la rete interna di un'organizzazione e Internet. In questa zona sono posizionati i server che devono essere accessibili dall'esterno, come il server web, il server di posta elettronica, il server FTP e il server DNS. Questa configurazione permette di proteggere la rete interna, poiché in caso di un attacco solo i server nella DMZ sarebbero compromessi, mantenendo così al sicuro i dati sensibili all'interno della rete interna. In quest'area uno o più firewall confinano il traffico proveniente da Internet, impedendo l'accesso ai dati della rete privata.
Una DMZ può essere progettata in diversi modi che utilizzano un firewall singolo o due o più firewall:

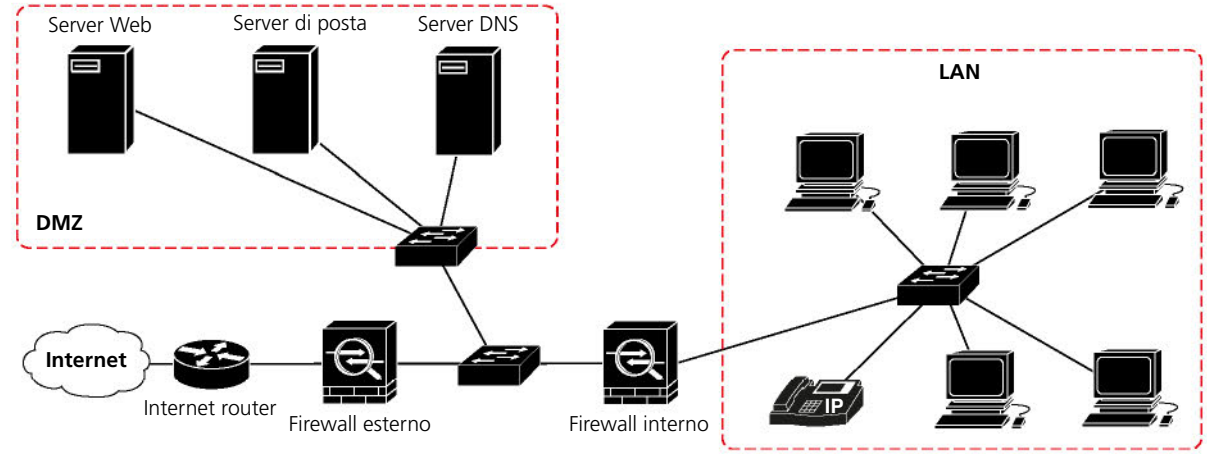
- **Firewall singolo**. In Figura 17a è mostrata una DMZ gestita da un singolo firewall che richiede tre interfacce di rete: una delle interfacce è collegata a Internet, un'altra alla rete DMZ e una terza interfaccia si collega alla rete interna. Le richieste che provengono da Internet sono deviate verso la zona de-

Fig. 17 a. DMZ e rete con singolo firewall. **b.** DMZ e rete con doppio firewall.

a



b

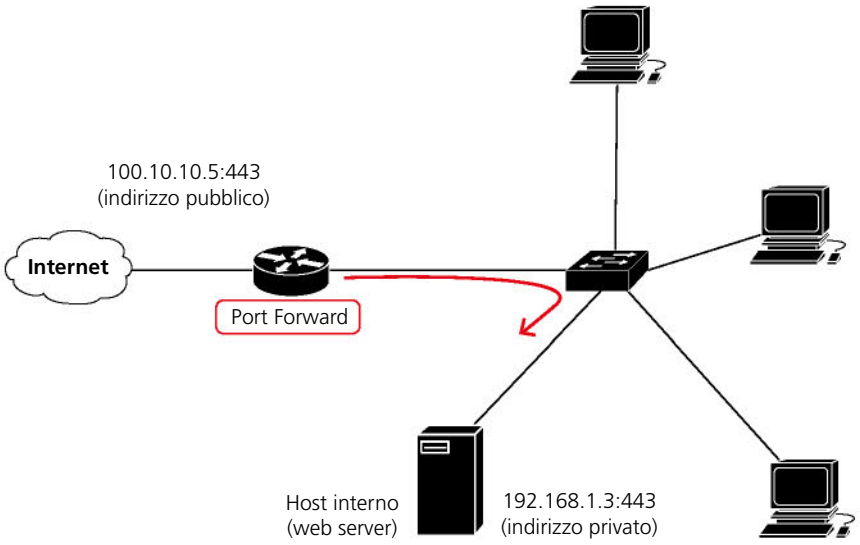


militarizzata. In caso di attacco, saranno compromessi solo i servizi collegati al server pubblico, proteggendo così i dati privati presenti in LAN. Questo è uno dei vantaggi principali della DMZ: anche se i server esposti vengono compromessi, l'attaccante non avrà accesso diretto alla rete interna.

- **Firewall doppio.** L'utilizzo di due firewall con una DMZ tra di essi è l'opzione più sicura e maggiormente utilizzata. Come illustrato in Figura 17b, Il primo firewall filtra il traffico esterno alla DMZ e consente il traffico esclusivamente verso la DMZ, mentre il secondo consente solo il traffico tra la DMZ e la rete interna. Se un attaccante riesce a compromettere il primo firewall, deve ancora superare il secondo per accedere alla rete interna.

Port forwarding

Il **port forwarding** è una tecnica utilizzata nei router per indirizzare il traffico di rete da una porta specifica dell'indirizzo IP pubblico del router a una porta specifica di un dispositivo all'interno della rete locale (LAN). Questa tecnica permette agli utenti in Internet di utilizzare risorse interne alla rete privata, come un computer o una telecamera di sicurezza.
Ad esempio, consideriamo la Figura 18. L'indirizzo IP pubblico del router è 100.10.10.5. Il computer che, nella rete locale, ospita un server web sulla porta 443, ha indirizzo IP 192.168.1.3. Quando si configura il port forwarding, si sta dicendo al router che una richiesta che arriva al suo indirizzo pubblico 100.10.10.5:443 deve essere inoltrata all'indirizzo privato 192.168.1.3:443. In questo modo, quando qualcuno cerca di accedere all'indirizzo IP pubblico sulla porta 443, verrà indirizzato direttamente al server web interno. Può capitare, soprattutto a chi utilizza un'applicazione di gaming online o scarica musica, di non riuscire a fare un port forwarding perché le porte su cui queste applicazioni operano sono bloccate. Per "aprire le porte" e sbloccarle, è necessario intervenire sulle impostazioni del router o del firewall (come mostrato in Figura 19). È importante ricordare che questa operazione dovrebbe essere eseguita con cautela, poiché l'apertura delle porte può esporre la rete a potenziali rischi di sicurezza. Sarebbe anche utile impostare filtri o regole sul router per limitare l'accesso solo a determinati indirizzi IP esterni.



↑ **Fig. 18** Port-forwarding: il traffico in entrata che raggiunge 100.10.10.5 sulla porta 443 viene tradotto nell'IP di destinazione 192.168.1.3 sulla porta 443, che è l'indirizzo del server web.

notabene

È una buona pratica avere un server Web HTTPS in ascolto sulla porta 443, perché i dati sono crittografati con il protocollo TLS. Tuttavia gli attacchi possono avvenire su qualsiasi porta, pertanto è fondamentale proteggere le attività di rete con un firewall.

Pit Stop

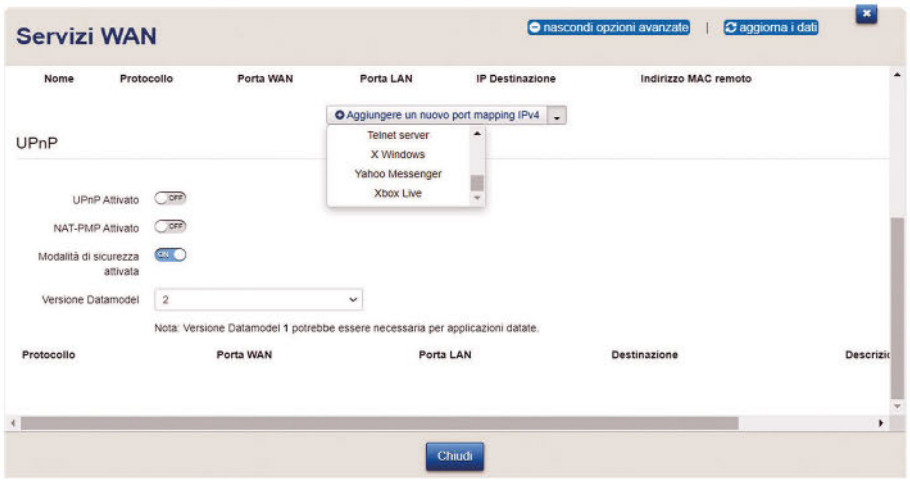
10 Che cos'è una DMZ?

11 Quando è utile fare il port forwarding?

Il port forwarding, sebbene utile in alcuni casi, presenta dei rischi per la sicurezza:

- **Accesso non autorizzato**: il port forwarding può creare una porta di accesso da Internet alla rete interna permettendo a utenti non autorizzati di penetrare nella rete.
- **Bypass della VPN**: il port forwarding potrebbe rendere inutile la protezione offerta da una VPN.
- **Rischi per la privacy**: la privacy potrebbe essere a rischio a causa dell'esposizione di dispositivi interni.
- **Dispositivi vulnerabili in una rete IoT**: i dispositivi esposti attraverso il port forwarding diventano punti vulnerabili in una rete IoT.

Una considerazione finale riguarda l'attualità della DMZ che è stata per molti anni la soluzione più diretta per segmentare una rete e mitigare il fenomeno degli attacchi ai server web, DNS e di posta elettronica. Tuttavia, l'avvento del **cloud computing** ha cambiato questo scenario. Molte aziende hanno preferito non ospitare i propri server in casa, ma spostarli presso **strutture esterne accessibili da Internet, dotate di tutti i meccanismi di sicurezza, affidabilità e continuità del servizio**. Questo ha ridotto la necessità di una DMZ per molte organizzazioni. Tuttavia, il concetto di protezione è rimasto intatto. Anche se la maggior parte delle organizzazioni non ha più bisogno di una DMZ, la necessità di fornire servizi pubblici senza permettere l'accesso ad archivi privati rimane un requisito fondamentale. Inoltre, con l'aumento delle minacce alla sicurezza, una DMZ rimane uno strato di sicurezza essenziale, specialmente per proteggere dati sensibili.
È comunque una buona prassi combinare DMZ con il **port forwarding**, inoltrando ai server nel segmento di rete protetto solo le porte necessarie per esporre i servizi.



➜ **Fig. 19** L'aggiunta automatica di porte per servizi standard su un router domestico.

Approfondimento - Tecnologia

Intelligenza Artificiale e sicurezza



L'Intelligenza Artificiale sta rivoluzionando anche il campo della sicurezza informatica grazie a diversi fattori:

- **Ispezione del traffico**: l'IA è in grado di ispezionare il traffico in entrata e in uscita, correlando gli eventi critici provenienti da diverse fonti, compresi gli indirizzi IP.
- **Rilevamento di attività anomale**: la velocità con cui l'IA rileva attività fuori dall'ordinario consente di rispondere tempestivamente alle minacce e di prevenire intrusioni non autorizzate.
- **Apprendimento automatico**: l'IA utilizza tecniche di apprendimento automatico per identificare comportamenti anomali. Questo può basarsi sui log di sistema o delle applicazioni, nonché sulle regole imposte dalle normative internazionali che definiscono comportamenti accettabili o sospetti. Gli errori passati possono anche essere utilizzati come esperienza di apprendimento per addestrare i modelli di apprendimento automatico.
- **Bilanciamento del traffico di rete**: la distribuzione del traffico tra diversi server aiuta a ridurre il rischio di sovraccarico e a mitigare gli attacchi DDoS.
- **Decodifica del traffico TLS**: l'IA è in grado di decifrare il traffico TLS per identificare potenziali attacchi.

Un esempio di modello di apprendimento supervisionato è l'**albero di decisione** che permette di **classificare gli eventi in arrivo e prendere decisioni**. Ad esempio, consideriamo il caso dell'arrivo di una e-mail. Percorrendo i rami dell'albero (semplificato) il sistema deve decidere se si tratta di un tentativo di phishing o meno. Se l'e-mail contiene link sospetti, la gestione dipende dal mittente e dal contenuto:

- **E-mail senza link sospetti**
  - **E-mail legittima**: Nessuna azione richiesta.
- **E-mail con link sospetti**
  - **Mittente noto**
    - **Mittente autenticato**
      - **E-mail legittima**: Nessuna azione richiesta.
    - **Mittente non autenticato**
      - **E-mail legittima**: Nessuna azione richiesta.
      - **E-mail sospetta** (ad esempio, manca la firma digitale): valuta il contenuto ed eventualmente segnala come phishing.
  - **Mittente sconosciuto**
    - Valuta il contenuto:
      - **E-mail che appare legittima**: Nessuna azione richiesta.
      - **E-mail sospetta**: segnala come phishing.

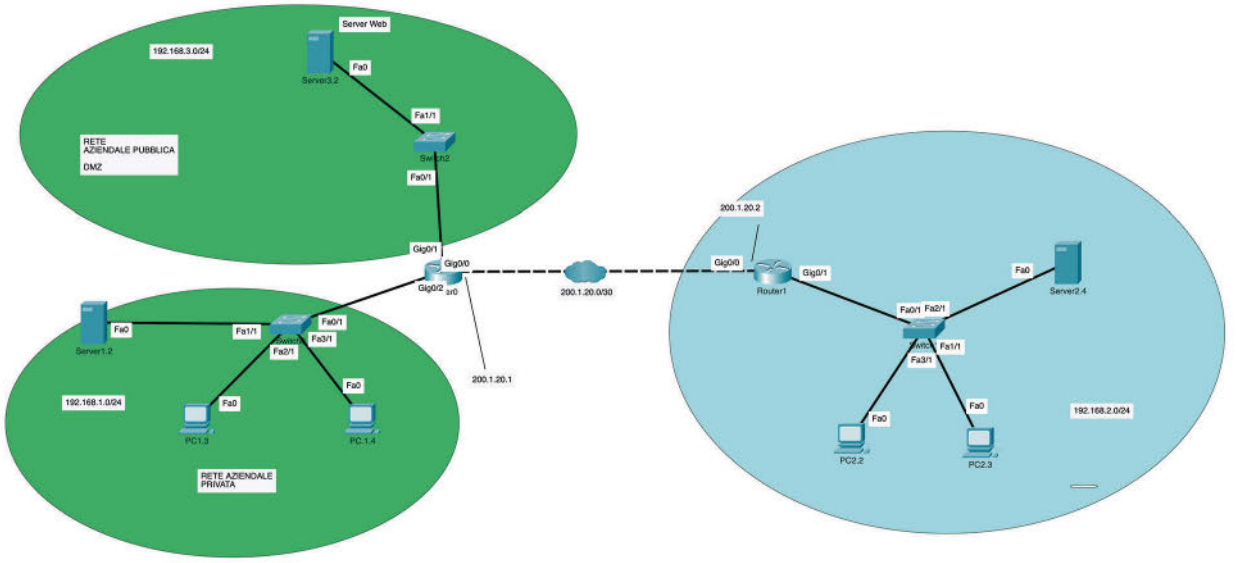
L'Intelligenza Artificiale può intervenire in vari punti dell'albero di decisione, ad esempio può **esaminare il contenuto e la forma di scrittura**, o può **prendere in considerazione i log** per individuare comportamenti sospetti, come orario insolito o posizione.

Laboratorio

ATTIVITÀ 1
Realizzare una DMZ impostando le ACL su un router di confine

Scenario

Consideriamo la situazione di un'organizzazione (azienda, scuola...) in cui è presente una LAN. L'organizzazione ha la necessità di rendere disponibile il suo sito web a chiunque. Il sito è su un server interno alla infrastruttura dell'organizzazione.



Consegna

1. Progettare una DMZ per isolare l'area pubblica della rete aziendale e proteggere l'area privata da accessi esterni. Deve essere consentito l'accesso da qualunque host esterno verso il server web e fermato ogni accesso esterno verso l'area privata.
2. Deve inoltre essere consentito al personale interno all'organizzazione di accedere a Internet e navigare sul Web.

Svolgimento

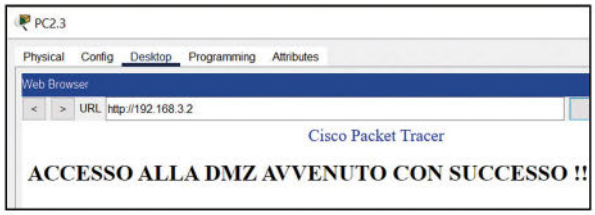
Passo 1

Per consentire l'accesso dall'esterno al server web interno all'organizzazione e fermare qualunque altro ingresso, occorre agire sul router dell'organizzazione in ingresso.
Definiamo una ACL da impostare sull'interfaccia esterna del router, in ingresso:

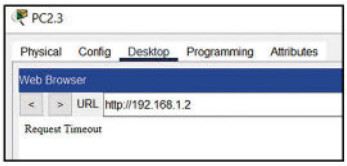
```
interface g0/0
access-list 100 permit tcp any host 192.168.3.2 eq 80
interface g0/0
ip access-group 100 in
```

Non occorre specificare che è bloccato qualunque altro ingresso perché, se non è specificata una regola da applicare, il pacchetto è scartato.

Passo 2
Verificare il funzionamento della regola.
Con il browser di un PC esterno, per esempio PC2.3, fare una richiesta HTTP verso il server web su Server3.2 sulla DMZ e verificare il corretto funzionamento.



Con il browser di un PC esterno, per esempio PC2.3, fare una richiesta HTTP verso il server web su Server1.2 sulla LAN privata e verificare che l'accesso non è consentito.



Passo 3
Vogliamo ora consentire la navigazione nel Web al personale interno all'organizzazione.
Per esempio, supponiamo che PC1.3 faccia una richiesta HTTP al Server2.4. Consideriamo le seguenti fasi:

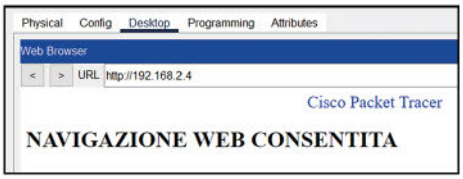
1. Richiesta HTTP da PC1.3 a Server2.4 (server web).
2. Risposta HTTP da Server2.4 a PC1.3.

Per la Fase 1 non ci sono problemi.
Il problema è far rientrare nella rete privata il messaggio di risposta HTTP proveniente da un host esterno.
Il messaggio, infatti, sarà bloccato per quanto già detto nei passi precedenti.
Occorre quindi fare in modo che il router possa distinguere se il traffico che entra è la risposta a una precedente richiesta, oppure è una richiesta proveniente dall'esterno con alta probabilità che sia un attacco.
È la differenza tra il funzionamento dei firewall stateless rispetto ai firewall statefull.
Per risolvere il problema occorre aggiungere una regola alla lista del controllo degli accessi, per consentire l'accesso alla rete da un qualunque IP, ma con porta mittente 80.

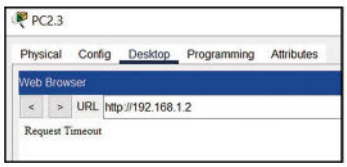
```
access-list 100 permit tcp any eq 80 192.168.1.0 0.0.0.255
established
```

In una ACL la parola **`established`** consente di bloccare il traffico in arrivo dall'esterno, a eccezione del traffico TCP di ritorno, dovuto a una sessione TCP iniziata dall'interno. È utilizzata solo con il protocollo TCP e implica il controllo sui flag ACK-SYN usati in apertura della connessione TCP.

Passo 4
Verificare il funzionamento della regola.
Con il browser di un PC interno, per esempio PC1.3, fare una richiesta HTTP verso il server web su Server2.4 in Internet e verificare il corretto funzionamento.



Con il browser di un PC esterno, per esempio PC2.3, fare una richiesta HTTP verso il server web su Server1.2 sulla LAN privata e verificare che l'accesso non è consentito.

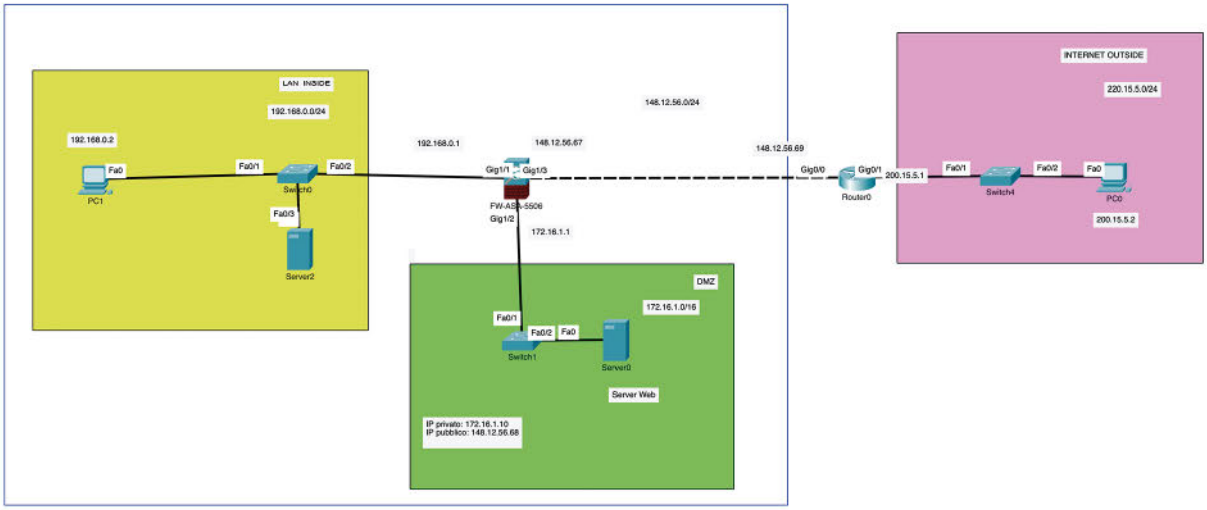


ATTIVITÀ 2

Realizzare una DMZ con un firewall

Scenario

Consideriamo la situazione di un'organizzazione (azienda, scuola...) in cui è presente una LAN. L'organizzazione ha la necessità di rendere disponibile il suo sito web a chiunque. Il sito è su un server interno all'infrastruttura dell'organizzazione.



Consegna

Utilizzando Packet Tracer, progettare una DMZ per isolare l'area pubblica della rete aziendale e proteggere l'area privata da accessi esterni con un firewall. Deve essere consentito l'accesso da qualunque host esterno verso il server web.

Svolgimento

Passo 1: configurazione delle interfacce del firewall

In questa attività utilizzeremo un firewall ASA-5506. Configuriamo le interfacce del firewall definendo: nome dell'interfaccia, indirizzo IP, livello di sicurezza.
Ricordiamo che di default è possibile passare solo da un determinato livello di sicurezza a uno più basso.

```
! interfaccia LAN
interface GigabitEthernet1/2
nameif inside
ip address 192.168.0.1 255.255.255.0
security-level 100
no shutdown
exit

! interfaccia WAN
interface GigabitEthernet1/3
nameif outside
ip address 148.12.56.67 255.255.255.0
security-level 0
no shutdown
exit

!interfaccia DMZ
interface GigabitEthernet1/1
nameif dmz
ip address 172.16.1.1 255.255.0.0
security-level 50
no shutdown
exit
```

Passo 2: configurazione NAT

Configurariamo il NAT per consentire agli utenti della rete interna (LAN) di accedere a Internet.
Ricordiamo che per mascherare gli indirizzi IP privati usati all'interno di una LAN con un unico indirizzo IP pubblico assegnato alla rete occorre configurare il NAT (*Network Address Translation*).
Il firewall ASA 5506 dispone della funzionalità Auto NAT che è particolarmente utile quando l'indirizzo IP di una rete è dinamico, assegnato da DHCP. Occorre creare un oggetto di rete per ogni segmento della rete interna (nel nostro caso la LAN parte privata e la DMZ) e definire una regola per effettuare il PAT da un dispositivo interno verso la rete internet.
Auto NAT utilizza i nomi delle interfacce (che abbiamo definito precedentemente nella fase di configurazione).

- NAT dinamico per consentire agli host della LAN l'accesso a Internet:

```
object network LAN
subnet 192.168.0.0 255.255.255.0
nat (inside,outside) dynamic interface
```

- NAT dinamico per consentire agli host della DMZ (server pubblici) l'accesso a Internet:

```
object network DMZ
subnet 172.16.1.0 255.255.255.0
nat (DMZ,outside) dynamic interface
```

- NAT statico per consentire dall'esterno l'accesso al server web sulla DMZ (regola bidirezionale):

```
object network webserver
host 172.16.1.10
nat (DMZ,outside) static 148.12.56.68
```

Passo 3: routing

Definiamo una rotta di default per instradare tutto il traffico in uscita verso il router esterno:

```
route outside 0.0.0.0 0.0.0.0 148.12.56.69
```

Passo 4: definizione delle ACL

- Definiamo delle regole per consentire l'utilizzo di ICMP e accettare le risposte echo in arrivo e per consentire il traffico in entrata verso il server web con indirizzo pubblico sulla DMZ. Applichiamo poi le regole all'interfaccia outside.

```
access-list OUTSIDE extended permit icmp any any echo-reply
access-list OUTSIDE extended permit icmp any any unreachable

object network webserver-external-ip
host 148.12.56.68

access-list OUTSIDE extended permit tcp any object webserver
eq www
access-list OUTSIDE extended permit tcp any host 148.12.56.68
eq www

access-group OUTSIDE in interface outside
```

Passo 5: verifica

Proviamo ora a fare una richiesta HTTP verso il server web sulla DMZ, utilizzando il browser del PC0 in Internet e verifichiamone il corretto funzionamento.



Passo 6: utilizzo delle politiche

Utilizzando il comando `show running-config` è possibile rivedere tutte le impostazioni del firewall.

In particolare quelle relative alle policy usate per ispezionare il traffico. Osserviamo le impostazioni predefinite:

- class-map: ispeziona i pacchetti che usano un determinato protocollo di livello trasporto (TCP, UDP) o livello applicazione (HTTP, DNS, ...);
- policy-map: definisce l'azione da fare (inspect, permit, drop, log) sul pacchetto ispezionato;
- service-map: applica le impostazioni a una interfaccia;

- "global" indica che la policy è applicata di default a tutte le interfacce:

```
ciscoasa#show running-config
…..
class-map inspection _ default
match default-inspection-traffic
!
policy-map type inspect dns preset _ dns _ map
parameters
message-length maximum 512

policy-map global _ policy
class inspection _ default
inspect dns preset _ dns _ map
inspect ftp
inspect tftp
!
service-policy global _ policy global
```

SINTESI

SICUREZZA PERIMETRALE
Protegge il confine tra una rete privata e la rete pubblica per prevenire l'accesso non autorizzato ai dati della rete privata.

FIREWALL
Dispositivo che separa una rete LAN da una WAN. Permette di applicare regole di sicurezza per monitorare il traffico in entrata e in uscita o bloccare minacce e attacchi.

ACL
Elenco di regole impostate su un'interfaccia di un router o di un firewall, in ingresso o in uscita, per stabilire quali pacchetti possono entrare o uscire da una rete.
Le regole possono consentire il passaggio del traffico (*permit*) o impedirlo (*deny*). Ogni regola è impostata a livello di indirizzi IP, di porta o di protocollo.

PROXY
Sistema (un computer o un'applicazione) che agisce come intermediario tra un host della LAN e i siti web o le risorse Internet, concentrando in un unico punto il passaggio dei pacchetti tra la rete interna e quella esterna.
Altre funzioni svolte: monitoraggio del traffico, filtro del traffico a livello Applicazione, cache delle ultime pagine web visitate.

DMZ
Segmento di una rete LAN che ospita server pubblici e deve essere isolato dal resto della LAN per non comprometterla.

PORT FORWARDING
Tecnica utilizzata (su router o firewall) per indirizzare il traffico di rete a una porta specifica di un dispositivo all'interno di una LAN.

STATELESS
Operano a livello Rete e Trasporto. Applicano regole di filtraggio sugli indirizzi IP e sulle porte. Non tengono memoria dello stato della comunicazione.

STATEFUL
Operano a livello Rete e Trasporto, ma conservano memoria dello stato della connessione perché considerano SYN, ACK, sequence number di TCP. In questo modo è consentito il traffico dall'esterno all'interno, a patto che sia la risposta a una precedente richiesta.

STANDARD
Filtrano il traffico solo sulla base dell'indirizzo IP sorgente dei pacchetti in arrivo.

ESTESE
Filtrano il traffico sulla base di vari criteri, come l'indirizzo IP di origine e di destinazione, il numero di porta.

FORWARD
Riceve le richieste dai client della LAN e le inoltra ai server su Internet.

REVERSE
Riceve le richieste da Internet e le inoltra ai server sulla rete interna.

Verifica delle CONOSCENZE

Vero o Falso?

1 Un firewall è una periferica di output. V F

2 Un firewall è in esecuzione su uno switch. V F

3 Un firewall garantisce la segretezza dei messaggi. V F

4 Il port forwarding indirizza il traffico verso una porta. V F

5 Un proxy server lavora a livello di rete. V F

6 Il proxy può avere sia funzione di server sia funzione di client. V F

7 Un firewall può essere hardware o software. V F

8 Un firewall può lavorare a livello di rete, a livello trasporto o a livello applicazione. V F

9 Una DMZ è utile quando si usa un servizio in hosting. V F

10 Una DMZ è utile per isolare server in Internet. V F

11 Un reverse proxy filtra il traffico in uscita dalla LAN. V F

12 Le ACL servono sempre e solo a impedire il passaggio di traffico. V F

13 I firewall stateful inspection analizzano i flag ACK e SYN di TCP. V F

14 Una ACL è assegnata ad una interfaccia di uno switch. V F

15 Una ACL può consentire o negare il passaggio di traffico. V F

16 Un firewall può controllare le connessioni TCP. V F

17 Un firewall può essere un host della LAN. V F

18 Le ACL possono filtrare il traffico relativo a determinati protocolli. V F

19 Le ACL sono applicate solo sul traffico in entrata verso la LAN. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

20 Un Packet filtering firewall:

a può bloccare richieste di connessione dall'esterno della LAN
b può lavorare solo se è presente una DMZ
c può essere usato per garantire l'integrità dei dati
d autentica gli utenti di una LAN

21 Un firewall Stateful Packet Inspection:

a definisce lo stato di un server proxy
b seleziona le richieste di connessioni che possono passare
c lavora a livello di applicazione
d ispeziona il contenuto di un messaggio di posta elettronica

22 Le regole di filtraggio di un firewall:

a servono per decidere il tipo di firewall da utilizzare
b sono indipendenti dall'organizzazione aziendale
c sono applicate secondo un ordine prestabilito
d devono sempre esplicitare che cosa non far passare

23 Utilizzando le ACL su un router, se nessuna regola viene soddisfatta, il pacchetto:

a è automaticamente autorizzato
b è automaticamente scartato
c è inviato a tutti i nodi della rete
d è rimandato al mittente

24 Un firewall stateful inspection

a lascia entrare nella LAN richieste HTTP dall'esterno
b è usato solo con una DMZ
c lascia entrare nella LAN il traffico di risposta a precedenti richieste uscite dalla LAN
d filtra solo gli indirizzi IP

Domande per la prova orale

25 Che cos'è un firewall?

26 Che cosa si intende per "personal firewall"?

27 Che cos'è un proxy server?

28 Quali problemi risolve un proxy server?

29 Che cos'è una DMZ e quali problemi risolve?

30 Che cosa si intende per port forwarding?

31 Come si può realizzare una DMZ?

32 Quali sono le principali differenze tra un router e un firewall?

33 Che cosa si intende per "reverse proxy"?

34 Configurare un router usando ACL per permettere il traffico proveniente dalla rete 10.0.0.0 e contemporaneamente bloccare quello da altre reti.

35 Considerare la rete LAN di una organizzazione con un'unica sede. Le politiche dell'organizzazione hanno evidenziato, tra le altre, le seguenti necessità:

- la rete deve essere protetta da eventuali attacchi o traffico indesiderato;
- l'organizzazione ha un data center on premise (interno) e gestisce in proprio il sito web e i servizi di e-commerce;
- tutti i lavoratori possono accedere al Web.

Fare un elenco puntato delle soluzioni da adottare per far fronte alle necessità elencate, motivando le scelte fatte.

36 Configurare un router con ACL per consentire:

- richieste HTTP dall'interno della LAN;
- risposte HTTP provenienti dall'esterno associate a precedenti richieste.

Spiega quali informazioni devono essere prese in considerazione per attuare questa regola.

37 Configurare tre interfacce di un router per creare una DMZ, impostare il NAT dinamico dalla LAN verso l'esterno e il NAT statico verso un server web pubblico.

38 Configurare un port forwarding su un router, per accedere a un server web su una LAN. Fare anche il disegno della rete.

39 Illustra come il port forwarding può essere utilizzato nell'ambito della domotica.

40 Racconta di quella volta in cui hai dovuto aprire una porta su un router per un gioco multiplayer.



Esercizi in più

Perimeter Security

Abstract

A firewall is a hardware or software device placed in the perimeter area of a network, that is, at the point where the LAN connects to the Internet, in order to protect the LAN. It monitors inbound and outbound traffic, as the drawbridge of a castle. A firewall can operate in different ways. At the network or application layer, it filters packets by IP address, by port or by checking SYN and ACK flags in order to control inbound and outbound requests for connections. At the application layer, it can authenticate users (assuming the role of a proxy server) or check the actual content of the data.
A firewall can then be configured to define a DMZ (i.e. a part of the local network to which servers are typically connected on the Internet) in order to protect the LAN from any intruders that may use these servers to get to corporate resources. Other measures used for perimeter security are: Access Control Lists (a set of rules applied to an interface of a router or firewall, inbound or outbound, to determine which packets can enter or leave a network), the DMZ (a technique to isolate public servers on a LAN), the use of proxy servers (a system, computer, or application that acts as an intermediary between a LAN host and websites or Internet resources).

Questions

Answer all questions

1 What is a firewall?
2 What is a proxy server?
3 How to set up ACLs?
4 What is a DMZ?

Choose the correct answer

5 The firewall packet filtering mode
- a is only used on a LAN's clients
- b filters connection requests
- c filters inbound or outbound users
- d filters inbound or outbound applications

6 A proxy server
- a is an Internet server
- b works on the network layer
- c works on the application layer
- d is connected to the DMZ

7 The DMZ:
- a is used to allow web access at an ISP
- b is used to isolate the proxy server
- c is used to isolate public servers on a LAN
- d is a next-generation firewall

8 A firewall
- a is a particular application
- b is a hardware or software device
- c is a part of a VLAN
- d is the most peripheral part of a LAN

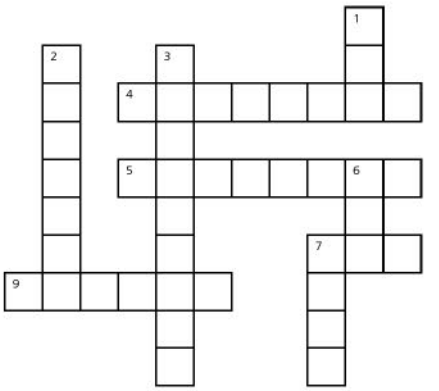
Crosswords

Across

4 Device that controls incoming or outgoing traffic of a LAN
5 Firewall that keeps track of the state of a connection
7 Isolates public servers in a LAN
9 Authorize data traffic

Down

1 Rules used to filter traffic on routers or firewalls
2 Function of a proxy that receives requests from the Internet and forwards them to the LAN hosts
3 It is the function of a firewall
6 Integrates various security functions into a single solution
7 Traffic denial

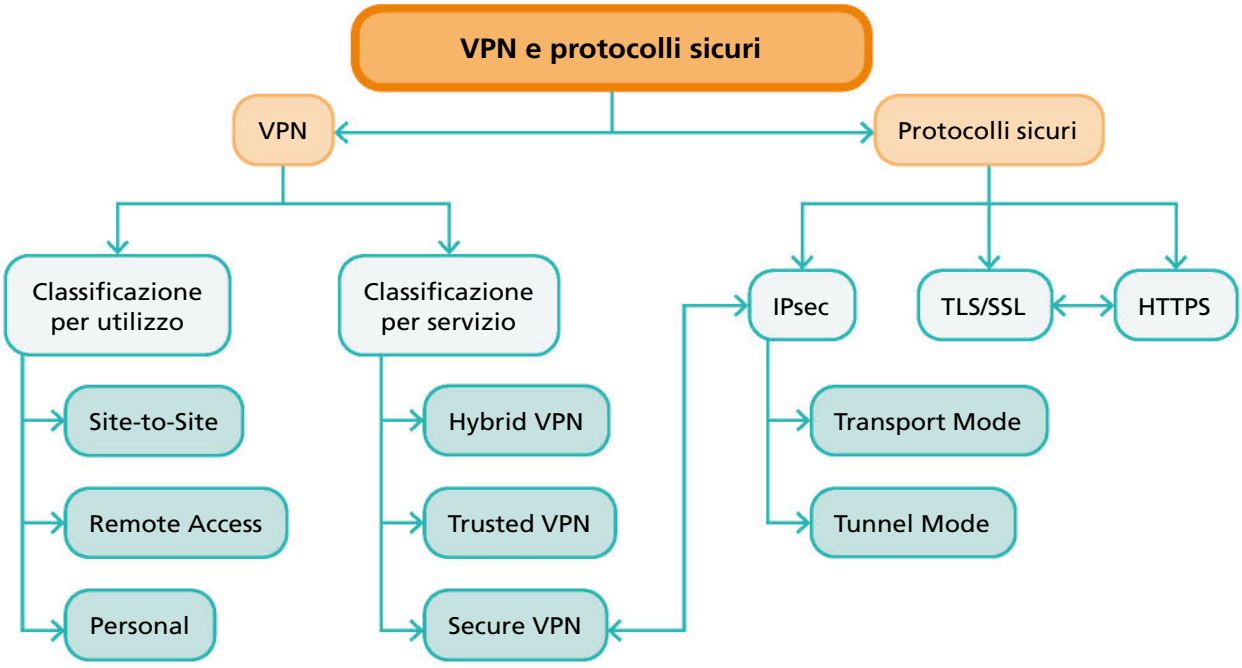




Unità

6

VPN e protocolli sicuri



Visione d'insieme

- Le VPN: cosa sono, classificazione per utilizzo e per modalità di servizio, come si usano.
- Protocolli sicuri di livello Rete, livello Trasporto: IPsec, TLS.
- I protocolli sicuri di livello Applicazione e HTTPS.

1 Introduzione

Internet è uno strumento indispensabile per la nostra vita quotidiana. Tuttavia, nonostante i suoi numerosi vantaggi, presenta anche dei rischi. Ad esempio, i nostri dati, trasmessi in rete, possono essere intercettati e rubati.
La **VPN** (**V***irtual* **P***rivate* **N***etwork*) è una tecnologia che crea una "rete privata virtuale", scavando una sorta di "tunnel" all'interno della rete Internet. La crittografia applicata alla trasmissione dei dati sulle VPN garantisce sicurezza, privacy e anonimato, anche quando si accede a Internet da un ambiente pubblico. L'utilizzo di una VPN è incoraggiato per diverse ragioni:

- L'esigenza di collegare sedi lontane e distaccate di un'azienda alla rete della sede centrale in modo sicuro;
- La possibilità di collegarsi da casa lavorando in smart working;
- La necessità di proteggere la privacy navigando nell'anonimato e di aggirare eventuali blocchi geografici che impediscono l'accesso a determinate risorse.

In questa unità, esploreremo come funziona una VPN, perché è importante, e quali sono i protocolli di sicurezza che vengono applicati alle VPN e ad altri protocolli a livello Appliczione.

2 Cos'è una VPN

La VPN è una rete privata virtuale che utilizza la rete pubblica (Internet) per collegare dispositivi remoti come se appartenessero alla stessa rete locale privata.
Le reti VPN sono:

- **private** perché la comunicazione tra LAN remote le fa apparire come appartenenti alla stessa rete privata;
- **virtuali** perché i collegamenti non sono fisici, ma logici, sopra un'infrastruttura di rete pubblica.

notabene

In genere una VPN utilizza Internet come infrastruttura geografica. A volte, in realtà aziendali che hanno particolari esigenze, sono usate reti geografiche fornite da un operatore di telecomunicazione che eroga il servizio utilizzando specifici protocolli.

In questo modo dispositivi remoti sono connessi tra loro come fossero su una stessa rete privata, con la differenza che al posto del collegamento fisico (cavo o Wi-Fi) è stabilito un collegamento che può essere di due tipi:

- predefinito e riservato;
- tunnel VPN su cui i dati transitano cifrati (tunneling).

La VPN nasce principalmente:

- per consentire il collegamento da remoto a risorse aziendali, come per esempio, server di storage. Per esempio, un lavoratore che lavora in una postazione esterna e remota (come nel caso dello smart working) e deve accedere a risorse aziendali;
- per consentire di collegare sedi aziendali remote, per esempio sedi di un'azienda dislocate in città o paesi diversi.

La VPN è usata anche per navigare in anonimato utilizzando servizi offerti in rete. In questo caso, il client si collega al server di un fornitore del servizio tramite un tunnel virtuale e criptato e con un indirizzo IP non riconducibile al proprio PC.

La Tabella 1 sintetizza i vantaggi offerti dalle VPN e gli svantaggi che comporta.

Pit Stop

1 Che cosa sono le VPN e quali sono i motivi per cui sono nate?

VPN	
Vantaggi	**Svantaggi**
• **Riduzione dei costi**: non è necessario affittare delle linee dedicate (molto costose) per collegare tra loro le varie sedi. • **Utilizzo di risorse già disponibili**: è possibile utilizzare i normali collegamenti a Internet già presenti nelle aziende. • **Flessibilità di accesso alle risorse**: con gli opportuni permessi, si può accedere a una risorsa della propria azienda indipendentemente dalla sede in cui ci si trova in quel momento. • **Connessioni sicure**: tutte le trasmissioni sono automaticamente cifrate. • **Architettura facilmente scalabile**: è molto semplice e veloce aggiungere ulteriori sedi alla rete aziendale. • **Supporto dei servizi in video e voce** con protocollo di cifratura. • **Semplicità d'uso**. • **Anonimato**: una VPN può mascherare l'identità online, rendendo più difficile tracciare le attività online. • **Accesso a contenuti bloccati geograficamente**: alcuni contenuti online possono essere bloccati in determinate regioni o paesi. La VPN può aggirare questi blocchi, dando l'impressione di navigare da un'altra posizione. • **Sicurezza su reti Wi-Fi pubbliche**: una connessione VPN è crittografata, proteggendo da potenziali attacchi. • **Controllo degli accessi** (pro): solo gli utenti autorizzati possono accedere a determinate risorse. Questo può essere particolarmente utile in un contesto aziendale, dove è importante proteggere le informazioni sensibili.	• **Riduzione della velocità di connessione**: la necessità di crittografare i dati e poi inviarli a un server VPN può ridurre la velocità di connessione. • **Complessità**: sebbene molte VPN siano facili da usare, la configurazione e la manutenzione di una VPN possono essere complesse. • **Costi**: alcune VPN sono gratuite, altre richiedono un pagamento. • **Problemi di privacy**: nonostante una VPN migliori la privacy, il provider della VPN può controllare le attività online. • **Controllo degli accessi** (contro): la gestione delle credenziali degli utenti e l'implementazione di politiche di accesso possono essere complesse e richiedere tempo. Inoltre, la perdita o il furto delle credenziali di accesso possono portare a violazioni della sicurezza.

← **Tab. 1** Vantaggi e svantaggi delle VPN.

3 La classificazione delle VPN

Possiamo classificare le VPN secondo due criteri diversi.
Cominciamo con l'osservare le VPN "da lontano", come quando in fisica studiamo il comportamento di un gas a livello delle sue variabili di stato: temperatura, volume ecc.

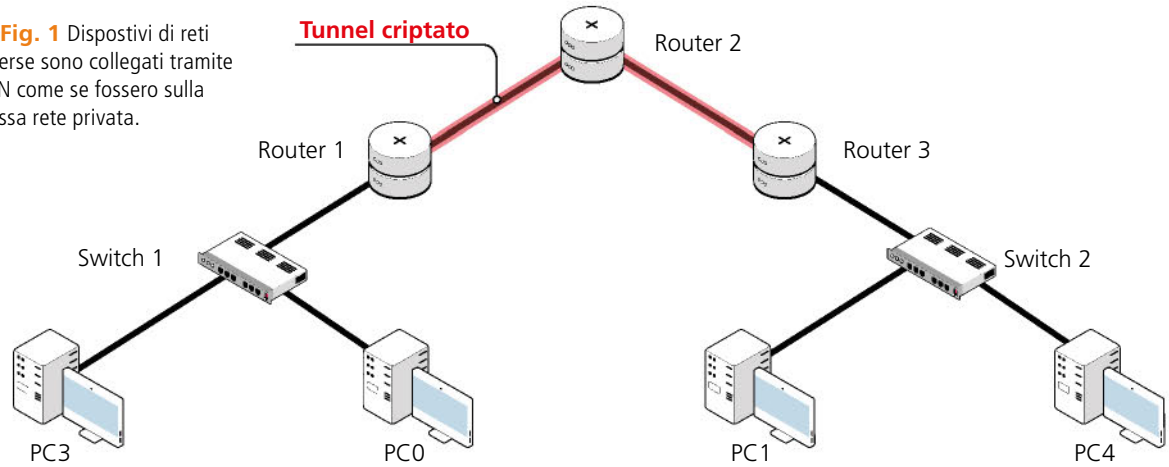
In questo senso possiamo classificare le VPN in base al loro utilizzo e, in particolare, al modo in cui comunicano.
Se osserviamo le VPN "da vicino", andando a studiare il loro comportamento, come se fossero le molecole del gas che si muovono e si urtano tra loro, possiamo classificare le VPN in funzione del livello di sicurezza e affidabilità.
Ci sono diversi tipi di VPN che possono essere classificate in base al tipo di servizio prestato o in base al livello di sicurezza e affidabilità fornito.
In base all'utilizzo, le VPN si suddividono in:

- **Site-to-Site VPN**: per stabilire una connessione sicura in Internet tra sedi aziendali remote;

- **Remote Access VPN**: per l'accesso a risorse aziendali da remoto da un qualsiasi client;
- **Personal VPN**: usata da utenti individuali per navigare in maniera anonima o per aggirare zone geografiche.

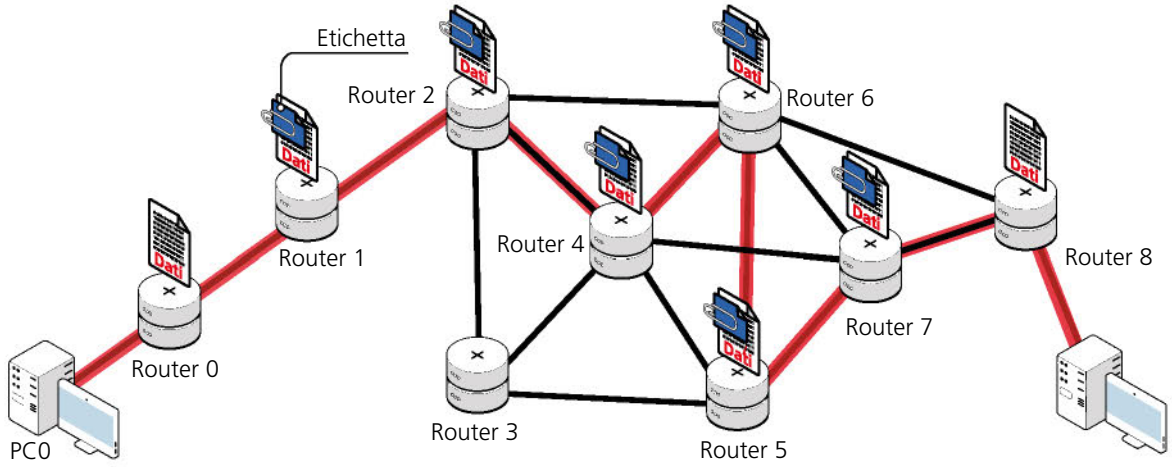
In base al livello di sicurezza e affidabilità richiesto, le VPN si suddividono in:

- **Secure VPN**: hanno come obiettivo la **sicurezza** in termini di riservatezza. Utilizzano tunnel virtuali sicuri su Internet con protocolli come IPsec o TLS. Un utente (o un'applicazione) può trasmettere da qualsiasi dispositivo della rete in sicurezza poiché i dati viaggiano criptati. In questo caso la VPN crea "**tunnel virtuali**" (Figura 1) nei quali i dati sono cifrati all'entrata del tunnel e decifrati all'uscita. Un pacchetto, prima di uscire sulla rete, è criptato e incapsulato in un ulteriore pacchetto dal software VPN. Quando giunge a destinazione deve essere decriptato dal software VPN.



➜ **Fig. 1** Dispostivi di reti diverse sono collegati tramite VPN come se fossero sulla stessa rete privata.

- **Trusted VPN**: hanno come obiettivo la **qualità del servizio**. Un ISP crea e gestisce la rete privata, definendo un percorso dedicato (Figura 2) su cui viaggiano i pacchetti per ottenere un buon QoS (*Quality Of Service*).



↑ **Fig. 2** Nella Trusted VPN, l'ISP definisce un percorso dedicato per l'instradamento dei pacchetti al fine di aumentare la qualità del servizio. Il percorso è identificato da un'etichetta aggiunta al pacchetto.

È utilizzato il protocollo MPLS (*MultiProtocol Label Switching*) che aggiunge un'etichetta ai pacchetti per identificare il percorso che i router devono utilizzare nel routing, come se fosse definito un circuito virtuale.

La **Tabella 2** riassume la classificazione delle VPN.

← Tab. 2

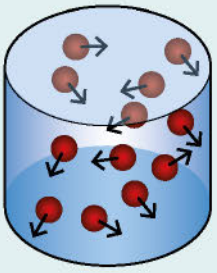
Classificazione Generale delle VPN	Descrizione
Site-to-Site VPN	Collegano reti in luoghi diversi tramite Internet, ideali per aziende che vogliono estendere la propria rete.
Remote-Access VPN	Consentono l'accesso remoto a reti aziendali, garantendo sicurezza anche da luoghi pubblici.
VPN personali	Destinate all'uso individuale per proteggere la privacy online.
Classificazione per Sicurezza e Affidabilità	**Descrizione**
Secure VPN	Utilizzano tunnel sicuri su Internet con protocolli come IPsec o TLS.
Trusted VPN	Si affidano alla rete di un provider di servizi di fiducia che offre un'infrastruttura sicura e scalabile.
Hybrid VPN	Combinano le caratteristiche delle VPN Secure e Trusted.

Pit Stop

2 Come possono essere classificate le VPN?

Comprendi con l'analogia

Lo studio di una VPN è come l'analisi degli stati di un gas



Nell'analisi dei gas in fisica, possiamo riferirci al **macrostato** o al **microstato**. Osservare il macrostato di un gas, come la sua temperatura o pressione, significa osservarlo "da lontano", da una prospettiva esterna, senza considerare le sue componenti interne, che vengono volutamente trascurate. Allo stesso modo, quando definiamo una VPN Site-to-Site, la stiamo classificando in base al suo utilizzo e al modo in cui funziona, senza entrare nel dettaglio di come è strutturata internamente e dei protocolli che la supportano.

Quando studiamo un gas dal punto di vista dei suoi microstati, invece, esaminiamo lo stato di tutte le sue componenti, come la posizione e la velocità di ogni singola molecola o atomo che compone il gas. Analogamente, classificare le VPN "da vicino" significa indagare i protocolli e i metodi di crittografia utilizzati, ad esempio, per creare un tunnel su Internet.

Questo ci porta a una considerazione finale: in fisica, passare dal microstato al macrostato è relativamente semplice utilizzando metodi statistici come la media. Tuttavia, il passaggio inverso è molto più complesso perché, ad esempio, la stessa temperatura può essere raggiunta con microstati diversi. Allo stesso modo, il funzionamento di una VPN Site-to-Site può essere ottenuto con una varietà di protocolli e sistemi crittografici differenti.

Nei prossimi paragrafi, approfondiremo i protocolli di sicurezza **IPsec** (**I***nternet* **P***rotocol* **S***ecurity*) e **TLS** (**T***ransport* **L***ayer* **S***ecurity*), esaminandone le caratteristiche, il funzionamento e le applicazioni pratiche. Inoltre, nella Tabella 4, classificheremo alcuni dei principali protocolli di sicurezza in base ai livelli dello **stack TCP/IP**, fornendo un'analisi comparativa che evidenzia come ciascun protocollo operi a diversi strati per garantire la sicurezza delle comunicazioni in rete.

Site-to-Site VPN

Una **VPN Site-to-Site è progettata per connettere tra loro due o più reti**. Ad esempio, potrebbe collegare la rete aziendale alla rete di una filiale situata in una diversa area geografica.

notabene

Una VPN site-to site non tratta di connessioni individuali per ogni utente, ma riguarda una singola connessione tra reti.

Questo tipo di VPN crea una sorta di tunnel attraverso Internet, con lo scopo di proteggere i dati aziendali da possibili intercettazioni. Per questo si utilizzano dei protocolli sicuri che crittografano i dati in transito (Figura 3).

Il tunnel VPN è stabilito tra i dispositivi di rete (gateway o router, spesso chiamati *Customer Premises Equipment*) situati nelle sedi remote, attraverso cui passa il traffico dati. Questo significa che i dispositivi all'interno della rete non necessitano di alcun software specifico di configurazione. Inoltre, le VPN Site-to-Site offrono un livello di sicurezza elevato, poiché tutti i dati trasmessi tra le sedi sono criptati. Questo rende molto difficile per gli attaccanti intercettare o compromettere i dati. Tuttavia questo tipo di VPN va configurato su tutte le reti delle diverse sedi e richiede una manutenzione complessa e non alla portata di tutti. Inoltre le VPN Site-to-Site non funzionano per un dipendente che lavora in smart working o da una postazione pubblica, perché l'azienda non ha alcun controllo sulle reti che sta usando.

Le VPN Site-to-Site utilizzano una serie di protocolli per la creazione del tunnel, stabilire una connessione sicura e per crittografare i dati. Tra questi il più noto è certamente **IPsec**.

Pit Stop

3 Quali sono le principali caratteristiche delle VPN Site-to-Site?

Intranet ed Extranet

Le VPN Site-to-Site possono essere ulteriormente classificate in Intranet o Extranet (Figura 4). Una VPN intranet collega gli uffici della stessa azienda. La VPN extranet è creata per connettere all'azienda un partner o un cliente. Questo permette una comunicazione sicura e protetta anche con entità esterne all'azienda.

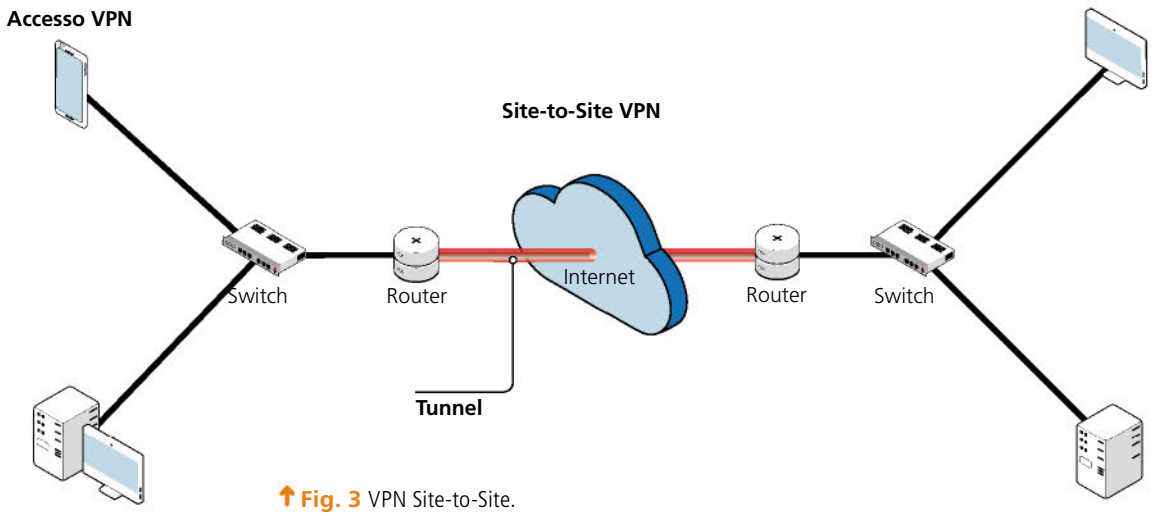


Fig. 3 VPN Site-to-Site.

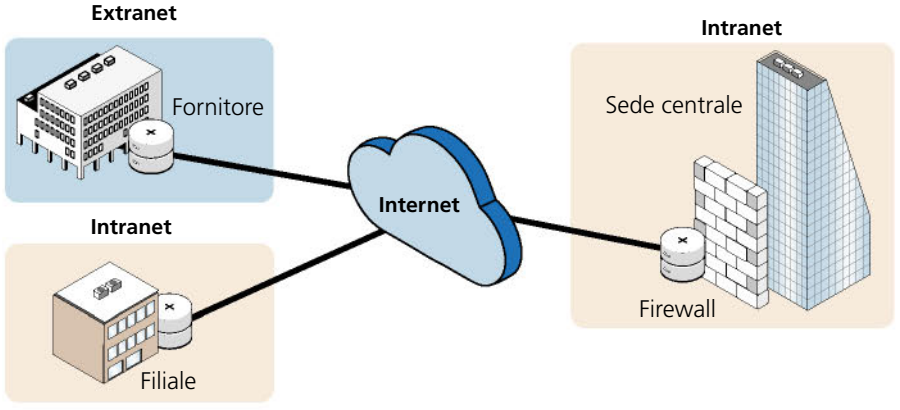
Vediamo nel dettaglio i servizi di Intranet ed Extranet:

- **Intranet** È una rete locale all'interno di un'organizzazione che utilizza i protocolli di Internet.
  - Fornisce servizi e risorse ai dipendenti all'interno dell'azienda o dell'organizzazione. Ad esempio:
    - pagine web interne con informazioni come orari, corsi,stipendi ecc.
    - posta elettronica interna;
    - repository documentali;
    - forum per la collaborazione interna.
  - Accesso dall'esterno: i dipendenti che lavorano in smart working o per coloro che effettuano servizi commerciali presso i clienti.
- **Extranet** È una parte dell'Intranet aperta a persone esterne all'organizzazione, coinvolgendo partner commerciali, fornitori o clienti:
  - fornisce un accesso sicuro a risorse aziendali per collaboratori esterni; per esempio, un ospedale può rendere disponibili ai pazienti il servizio di prenotazione o le loro schede mediche. Un ufficio di contabilità potrebbe fornire l'accesso ai suoi clienti per le pratiche fiscali. I fornitori che collaborano con l'azienda possono aver bisogno di accedere a determinati servizi o risorse (ad esempio, un sistema di gestione degli ordini);
  - la sua implementazione viene realizzata tramite una VPN per garantire la sicurezza dei dati scambiati.

L'utilizzo di una VPN per l'accesso sia all'Intranet che all'Extranet è cruciale per assicurare confidenzialità e sicurezza dei dati durante la comunicazione tra le reti. Con l'evoluzione verso il cloud computing e il lavoro da remoto, diventa essenziale adottare soluzioni di rete meno dipendenti da località fisiche. Per esempio, è necessario un modello che faciliti l'accesso alle risorse aziendali direttamente attraverso un'infrastruttura cloud. In questo contesto, il **Secure Access Service Edge** (**SASE**) emerge come una soluzione innovativa, offrendo servizi di connettività e sicurezza di rete necessari alle imprese, gestiti direttamente tramite un'infrastruttura cloud.

notabene

Ogni utente che utilizza una VPN di accesso remoto ha la propria connessione individuale con la rete privata remota.



← **Fig. 4** VPN intranet ed extranet.

Remote Access VPN

Le VPN di accesso remoto sono progettate per permettere agli utenti di connettersi dalla propria postazione a una rete privata remota.

notabene

Il client VPN può essere installato tanto su un dispositivo individuale, come un PC o uno smartphone, quanto su un router di accesso, a seconda delle esigenze dell'utente e della configurazione della rete aziendale. Installare il client VPN su un router permette a tutti i dispositivi connessi a quel router di accedere alla rete aziendale tramite la VPN.

notabene

ISAKMP (*Internet Security Association and Key Management Protocol*) è un protocollo definito dall'RFC 2408 che definisce i formati per lo scambio di chiavi e dei dati di autenticazione per stabilire associazioni di sicurezza (SA).

Una VPN remote access è utilizzata, ad esempio, da un dipendente che lavora in mobilità e che si trova fisicamente lontano dalla sede aziendale, per accedere alle risorse della rete locale come se fosse fisicamente presente in azienda, oppure dai fornitori esterni all'azienda che si collegano dai loro uffici.
Non è raro che sia l'azienda stessa a stabilire le regole di accesso ai propri server e fornisca il software client VPN, installabile sia su un dispositivo individuale sia su un router di accesso, per instaurare la connessione VPN e criptare i dati trasmessi. In questo modo, sia i singoli dipendenti in mobilità sia i dispositivi in una sede remota possono operare in sicurezza, indipendentemente dalla loro posizione geografica, usufruendo dello stesso livello di protezione di una postazione fisica.
La **configurazione di una VPN** è un processo complesso che comprende una serie di elementi, tra cui:

- un server VPN che serve a:
  - creare un tunnel sicuro e crittografato attraverso Internet;
  - crittografare i dati trasmessi attraverso il tunnel;
  - dirigere il traffico di rete attraverso il tunnel VPN;
  - assicurare una connessione sicura e controllata, proteggendo la privacy degli utenti e la sicurezza dei dati aziendali, applicando le regole di un server AAA (Autenticazione, Autorizzazione, Accounting): gestire le richieste di accesso, eseguire l'autenticazione definendo anche il modo di autenticazione, come ad esempio password o altro; concedere o negare l'autorizzazione a usufruire delle risorse a cui gli utenti possono accedere una volta autenticati, e tener conto delle attività dell'utente;
- l'individuazione della policy ISAKMP (*Internet Security Association and Key Management Protocol*) con l'impostazione dell'algoritmo di crittografia, il metodo di autenticazione e l'algoritmo di hashing;
- l'assegnazione di un insieme di indirizzi IP che verrà assegnato agli utenti remoti quando si connettono alla VPN, utile anche per filtrare il traffico;
- la definizione del profilo dei client VPN con nome, chiavi, regole di accesso e numero di utenti.

La Figura 5, insieme alla Tabella 3, mostra un esempio con lo schema di una VPN ad accesso remoto. L'utente remoto si collega, tramite un router configurato come client VPN, al server VPN presente in azienda. I dati transitano in un tunnel crittografati con il protocollo IPsec. I router hanno un indirizzo IP pubblico verso

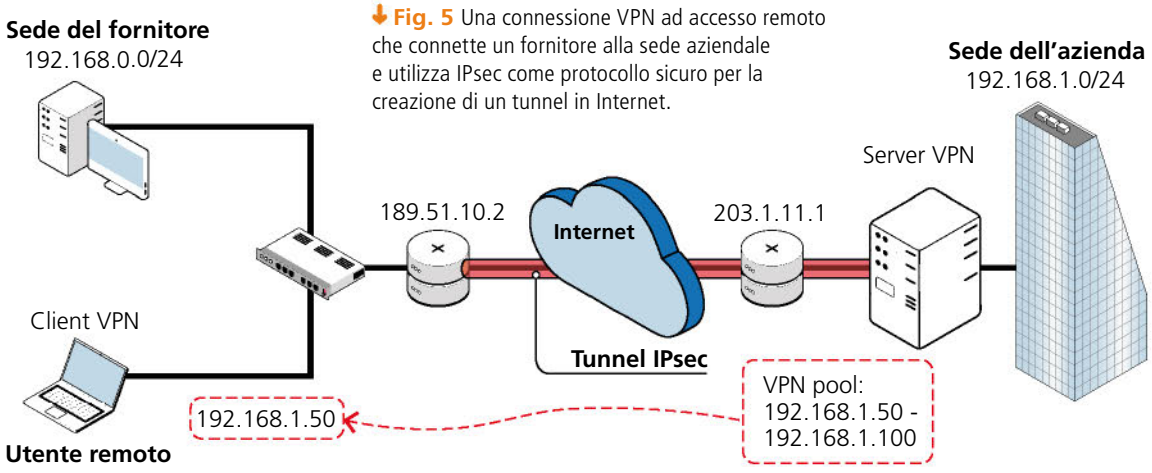


Fig. 5 Una connessione VPN ad accesso remoto che connette un fornitore alla sede aziendale e utilizza IPsec come protocollo sicuro per la creazione di un tunnel in Internet.

Internet. Le reti LAN hanno indirizzi privati. È possibile configurare un pool di indirizzi IP che la sede centrale assegna dinamicamente ai client VPN remoti durante la connessione. Quando un dispositivo della sede remota si connette alla VPN, riceverà un indirizzo IP dal pool VPN della sede centrale, permettendogli di accedere alle risorse come se fosse fisicamente presente nella sede centrale.

Sede	Tipo di Indirizzo	Range di Indirizzi LAN	Indirizzo IP Pubblico	Pool VPN
Centrale (Azienda)	Locale	192.168.1.0/24	203.1.11.1	192.168.1.50-192.168.1.100
Remota (Fornitore)	Locale	192.168.0.0/24	189.51.10.2	il Server VPN della sede centrale assegnerà un indirizzo IP preso dal pool VPN, come ad esempio 192.168.1.50.

← **Tab. 3** Configurazione della rete ad accesso remoto di **Fig. 5**.

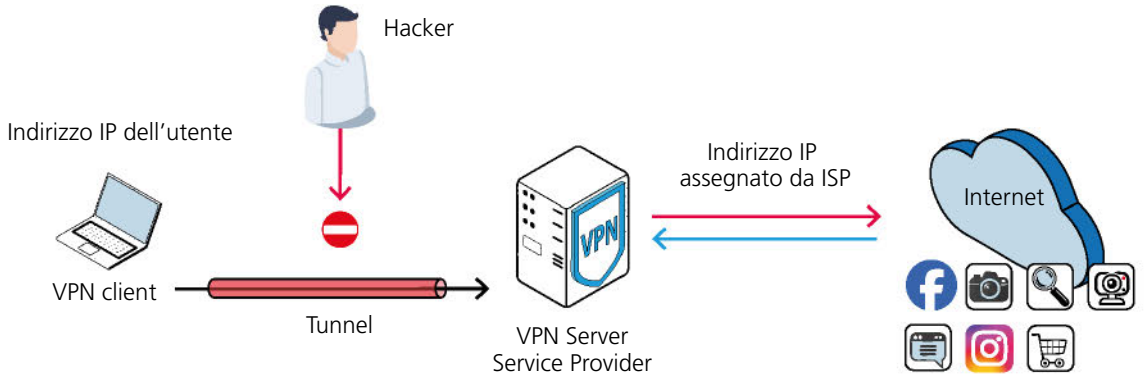
Le VPN di accesso remoto si avvalgono di diversi protocolli per stabilire una connessione sicura e per criptare i dati e creare il tunnel, tra cui **IPsec** e **TLS**.
In particolare le **VPN SSL** sono un tipo di VPN che sfrutta un browser web, insieme al protocollo SSL/TLS. Gli utenti autenticati possono utilizzare la VPN SSL per connettersi al server remoto e accedere ai servizi di rete.

Pit Stop

4 Quali sono le principali caratteristiche delle VPN Remote Access?

VPN personali

Una VPN personale è destinata agli utenti privati che si avvalgono di un fornitore di servizi per aggirare blocchi geografici, censure, discriminazioni o limitazioni che impediscono l'accesso diretto a determinate risorse online. Una VPN di questo tipo maschera l'indirizzo IP pubblico con cui l'utente si collega al proprio ISP. Quando l'utente collega il proprio dispositivo al server di un provider, il pacchetto dati, contenente l'IP dell'utente, viene criptato e inviato al server VPN. Quest'ultimo decifra il pacchetto e lo invia in Internet con il proprio indirizzo IP, nascondendo completamente l'origine del pacchetto (**Figura 6**).



↑ **Fig. 6** La connessione VPN personale è divisa in due parti: il client VPN, con il proprio indirizzo IP, si collega al server VPN tramite un canale sicuro. Dal server del provider i dati, non crittografati, sono replicati in Internet con un indirizzo IP nuovo, assegnato dal provider

In questo modo, è impossibile risalire alla posizione geografica dell'utente, mantenendo le attività online completamente riservate e proteggendo l'utente da hacker, provider, curiosi e persino autorità governative. La navigazione è protetta da crittografia.
Le VPN personali, oltre a superare le restrizioni geografiche che applicano servizi e tariffe diverse a seconda del paese di provenienza, sono utilizzate per proteggere la navigazione Wi-Fi in luoghi pubblici, mantenere riservati i dati sensibili durante l'home banking, fare e-commerce e in qualsiasi situazione in cui sia necessaria sicurezza e riservatezza.
Per utilizzare una VPN personale, un utente può utilizzare un client VPN, come OpenVPN, configurato con le credenziali fornite dal provider, oppure può servirsi di un servizio, pronto all'uso e già preconfigurato, offerto da uno dei molti provider che forniscono VPN.

Pit Stop

5 Quali sono le principali caratteristiche delle VPN personali?

6 Che cosa sono le Trusted VPN e qual è il loro principale utilizzo?

Trusted VPN

La **trusted VPN** è un tipo di VPN gestito da un provider esterno che traccia i tunnel, simili a circuiti virtuali, nei quali transitano i dati. Nel corso degli anni, si è passati dal noleggio di circuiti privati offerti dai fornitori di telecomunicazioni a reti IP private noleggiate dai fornitori di servizi Internet. In questo contesto, gli utenti si affidano alla "fiducia" che i dati siano protetti durante il loro percorso. Ne fanno uso, in particolare, le aziende che non hanno le risorse o l'esperienza per gestire una VPN internamente e che trovano più efficiente affidare la gestione e la manutenzione dell'infrastruttura VPN al provider di servizi.
Attualmente, la soluzione più diffusa per una VPN trusted è quella basata sul protocollo **MPLS** (***M**ultiprotocol **L**abel **S**witching*), utilizzato per l'incapsulamento e la gestione del routing all'interno della rete dell'operatore (Figura 7):

- il pacchetto che parte dal router della sede A viene inoltrato al nodo edge del fornitore, su cui è implementato il protocollo MPLS;
- al pacchetto viene aggiunta una "label" (una nuova intestazione) tra l'header di livello 2 (PPP o Ethernet) e quello di livello 3 (IP). Questa label identifica il pacchetto e gli permette di viaggiare attraverso i router di core fino ad arrivare al router dell'ISP di destinazione;
- il router dell'ISP di destinazione rimuove la "label" e consegna il pacchetto al router dell'utente nella LAN finale.

notabene

In generale, quando si cerca un servizio VPN affidabile, è importante considerare fattori come la privacy, la sicurezza delle connessioni e la velocità del servizio che contribuiscono a determinare la fiducia che si può riporre in un fornitore.

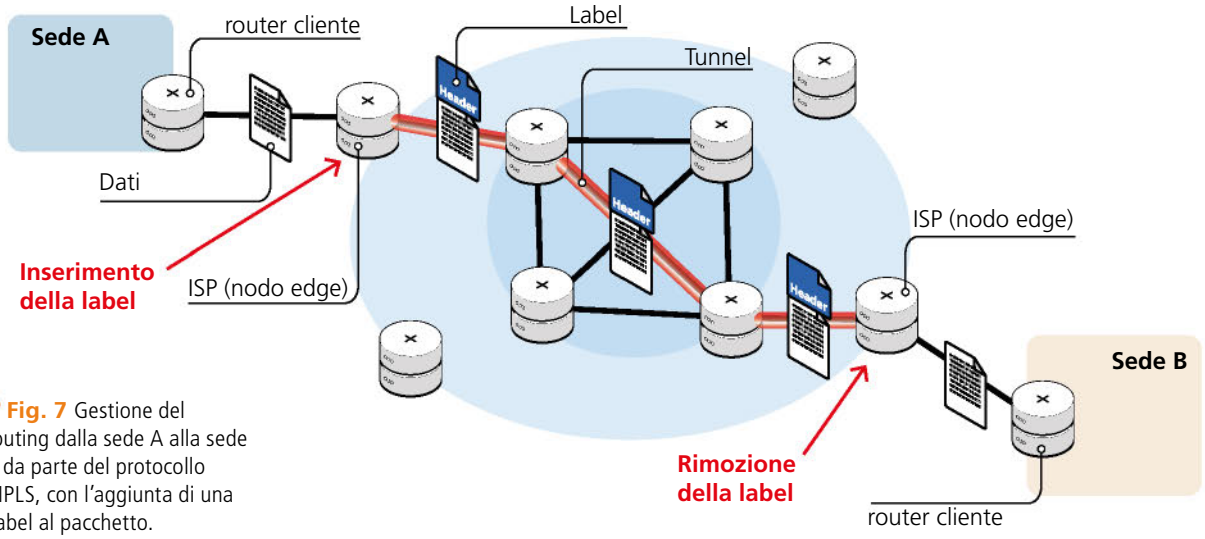


Fig. 7 Gestione del routing dalla sede A alla sede B da parte del protocollo MPLS, con l'aggiunta di una Label al pacchetto.

La trusted VPN presenta vantaggi in termini di sicurezza, affidabilità e qualità del servizio (QoS) che il cliente delega al fornitore.

- Qualità di servizio (QoS): la VPN definisce un percorso ottimale a carico del fornitore, consentendo al cliente di non preoccuparsi dei dettagli di implementazione e sicurezza;
- Sicurezza: la rete privata con infrastruttura e protocolli di instradamento proprietari, è protetta dall'hacking del traffico. Le label, che il protocollo MPLS applica ai pacchetti, consentono di distinguere le varie origini di traffico e di mantenere segregati i diversi flussi di dati.
- Algoritmi interni alla rete: si basano sulla priorità del traffico e consentono bassi tempi di ripristino da malfunzionamenti.
- Piano di indirizzamento IP: è quello del cliente, con la creazione di un'unica LAN logica in ambito geografico.

MPLS rende più efficiente il traffico di rete, ordinando i pacchetti di dati e fornendo loro delle priorità in base alla loro classe di servizio, come per esempio filmati o voce. Tuttavia, MPLS non è completamente al riparo da eventuali intrusioni: di fatto, si tratta di una peer-to-peer VPN con scambio di informazioni tra i router aziendali e quelli dell'ISP. Inoltre la mancanza di cifratura rende i pacchetti MPLS intercettabili.

Pit Stop

7 Quali sono le fasi principali del routing MPLS?

VPN a confronto

La **Tabella 4** permette di confrontare tra loro VPN di accesso remoto, VPN Site-to-Site, Trusted VPN e VPN personali.

↓Tab. 4

	VPN di Accesso Remoto	VPN Site-to-Site	Trusted VPN	VPN Personali
Chi si connette a cosa	L'utente si connette a una rete privata	La rete si connette a un'altra rete	L'utente o la rete si connette a una rete privata	L'utente si connette a una rete privata
Installare un software	Gli utenti devono installare un software sul dispositivo	Gli utenti non devono installare alcun software	Dipende dal provider del servizio	Gli utenti devono installare un software sul dispositivo
In genere si utilizza per	Connettersi alla rete aziendale, o altra rete privata, da casa o da una postazione remota	Unire due o più reti	Connettersi a una rete privata in modo sicuro e scalabile	Proteggere la privacy dell'utente durante la navigazione su Internet
Principali protocolli utilizzati	TLS, IPsec	IPsec	Dipende dal fornitore del servizio. MPLS	SSL, IPsec, PPTP, L2TP, OpenVPN, ecc
Numero di utenti	Ogni utente ha la propria connessione unica con la rete privata.	Connette due reti intere tra loro	Dipende dal provider del servizio	Di solito, è limitato a un solo utente
Configurazione del tunnel VPN	Ogni utente deve configurare il tunnel VPN	Gli utenti non hanno la necessità di configurare il tunnel VPN	Dipende dal provider del servizio	Ogni utente deve configurare il tunnel VPN

4 Sicurezza dei protocolli dal livello Rete al livello Applicazione

Pit Stop

8 Cosa significa "protocollo sicuro"?

9 Quali sono i principali protocolli sicuri relativi ai livelli del TCP/IP?

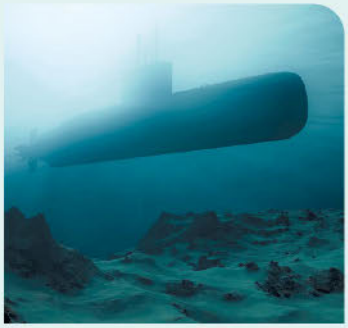
La crittografia viene applicata ai protocolli del modello TCP/IP a partire dal livello rete fino al livello applicazione. Rendere sicuro un protocollo di un determinato livello garantisce che lo siano anche quelli di livello superiore. Così, se viene applicata la crittografia a livello di rete, i protocolli di livello trasporto e applicazione saranno sicuri; se viene applicata a livello trasporto, le applicazioni saranno sicure. La Tabella 5 offre una panoramica sui protocolli principali che saranno oggetto di studio nei prossimi paragrafi.

Livello TCP/IP	Protocollo	Descrizione
Livello Applicazione	Kerberos	Kerberos è un protocollo di autenticazione utilizzato per verificare l'identità di un utente o di un host. È ampiamente utilizzato nei sistemi operativi Windows e in altre piattaforme.
	OpenVPN	OpenVPN è un software open source, tra i più utilizzati, che permette di stabilire un "tunnel" sicuro tra un client e un server VPN. È ampiamente utilizzato dai fornitori di servizi VPN e permette di configurare un server o una rete VPN autonomamente. Il protocollo utilizza la libreria OpenSSL che gestisce la crittografia e l'autenticazione.
	PGP (*Pretty Good Privacy*)	PGP è utilizzato per crittografare e decrittografare messaggi e file. È ampiamente utilizzato per la firma digitale e la protezione della privacy delle comunicazioni via e-mail e altri canali di messaggistica.
Livello Trasporto	TLS (*Transport Layer Security*)	TLS è un protocollo crittografico progettato per garantire la sicurezza delle comunicazioni su reti informatiche. Viene utilizzato in applicazioni come e-mail, messaggistica istantanea e HTTPS (RFC 8446).
Livello Rete	IPsec (*Internet Protocol Security*)	IPsec è un insieme di protocolli e algoritmi per fornire autenticazione, cifratura e controllo di integrità dei pacchetti IP. È spesso utilizzato per creare tunnel VPN per connessioni Site-to-Site (RFC 4301 e RFC 6071).

↑ Tab. 5 Classificazione di alcuni dei protocolli di sicurezza in base ai livelli dello stack TCP/IP.

Comprendi con l'analogia

Il Web è come un mare insidioso, pieno di risorse ma infestato da pirati

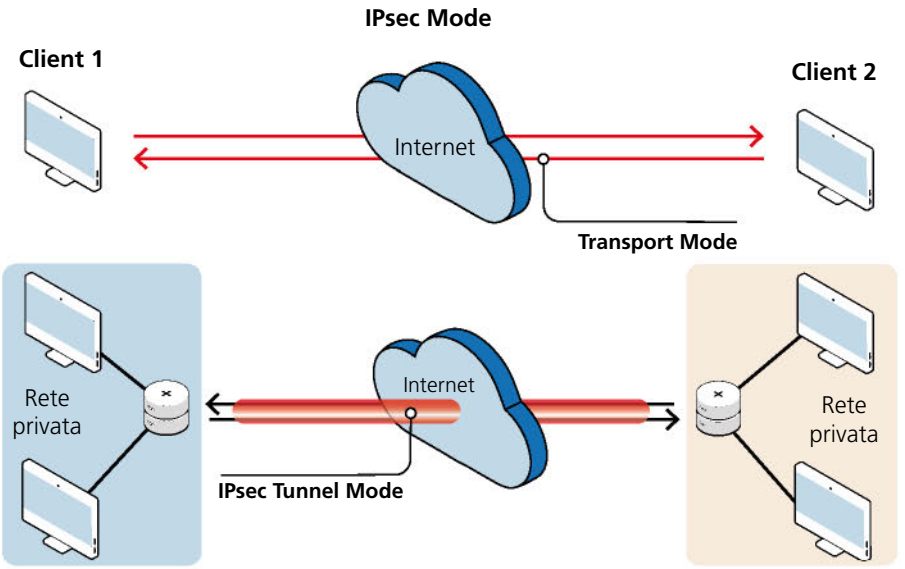


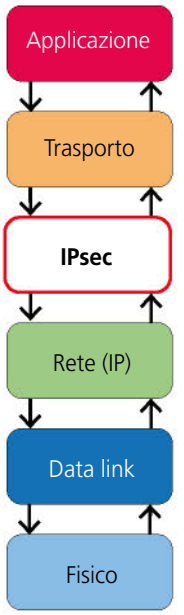
L'Oceano Sereno, con le sue innumerevoli isole e il mare calmo e cristallino, era un tempo considerato il paradiso della navigazione e del commercio. Navi di tutte le dimensioni solcavano liberamente le sue acque, scambiando merci e portando idee. Ma negli ultimi anni, la situazione è cambiata drasticamente. Il mare è ora pieno di insidie. Pirati, tempeste violente e reti da pesca fatte di acciaio robusto minacciano costantemente la sicurezza delle navi. I pirati, attratti da sogni di ricchezza, sono diventati così audaci e numerosi che è quasi impossibile viaggiare da un'isola all'altra senza essere attaccati, derubati o spiati. Tuttavia, le cose stanno cambiando. Una soluzione per proteggersi, seppur costosa, è stata trovata. Su ogni isola è stato installato un sistema avanzato di miscelazione e compressione che riceve le merci, le comprime e le mescola, creando un miscuglio che solo chi possiede il codice corretto può decomprimere e riportare allo stato originale. Queste merci sono messe in container e caricate sulle navi, che hanno ripreso a solcare le acque.
Ma c'è ancora di più. È stata creata una flotta speciale, diversa da tutte le altre, composta da sottomarini, che navigano esclusivamente in immersione. Questi sottomarini seguono rotte diverse, rendendosi invisibili ai pirati, sfuggendo alle tempeste ed evitando le reti da pesca.
Nelle profondità dell'Oceano Sereno si celano caverne oscure, accessibili solo con batiscafi. Navigare in questi

5 Internet Protocol Security (IPsec)

IPsec opera direttamente sopra il protocollo di rete IP (Figura 8), creando un percorso sicuro tra host che comunicano attraverso una rete non sicura.
IPsec opera in due modalità (Figura 9 e Figura 10):

- **Transport Mode** (Modalità di trasporto). IPsec fornisce sicurezza solo al payload del pacchetto IP: l'header IP rimane invariato, mentre il contenuto del pacchetto viene crittografato e autenticato. È spesso utilizzato per proteggere la comunicazione tra dispositivi finali.
- **Tunnel Mode** (Modalità tunnel). IPsec mette in sicurezza l'intero pacchetto IP, compreso l'header IP. Il pacchetto originale viene incapsulato in un nuovo pacchetto IPsec. È spesso utilizzato per creare VPN e collegare reti aziendali attraverso Internet.





↑ Fig. 8 Livello del protocollo IP.

← Fig. 9 Transport mode: protezione end-to-end; Tunnel mode: comunicazione LAN-to-LAN.

Pit Stop

10 Che cosa è IPsec?

11 In quali modalità opera IPsec?

abissi può essere necessario, in certi casi, ma rischioso, poiché si possono incontrare creature che si nascondono negli anfratti più reconditi, e sirene il cui canto melodioso seduce, trascinando verso baratri insondabili, simili all'attrazione gravitazionale dei buchi neri, che inghiottono tutto oltre l'orizzonte degli eventi. L'analogia considera i protocolli di sicurezza che vengono utilizzati per proteggere i dati durante la navigazione in Internet:

«Una soluzione per proteggersi, seppur costosa, è stata trovata.» Si riferisce all'introduzione di protocolli, come TLS, che possono essere costosi in termini di risorse di sistema e di tempo di elaborazione, ma forniscono un alto livello di protezione.

«Ogni isola dispone ora di una macchina potente…» Descrive il processo di crittografia che rende i dati (le "merci") incomprensibili ai pirati informatici, anche se riescono a intercettarli. I dati vengono "compressi e mescolati" in un formato crittografato che può essere letto solo da chi possiede la chiave.

«Queste merci vengono poi messe in container e spedite sulle navi…» Si riferisce al processo di incapsulamento dei dati crittografati in pacchetti di dati ("container") che vengono poi inviati attraverso la rete ("navi").

«È stata creata una flotta speciale…» L'introduzione delle VPN, sono come un modo speciale nel modo di navigare in Internet: inviano i dati attraverso un "tunnel" crittografato, con protocolli come IPsec, rendendoli invisibili ai pirati informatici, alle tempeste di malware e alle reti di pesca di phishing.

«Nelle profondità dell'Oceano Sereno si celano caverne oscure…» Si riferisce al Dark Web, dove è possibile navigare solo con software speciali. Il Dark Web è conosciuto soprattutto perché è un rifugio per traffici illegali. Tuttavia può avere anche scopi legali, come ad esempio per rimanere anonimi o per opporsi a forme di repressione.

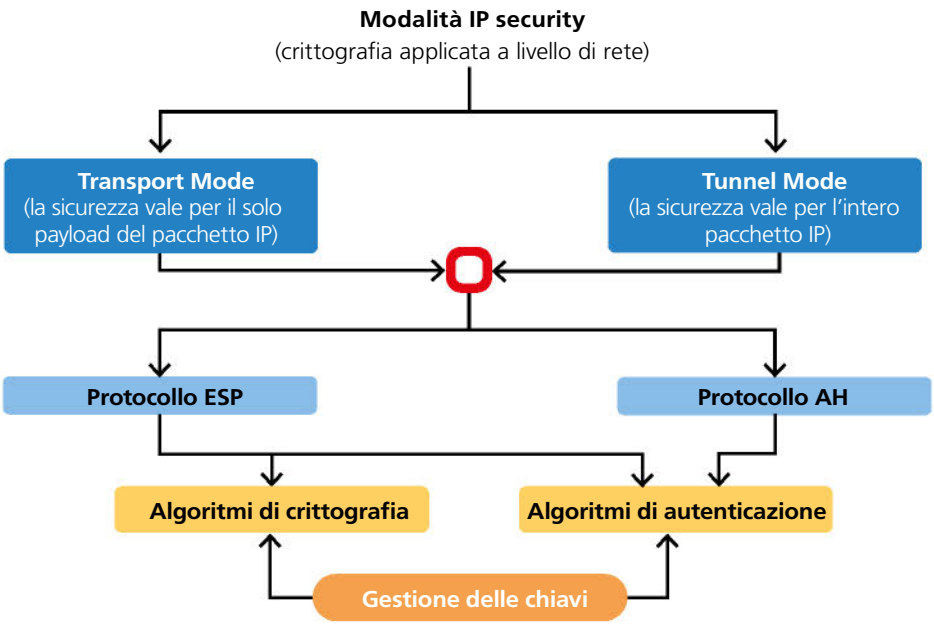


Fig. 10 IPsec prevede due modalità: *Transport mode* e *Tunnel mode*, con i protocollo AH e o ESP con la generazione e lo scambio di chiavi.

I protocolli AH e ESP

IPsec è supportato da due protocolli principali (**Figura 10**):

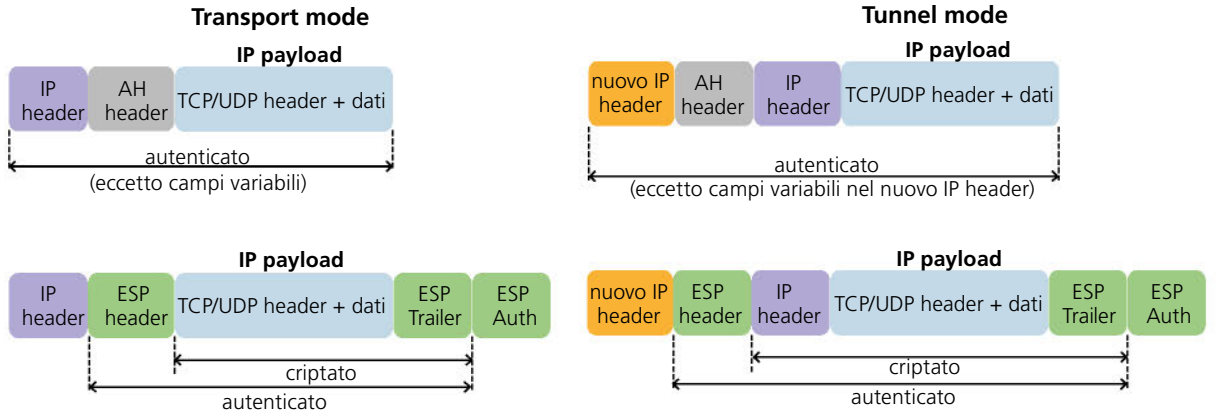
- **AH** (**A***uthentication* **H***eader*). Fornisce autenticazione e integrità per l'intero messaggio. L'header IP originale viene autenticato e il payload viene crittografato. AH non offre confidenzialità, ma garantisce che il messaggio non sia stato alterato durante la trasmissione.
- **ESP** (**E***ncapsulating* **S***ecurity* **P***ayload*). Garantisce autenticità, integrità e confidenzialità solo per il payload del messaggio. L'header IP originale viene incapsulato e crittografato. ESP è ampiamente utilizzato per creare canali sicuri tra host o reti.

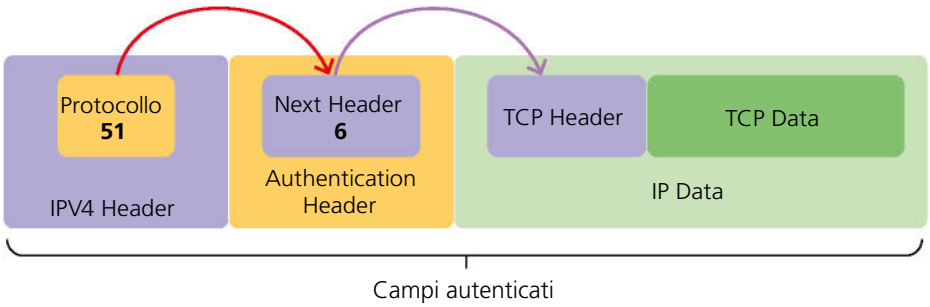
Pit Stop

12 Quali sono i protocolli che supportano IPsec?

Entrambi i protocolli possono essere utilizzati sia in Transport mode che in Tunnel mode, come si vede nella **Figura 11**, che illustra l'utilizzo di AH e ESP nel diversi casi e con le relative protezioni.
Concentriamo la nostra attenzione su Tunnel mode. Il tunnel che si crea serve al transito sicuro dei pacchetti IP privati. I pacchetti vengono completamente

Fig. 11 Transport mode con AH (**a.**) e ESP (**b.**); Tunnel mode con AH (**c.**) e ESP (**d.**).





← **Fig. 12** Intestazione AH all'interno di un pacchetto IP.

cifrati e incapsulati in un altro pacchetto nella cui intestazione sono contenuti gli indirizzi mittente e destinatario dei due router che costituiscono gli estremi del tunnel.
Utilizzato insieme a Authentication Header (AH) fornisce l'integrità e l'autenticazione di tutto il messaggio. Associato a Encapsulating Security Payload (ESP) garantisce autenticità, integrità e riservatezza del solo payload. Il funzionamento di questa modalità prevede la rimozione dell'intestazione del pacchetto IP originale e l'introduzione dell'intestazione "IPsec Header", che si traduce in "AH header" (**Figura 12**) oppure "ESP header" (si veda l'**Approfondimento**). Nel caso si utilizzi ESP, i dati vengono anche criptati, altrimenti si procede alla sola autenticazione del pacchetto. Infine viene applicato al pacchetto l'header IP originale

L'utilizzo di ESP in modalità tunnel impedisce di conoscere la sorgente del pacchetto, nascondendo gli indirizzi di origine e destinazione e la lunghezza del messaggio e fornisce un ottimo grado di riservatezza delle informazioni trasmesse.

La sicurezza e lo scambio delle chiavi in IPsec

IPsec utilizza sia la crittografia simmetrica che quella asimmetrica, ma per scopi diversi:

- La crittografia asimmetrica è utilizzata nella fase iniziale di negoziazione dei parametri del protocollo e, in particolare, nello "scambio di chiavi" affinché le due estremità di collegamento siano in grado di ottenere la stessa chiave condivisa senza compromettere la sicurezza.
- La chiave risultante (*chiave di sessione*) è utilizzata dalla crittografia simmetrica per offuscare i dati effettivi che vengono trasmessi e che sono contenuti nel payload.

Più precisamente IPsec utilizza diverse funzioni e protocolli per supportare la sicurezza:

- **SA** (**S***ecurity* **A***ssociation*). Un insieme di proprietà che definiscono come realizzare una comunicazione sicura tra due dispositivi. La SA descrive il tipo di connessione sicura che va instaurata, specificando i meccanismi usati, simile a un 'contratto'. Ogni SA ha un identificatore unico, un numero a 32 bit chiamato **SPI** (*Security Parameter Index*), che identifica il protocollo di sicurezza usato (AH o ESP) e l'indirizzo IP del dispositivo sorgente. Tutti i pacchetti che viaggiano su una SA avranno lo stesso SPI. Sono definiti anche gli algoritmi di cifratura da usare (ad esempio, MD5, SHA-1, DES), la chiave segreta per cifrare e autenticare il flusso di dati e le modalità di incapsulamento: transport o tunnel.
- **SAD** (**S***ecurity* **A***ssociation* **D***atabase*). È l'archivio delle SA attive in un sistema.

Pit Stop

13 Che cosa è una security association?

14 Che cos'è IKE?

- **SP** (***S**ecurity **P**olicy*). Sono le regole che informano IPsec su quali flussi di dati devono essere protetti da una specifica SA, includendo indirizzo IP sorgente e destinazione, porte, azioni da intraprendere, modalità di sicurezza (AH, ESP) e modalità di incapsulamento (transport, tunnel).
- **SPD** (***S**ecurity **P**olicy **D**atabase*). È un database che contiene le politiche usate per la gestione dei pacchetti in entrata e in uscita. Tra le azioni più utilizzate vi sono: "scarta", "non applicare" e "applica".
- **IKE** (***I**nternet **K**ey **E**xchange*). Le SA possono essere configurate manualmente o negoziate automaticamente tramite il protocollo IKE, che opera sulla porta 500 di UDP. IKE si occupa della generazione dinamica di nuove chiavi, creando chiavi di sessione diverse per ogni blocco di dati inviati. Questo assicura che, anche se un utente non autorizzato intercettasse una parte della comunicazione e la relativa chiave di sessione, non potrebbe avere tutte le informazioni, poiché la parte restante della comunicazione è criptata con chiavi diverse. È possibile gestire la frequenza di generazione delle chiavi o utilizzare un valore predefinito. Lo scambio delle chiavi in IPsec avviene tramite l'algoritmo Diffie-Hellman (DH), uno dei più sicuri: le due parti si scambiano pubblicamente le informazioni per la generazione delle chiavi, protette ulteriormente dalla firma di una funzione hash. Dopo aver ricevuto questi dati, mittente e destinatario possono generare la stessa chiave condivisa.
- **ISAKMP** (***I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol*). Questo protocollo fornisce le regole e i meccanismi per lo scambio delle chiavi crittografiche, ma non specifica quale protocollo di sicurezza utilizzare per la protezione dei dati, come IPsec. ISAKMP è usato in combinazione con IKE per per stabilire, negoziare, modificare e cancellare le Security Associations.

notabene

Il protocollo TLS è il successore di SSL (Secure Sockets Layer). SSL è molto più conosciuto rispetto a TLS, e spesso si fa riferimento a "certificato SSL" o "protocollo SSL/TLS", pur riferendosi alla versione attuale di TLS, cioè la 1.3, definita nella RFC 8446. TLS 1.3 migliora la precedente versione 1.2 (ancora utilizzata) rendendola più efficiente e sicura: TLS 1.3 ha rimosso alcuni algoritmi vulnerabili, in favore di nuove soluzioni più sicure.

6 Transport Layer Security (TLS)

TLS si colloca tra il livello Trasporto e il livello Applicazione del modello TCP/IP. L'obiettivo principale di TLS è garantire sicurezza – in termini di autenticazione, integrità dei dati e confidenzialità – ai protocolli che operano a livello Applicazione (Tabella 6).
Un esempio ben noto è il protocollo HTTPS, utilizzato per stabilire una connessione privata e sicura tra un browser e il server di un sito web. Tuttavia, TLS può essere utilizzato anche per le VPN. Ad esempio, l'accoppiata di MPLS e TLS può garantire che una VPN sia efficiente nell'instradamento dei pacchetti e nel trasferimento sicuro dei dati.

Protocollo Applicativo	Protocollo Sicuro = Protocollo + TLS	Porta	Protocollo di Trasporto	Descrizione
HTTP	HTTPS	443	TCP	accesso a siti web
FTP	FTPS	990	TCP	trasferimento di file
SMTP	SMTPS	465	TCP	invio di e-mail
POP3	POP3S	995	TCP	lettura di e-mail
IMAP	IMAPS	993	TCP	lettura di e-mail
DNS	DoT (DNS over TLS)	853	UDP, TCP	risoluzione dei nomi di dominio

↑ **Tab. 6** Protocolli di livello Applicazione che "diventano" sicuri ("S" sta per "Secure") con lo strato TLS.

In particolare, TLS raggiunge i suoi obiettivi attraverso:

- **Autenticazione**. Avviene tramite crittografia asimmetrica, ad esempio RSA, e lo scambio di certificati. È importante notare che il lato server del canale è sempre autenticato, mentre il client è autenticato solo opzionalmente.
- **Riservatezza**. I dati inviati sul canale dopo la sua creazione sono protetti da algoritmi di crittografia a chiave simmetrica, come AES.
- **Integrità**. I dati non possono essere modificati, grazie all'uso di funzioni di hash, come SHA-256, che impediscono qualsiasi cambiamento.

L'architettura di TLS

TLS ha due componenti principali (Figura 13):

- **Handshake Protocol**. Questo è il livello più alto, che si interfaccia con il livello Applicazione. L'handshake è utilizzato da client e server quando comunicano tra loro per la prima volta. Permette al client e al server di negoziare una versione del protocollo, selezionare algoritmi crittografici, passarsi le chiavi di crittografia e autenticarsi.
- **Record Protocol**. Questo è il livello più basso, che si appoggia sul livello Trasporto. il Record Protocol utilizza i parametri di sicurezza stabiliti nella fase di handshake per garantire l'integrità e la confidenzialità dei dati trasmessi.

Handshake Protocol

Durante la fase di handshake di TLS, vengono scambiati vari messaggi che contengono i campi necessari per l'instaurazione del protocollo. La Figura 14 illustra le tre fasi dell'handshake TLS: negoziazione dei parametri; scambio delle chiavi e autenticazione; generazione della chiave di sessione per la crittografia simmetrica.

1 Negoziazione

Il client invia un messaggio "**ClientHello**" al server, che include:

- la versione più alta di TLS che supporta (Protocol Version);
- un numero di sessione (Session Identifier). Se il numero di sessione è zero, si tratta di una nuova sessione, altrimenti si tratta di una precedente sessione che potrebbe essere riesumata;
- la lista degli algoritmi di crittografia supportati dal client (CipherSuite), tra cui il server effettuerà una scelta.

2 Scambio delle chiavi e autenticazione

Il server riceve il messaggio "ClientHello", elabora il suo contenuto e determina l'insieme appropriato di parametri crittografici.
Quindi risponde con un messaggio "**ServerHello**", che include:

- la versione di TLS scelta;
- un numero di sessione;
- l'algoritmo di cifratura scelto dal server tra quelli proposti dal client;
- un certificato che include la chiave pubblica del server;
- (facoltativamente, il server potrebbe richiedere al client di dichiarare il suo certificato).

Si osservi che questa parte dell'handshake riguarda lo scambio di certificati digitali. In particolare, il certificato digitale del server viene inviato al client. Il client considera il server attendibile se il certificato è stato firmato da una Certificate

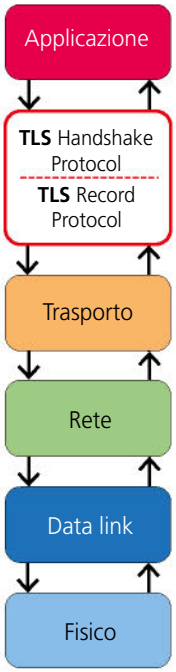


Fig. 13

notabene

Un Generatore di Numeri Pseudo-Casuali Crittograficamente Sicuro è un generatore di numeri pseudo-casuali adatto per la crittografia. Il termine "nonce" indica un numero pseudo-casuale utilizzato una volta sola, "per quella occasione", "for the nonce".

Authority (CA) di fiducia. In alcuni casi, il server potrebbe anche richiedere un certificato al client per autenticarlo.

3 Convalida e Generazione della chiave di sessione

Il client:

- convalida il certificato del server;
- genera una **chiave di sessione**. La chiave di sessione (nota anche come "nonce") è generata casualmente utilizzando un "Generatore di Numeri Pseudo-Casuali Crittograficamente Sicuro";
- crittografa la chiave di sessione con la chiave pubblica del server e la invia al server;
- (facoltativamente, invia al server il proprio certificato, se richiesto.)

Il server:

- decodifica la chiave di sessione con la sua chiave privata;
- eventualmente, valida il certificato del client.

Fine dell'handshake e inizio dello scambio dei dati applicativi

Una volta stabilita la chiave di sessione l'handshake ha termine e inizia la trasmissione protetta dei dati di applicazione che vengono crittografati e decrittografati utilizzando **la stessa chiave di sessione condivisa**.

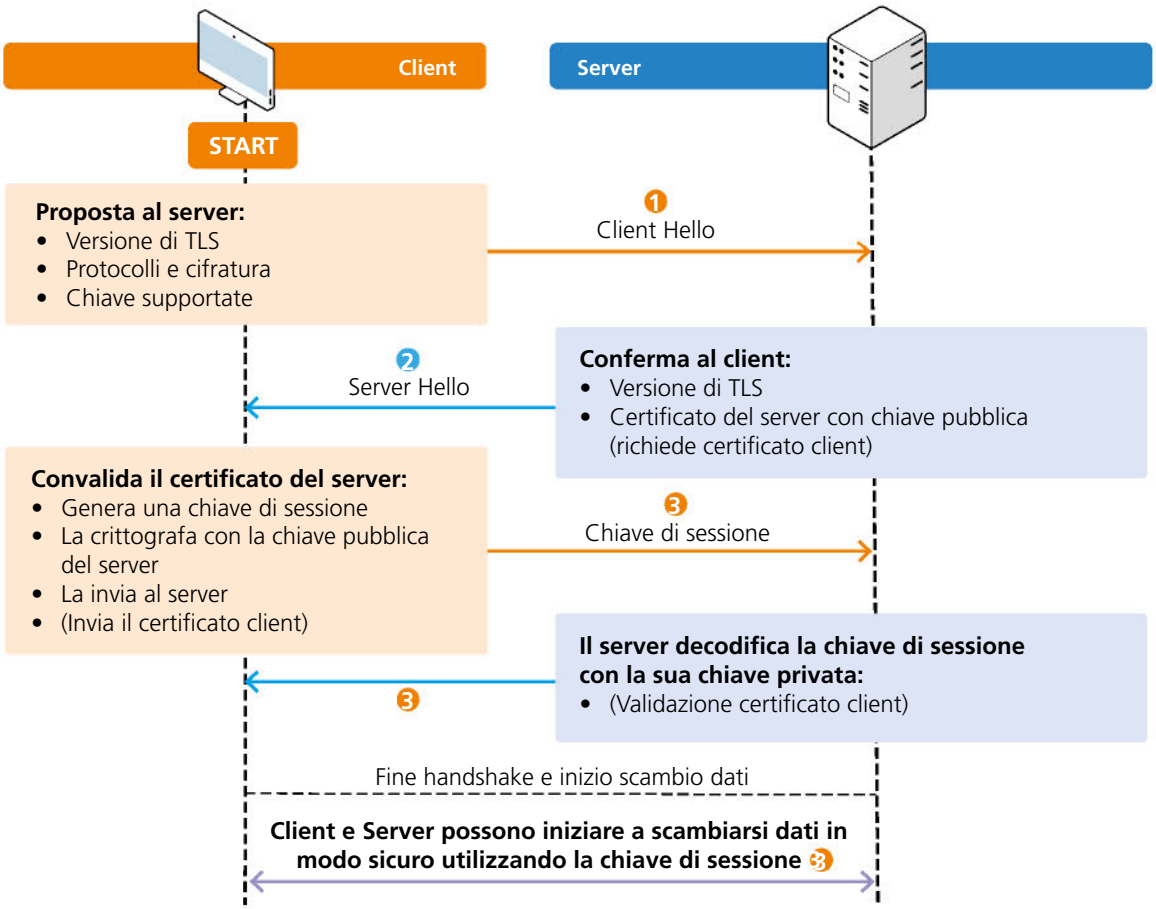


Fig. 14 Handshake TLS 1.3. La combinazione di "ClientHello" e "ServerHello" determina la chiave condivisa da utilizzare per crittare i dati.

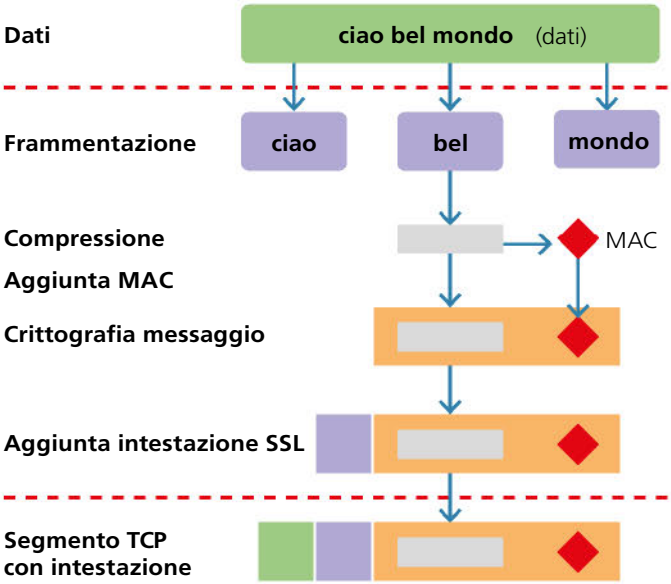


Fig. 15 Il processo seguito da Record Protocol per la formattazione dei record.

Record Protocol

I dati in arrivo dal livello Applicazione, vengono **formattati in record e crittografati prima di essere passati al livello trasporto**. I record in TLS 1.3 sono progettati per garantire sia la riservatezza che l'integrità dei dati trasmessi. Il processo che Record Protocol segue per la creazione di un record è il seguente (Figura 15):

- **Frammentazione**. I dati che provengono dalle applicazioni sono frammentati in blocchi di lunghezza massima non superiore a 214 byte.
- **Applicazione di AEAD** (**A***uthenticated* **E***ncryption with* **A***ssociated* **D***ata*). AEAD garantisce la riservatezza dei dati (grazie alla chiave segreta) e la integrità di informazioni aggiuntive ("dati associati") non riservate, ma la cui integrità è protetta: è impossibile modificare i dati in chiaro sottostanti al testo cifrato senza essere scoperti.
- **Formazione del record**. I dati crittografati vengono inseriti in un record che comprende i campi mostrati in Figura 16, che viene poi inoltrato al livello di trasporto per essere inserito in un segmento TCP.

Il ricevente applica il processo inverso ai blocchi ricevuti: li decifra, verifica la loro integrità, li riassembla e li passa al livello applicazione.

notabene

TLS 1.3 supporta diverse modalità di scambio delle chiavi, tra cui (EC) DHE (Diffie-Hellman), PSK solo, e PSK con (EC)DHE.

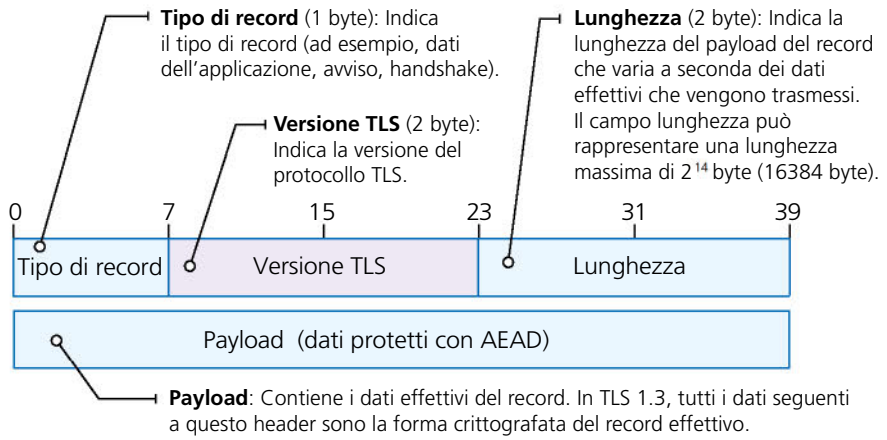


Fig. 16 La struttura del Record Protocol.

Pit Stop

15 Che cos'è TLS?

16 A quale livello TCP/IP si colloca TLS?

17 Come funziona TLS?

7 HTTPS – HyperText Transfer Protocol Secure

Pit Stop

18 Che cos'è HTTPS?

19 A quale livello TCP/IP si colloca HTTPS?

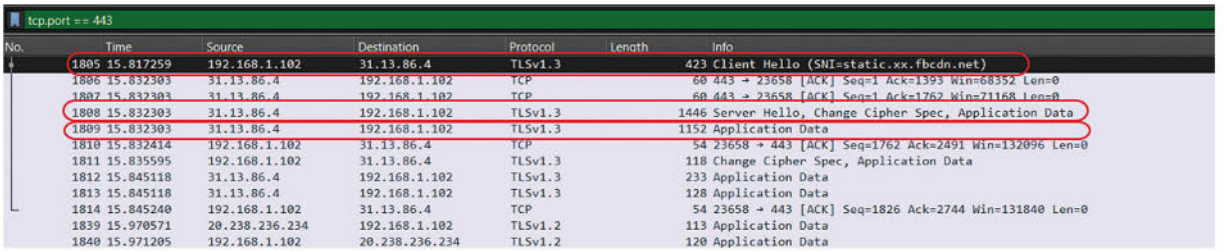
20 Che relazione c'è tra TLS e HTTPS?

Il processo di funzionamento di HTTPS, per l'importanza che riveste, merita un ulteriore approfondimento. La sessione di HTTPS si sviluppa in tre fasi:

- Apertura della connessione:
  - Il browser si connette alla porta 443 del server;
  - TLS intraprende la fase di handshake con lo scambio del certificato;
  - Il browser avvia la richiesta HTTP, i cui dati sono inseriti in un record TLS.
- Mantenimento della connessione:
  - Il trasferimento di dati è regolato dal protocollo HTTP;
  - I dati vengono crittografati e decrittografati utilizzando la chiave di sessione.
- Chiusura della connessione:
  - TLS procede alla chiusura della connessione.

La **Figura 17** mostra un collegamento HTTPS che sfrutta TLS 1.3 con handshake e scambio dei dati.

Fig. 17 Handshake TLS 13.3 con scambio delle chiavi. È mostrato tutto il traffico inviato e ricevuto sulla porta 443.



8 Conclusione

Confronto tra protocollo IPsec e protocollo TLS

IPsec e TLS sono due protocolli di sicurezza che possono sembrare simili, ma hanno obiettivi diversi e sono utilizzati in contesti diversi, come la **Tabella 7** evidenzia. Se TLS nasconde i dati come un portafoglio nasconde il suo contenuto, IPSec nasconde, oltre al portfolio, anche l'identità della persona stessa!

Tab. 7 Confronto tra i protocolli IPsec e TLS.

	IPsec	TLS
Livello nel modello TCP/IP	Livello Rete	Livello Trasporto
Utilizzo	Protegge e autentica l'intero pacchetto IP durante il tragitto. Fornisce sicurezza a livello rete, proteggendo tutti i dati dei livelli superiori. È tipicamente utilizzato per le VPN Site-to-Site.	Protegge i dati applicativi trasmessi tra due sistemi, come un browser web e un server, garantendo che i dati non possano essere letti o modificati durante il tragitto. È utilizzato nelle VPN SSL e nei protocolli HTTPS, SMTPS, FTPS, ecc.
Trasporto	Opera su un protocollo di rete non affidabile (IP).	Opera su un protocollo di trasporto affidabile (TCP).
Scambio di chiavi	Si basa su un protocollo esterno (IKE – Internet Key Exchange).	Contiene al suo interno gli algoritmi per la negoziazione di algoritmi di scambio di chiavi (algoritmo Diffie-Hellman).

Confronto tra dispositivi di sicurezza

Le VPN, i server proxy e i firewall hanno alcune somiglianze, come il fatto che tutti possono nascondere l'indirizzo IP dell'utente, offuscando così l'identità del navigatore. Inoltre, tutti e tre possono filtrare il traffico. Tuttavia, ci sono differenze significative tra queste tre soluzioni, soprattutto in termini di sicurezza e funzionalità. La Tabella 8 mette a confronto un server proxy, una VPN e un firewall.

Caratteristica	Server Proxy	VPN	Firewall
Funzione principale	Fa da intermediario tra il computer e i siti web che l'utente vuole raggiungere	Protegge la privacy e la sicurezza tra le reti pubbliche e private	Protegge la rete bloccando o consentendo il traffico in base alle regole di sicurezza impostate
Crittografia	Non cripta i dati	Cripta i dati	Può farlo, ma non è la sua funzione principale
Posizione in rete	• Ospitati su rete interna • Ospitati in Internet (server proxy pubblici)	• VPN private: i punti terminali sono ospitati in sedi remote e centrale • VPN pubbliche ospitate da provider	Posizionato, solitamente, tra la rete interna e Internet
Gestione del traffico	Opera a livello applicazione, ad esempio richieste web	Considera tutto il traffico	Considera tutto il traffico
Anonimato	Maschera l'indirizzo IP del client	Maschera l'indirizzo IP del client e offusca i dati	Non fornisce anonimato
Cache memory	Può fornire funzionalità di caching per migliorare le prestazioni	Non fornisce funzionalità di caching	Non fornisce funzionalità di caching
Filtraggio del contenuto	Può filtrare il traffico in base al contenuto, come URL, tipo di applicazione, ecc.	Può filtrare il traffico in base all'indirizzo IP, alla porta o al protocollo	Può filtrare il traffico in base all'indirizzo IP, alla porta, al protocollo, e al contenuto
Installazione	Computer, server dedicati, browser web, bastion host e alcuni router e firewall	Computer, firewall, router e altri dispositivi come i NAS (Network Attached Storage)	Dispositivo hardware dedicato, un software installato su un computer, o una funzionalità integrata in un router o in un altro dispositivo di rete

Tab. 8 Comparazione tra funzionalità di server proxy, VPN e firewall.

notabene

L'uso di TLS, insieme ad altre forme di "crittografia a strati", è fondamentale per il funzionamento della rete **Tor** ("The Onion Router") e del software che la supporta. Tor consente una navigazione anonima sul Web attraverso un browser specifico, l'**Onion Browser**. I dati trasmessi attraverso la rete Tor sono protetti da strati sovrapposti di crittografia, simili agli strati di una cipolla. Ogni nodo nel percorso elimina uno strato per individuare il nodo successivo a cui trasferire i dati. Una volta raggiunto il nodo di uscita, viene rimosso anche l'ultimo strato crittografico, rivelando i dati originali.

Approfondimento - Tecnologia 1

L'intestazione IPsec

IPsec Tunnel Mode, utilizzato insieme a Authentication Header (AH), fornisce l'integrità e l'autenticazione di tutto il messaggio. Associato a Encapsulating Security Payload (ESP) garantisce autenticità, integrità e riservatezza del solo payload. Il funzionamento di questa modalità prevede la rimozione dell'intestazione del pacchetto IP originale e l'introduzione dell'intestazione "IPsec Header" che si traduce in "AH header" (Figura 1) oppure "ESP header" (Figura 2). Nel caso si utilizzi ESP, i dati vengono anche criptati, altrimenti si procede alla sola autenticazione del pacchetto. Infine viene riapplicato al pacchetto l'header IP originale. Tunnel mode è usato per i collegamenti VPN tra reti private che accedono a router pubblici (gateway-to-gateway). Il tunnel che si crea serve al transito sicuro dei pacchetti IP privati. I pacchetti vengono completamente cifrati e incapsulati

L'intestazione AH contiene i seguenti campi:

- **Next Header**: con il numero di protocollo (il numero 6 indica che il protocollo contenuto nella busta è TCP; il numero 51 nell'header di IPv4 indica che la prossima intestazione è quella di AH);
- **Payload Length**: contiene la lunghezza dell'header di AH (il campo Reserved non è usato);
- **SPI – Security Parameter Index**: numero che, con l'indirizzo IP di destinazione e il protocollo di sicurezza, identifica la security association (SA) da utilizzare per questo pacchetto;
- **Sequence Number**: contiene un numero sequenziale che, partendo da 0, è incrementato per ogni pacchetto appartenente a quella SA (questo numero identifica in modo univoco ogni datagramma inviato, per impedire che lo stesso pacchetto possa essere rispedito se venisse catturato in un attacco di reply [replica] o di man in the middle, in cui un attaccante si interpone tra le due entità che sono in comunicazione e si impossessa del pacchetto per inoltrarlo successivamente);

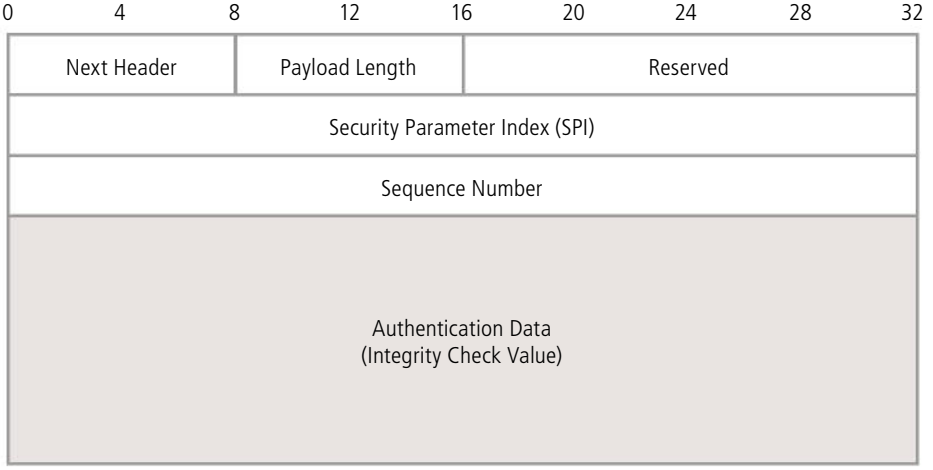


Fig. 1 L'intestazione AH.

- **Authentication Data**: contiene l'Integrity Check Value (ICV), un numero generato tramite un algoritmo di hashing, che costituisce la firma digitale realizzata con l'algoritmo specificato e concordato nella SA. La sintesi è calcolata sul pacchetto originale e assicura l'integrità e l'identità del mittente.

L'intestazione ESP contiene i seguenti campi.

- **SPI – Security Parameter Index**: come in AH, questo campo identifica la SA da usare per questo pacchetto.
- **Sequence Number**: come in AH, contiene un numero sequenziale che, partendoda 0, si incrementa per ogni pacchetto appartenente a quella SA.
- **ESP Payload data**: contiene i dati crittografati, tipicamente presenti nel pacchetto IP che è stato incapsulato e ha lunghezza variabile.
- **Padding**: riempie il campo di payload per farlo diventare multiplo di 32 bit.
- **Pad Length**: fornisce il numero di ottetti aggiunti in padding.
- **Next Header**: contiene il numero di protocollo del successivo header.
- **Authentication Data**: contiene l'Integrity Check Value (ICV) calcolato applicando l'algoritmo di autenticazione (opzionale).

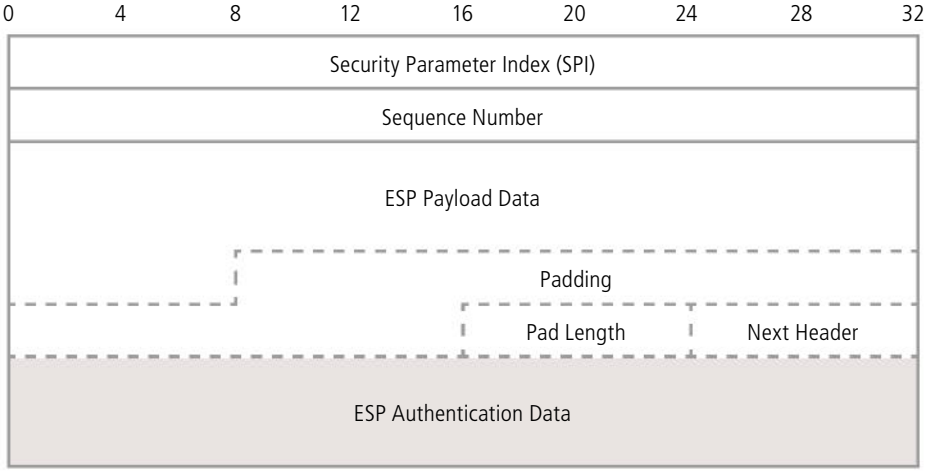


Fig. 2 L'intestazione ESP.

Approfondimento - Tecnologia 2

PGP: posta elettronica sicura

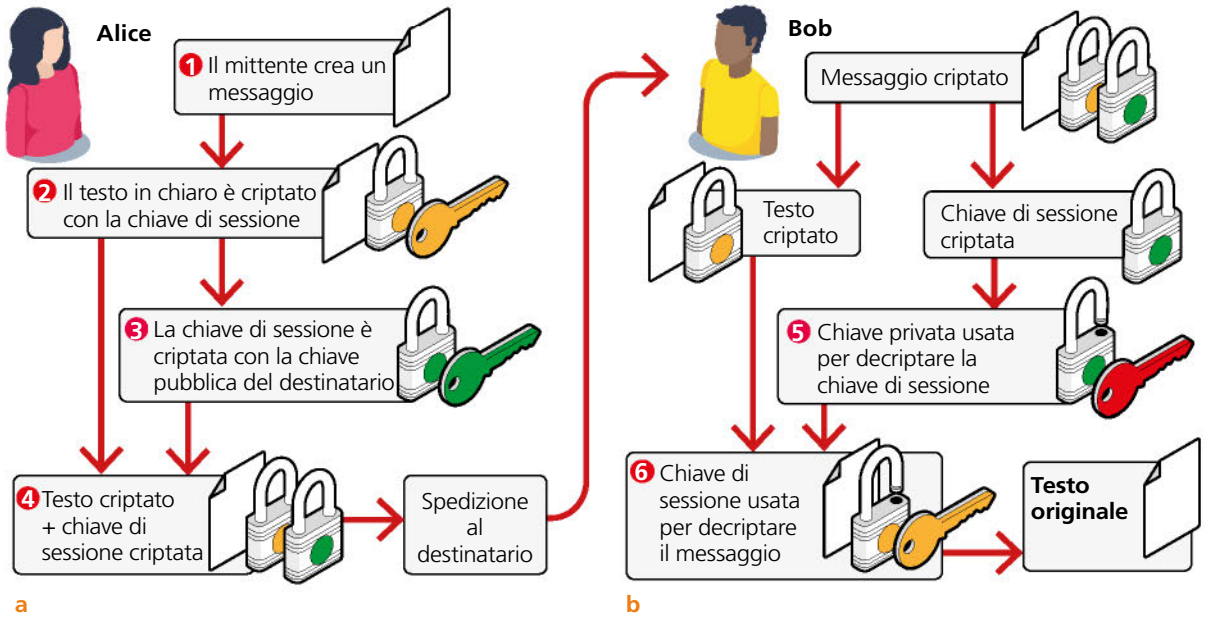
Gli algoritmi di crittografia possono essere applicati al servizio di posta elettronica per garantire:

- **riservatezza del messaggio** (se Alice invia una e-mail a Bob e non vuole che Trudy capisca il testo);

- **autenticazione del mittente** (se Alice scrive una e-mail a Bob, Bob vuole essere certo che la e-mail sia stata scritta da Alice);
- **autenticazione del ricevente** (se Alice scrive una e-mail a Bob, vuole essere certa che sia ricevuta proprio da Bob);
- **integrità del messaggio** (se Alice invia una e-mail a Bob, il messaggio che Bob riceve deve essere uguale a quello che Alice ha inviato; non deve essere modificato durante il percorso da Alice a Bob).

PGP (*Pretty Good Privacy*) è la modalità, ideata da Philip Zimmermann all'inizio degli anni Novanta del secolo scorso e descritta in RFC 4880, che si è affermata come standard di fatto per fornire questi servizi.
PGP usa la crittografia a chiave simmetrica, con la coppia di chiavi pubblica e privata, e una chiave segreta usata per cifrare il testo in chiaro. Le chiavi pubbliche degli utenti PGP possono essere messe a disposizione di chiunque.
PGP offre la possibilità di criptare il messaggio, di firmarlo o di fare entrambe le operazioni. Lo schema usato è simile a quelli visti finora.
Supponiamo che Alice voglia inviare un messaggio di posta elettronica a Bob in modo che la malevola Trudy non sia in grado di capire e modificare il messaggio e vediamo come Bob può essere certo che il messaggio sia stato inviato da Alice, e Alice può essere sicura che Bob l'abbia ricevuto.
Per quanto riguarda la **riservatezza** facciamo riferimento alle Figura 1a e 1b.
Il software PGP di Alice genera un numero casuale da utilizzare come chiave simmetrica di sessione.

Per ogni messaggio viene generata una nuova chiave di sessione (**1**).
Con questa chiave di sessione viene crittografato il messaggio (**2**) (Tabella 1).
La chiave di sessione viene crittata con la chiave pubblica di Bob (**3**).
Il testo cifrato e la chiave crittata vengono concatenati e inviati a Bob (**4**).



↑ **Fig. 1 a.** L'invio di un messaggio segreto prevede l'uso della chiave di sessione e della chiave pubblica del destinatario.
b. La ricezione di un messaggio segreto prevede l'uso della chiave privata per estrarre quella di sessione.

Bob, ricevuto l'intero messaggio crittografato, usa la sua chiave privata per decifrare la chiave di sessione (**5**) e la chiave di sessione per decifrare il messaggio (**6**). Per l'**autenticazione** e l'**integrità** vengono usati, rispettivamente, la firma digitale e il "riassunto" (digest) del messaggio:

- il software PGP di Alice applica una funzione di hash al messaggio per ottenere il digest;
- il digest viene criptato con la chiave privata di Alice per ottenere la firma digitale;
- il messaggio in chiaro e la firma digitale vengono concatenati e costituiscono i dati da inviare a Bob;
- Bob riceve il messaggio e decifra la firma con la chiave pubblica di Alice;
- Bob applica la funzione di hash al messaggio in chiaro;
- Bob confronta il "riassunto" ricevuto con quello ottenuto e, se coincidono, è sicuro che il messaggio, integro, provenga da Alice.

Funzione	Algoritmi	Descrizione
Cifratura del messaggio	RSA, 3DES	Il messaggio viene cifrato usando la chiave di sessione simmetrica.
Scambio della chiave di sessione	RSA	La chiave di sessione è cifrata con la chiave pubblica del destinatario.
Calcolo del digest (hash)	MD5, SHA	Il calcolo del message digest è attuato dalle funzioni di hash.
Firma digitale	RSA	Il digest del messaggio viene criptato con la chiave privata del mittente.
Compressione	ZIP	Il messaggio viene compresso per la memorizzazione e la trasmissione.
Gestione chiavi	Diffie-Hellman/DSS	

Tab. 1 Alcuni degli algoritmi utilizzati da PGP.

La parola a... Philip Zimmermann



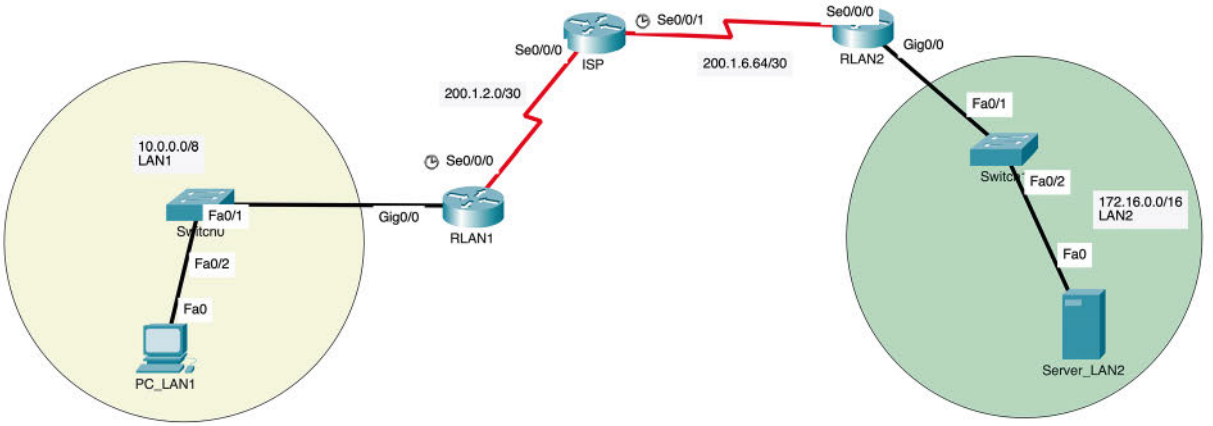
Philip Zimmermann, nato nel 1954 negli Stati Uniti, è il creatore di PGP, il software di crittografia per la posta elettronica più usato al mondo e distribuito come software libero dal 1991. PGP è stato creato con l'idea di rendere disponibile un sistema che permettesse agli attivisti per i diritti umani di esprimersi liberamente, protetti dall'anonimato. Lasciamogli la parola. «*Sono il creatore di PGP, un pacchetto software di crittografia a chiave pubblica per la protezione della posta elettronica. Da quando PGP è stato pubblicato a livello nazionale come freeware nel giugno del 1991, si è diffuso organicamente in tutto il mondo e da allora è diventato di fatto lo standard mondiale per la crittografia della posta elettronica. Ma questa rinascita della comunicazione digitale elettronica porta con sé una preoccupante erosione della nostra privacy. In passato, se il governo voleva violare la privacy dei comuni cittadini, doveva compiere un certo sforzo per intercettarne le comunicazioni. Ciò è analogo a catturare i pesci con un amo e una lenza, un pesce alla volta.A differenza della posta cartacea, i messaggi di posta elettronica sono semplicemente troppo facili da intercettare e scansionare. Ciò può essere fatto facilmente, regolarmente, automaticamente e in modo non rilevabile su larga scala. Questo è analogo alla pesca con reti a strascico e ciò fa una differenza quantitativa e qualitativa per la salute della democrazia.*»

Laboratorio

ATTIVITÀ 1
VPN Site-to-Site sicura

Scenario

Consideriamo un'azienda con due sedi remote.
Le due sedi sono dotate di LAN (LAN1 per la sede 1 e LAN2 per la sede 2), ciascuna collegata tramite un router al router di un fornitore di servizi (ISP).
La rete è rappresentata dalla seguente immagine:



Gli indirizzi utilizzati sono i seguenti:

Dispositivo	Interfaccia	Indirizzo IP	Subnet Mask	Default Gateway
RLAN1	G0/0	10.255.255.254	255.0.0.0	--
	S0/0/0	200.1.2.1	255.255.255.252	--
RLAN2	G0/0	172.16.255.254	255.255.0.0	--
	S0/0/0	200.1.6.65	255.255.255.252	
RISP	S0/0/0	200.1.2.2	255.255.255.252	--
	S0/0/1	200.1.6.66	255.255.255.252	--
PC_LAN1	Fa0	10.0.0.1	255.0.0.0	10.255.255.254
Server_LAN2	Fa0	172.16.0.2	255.255.0.0	172.16.255.254

Consegna

Utilizzando Packet Tracer, realizzare una VPN Site-to-Site tra LAN1 e LAN2 in modo che ogni dispositivo della LAN1 possa accedere al server web presente nella LAN2. La trasmissione deve avvenire in modo sicuro.

Svolgimento

Passo 1: configurare le interfacce del router dell'ISP (è stato utilizzato un router 1941)

```
hostname ISP
interface s0/0/0
ip address 200.1.2.2 255.255.255.252
no shutdown
exit

interface S0/0/1
ip address 200.1.6.66 255.255.255.252
no shutdown
exit
```

Passo 2: creare e configurare le LAN delle sedi aziendali
Nella LAN2 deve essere presente un server web.
Scegliere i dispositivi (come in figura), assegnare le configurazioni di rete e collegarli agli switch.

Configurare il router della LAN1 (è stato utilizzato un router 1941):

```
hostname RLAN1
interface Serial0/0/0
ip address 200.1.2.1 255.255.255.252
no shutdown
interface g0/0
ip address 10.255.255.254 255.0.0.0
no shutdown
exit
```

Impostare una rotta di default per instradare il traffico in uscita dal router RLAN1 verso l'interfaccia S0/0/0 del router ISP.

```
ip route 0.0.0.0 0.0.0.0 200.1.2.2
```

Configurare il router della LAN2 (è stato utilizzato un router 1941):

```
hostname RLAN2
interface Serial0/0/0
ip address 200.1.6.65 255.255.255.252
no shutdown
interface g0/0
ip address 172.16.255.254 255.255.0.0
no shutdown
exit
```

Impostare una rotta di default per instradare il traffico in uscita dal router RLAN2 verso l'interfaccia S0/0/1 del router ISP:

```
ip route 0.0.0.0 0.0.0.0 200.1.6.66
```

Collegare i router delle LAN al router ISP.

Passo 3: configuriamo ora i router delle LAN per attivare una VPN Site-to-Site tra LAN1 e LAN2 con il protocollo IPsec

Occorre creare un tunnel protetto e autenticato per consentire ai dati di viaggiare tra le due LAN in modo sicuro. Le estremità del tunnel sono rappresentate dalle interfacce outside dei due router.

- **Installazione del software *securityk9* sui router delle LAN (estremità del tunnel), salvataggio della configurazione e riavvio del router**
  Dalla modalità *config* utilizzare il comando e successivamente salvare la nuova configurazione.

```
license boot module c1900 technology-package securityk9
copy running-config startup-config
reload
```

Se l'installazione è andata a buon fine il comando `show version` fornirà il seguente risultato:

```
show version:
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            disable       None          None
data          disable       None          None
```

- **Configurazione VPN IPsec**

Impostazioni per il router RLAN1

Impostiamo una ACL per specificare qual è il traffico che può passare nel tunnel da RLAN1 a RLAN2:

```
access-list 100 permit ip 10.0.0.0 0.255.255.255 172.16.0.0
0.0.255.255
```

Utilizziamo il protocollo ISAKMP per lo scambio delle chiavi e per implementare le security association (SA).

```
crypto isakmp policy 10
    encryption aes 256
    authentication pre-share
    group 5

crypto isakmp key CHIAVESEGRETA address 200.1.6.65
```

Impostiamo le regole di negoziazione che devono essere utilizzate nel tunnel. Utilizzeremo la crittografia AES a 256 bit con codice di autenticazione del messaggio hash che fornisce riservatezza, integrità e autenticazione:

```
crypto ipsec transform-set RLAN1-RLAN2 esp-aes 256 esp-
sha-hmac
```

Definiamo la crypto map che raccoglie le regole definite:

```
crypto map IPSEC-CRYPTOMAP 100 ipsec-isakmp
 set peer 200.1.6.65
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set RLAN1-RLAN2
 match address 100
```

Applichiamo la crypto map all'interfaccia in uscita della LAN1:

```
interface Serial0/0/0
crypto map IPSEC-CRYPTOMAP
```

Analogamente, prestando attenzione agli indirizzi delle interfacce, procediamo per il router RLAN2.

Impostazioni per il router RLAN2

```
access-list 100 permit ip 172.16.0.0 0.0.255.255 10.0.0.0
0.255.255.255

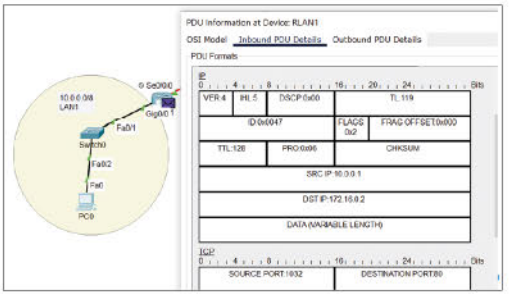
crypto isakmp policy 10
    encryption aes 256
    authentication pre-share
    group 5
!
crypto isakmp key CHIAVESEGRETA address 200.1.2.1

crypto ipsec transform-set RLAN2-RLAN1 esp-aes 256 esp-
sha-hmac

crypto map IPSEC-CRYPTOMAP 100 ipsec-isakmp
 set peer 200.1.2.1
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set RLAN2-RLAN1
 match address 100
interface Serial0/0/0
 crypto map IPSEC-CRYPTOMAP
```

Passo 4: verifica del funzionamento

Per verificare il funzionamento facciamo una richiesta HTTP dal PC_LAN1 al server_LAN2. Utilizziamo la modalità *simulation* di Packet Tracer per osservare i PDU nei passi più significativi.

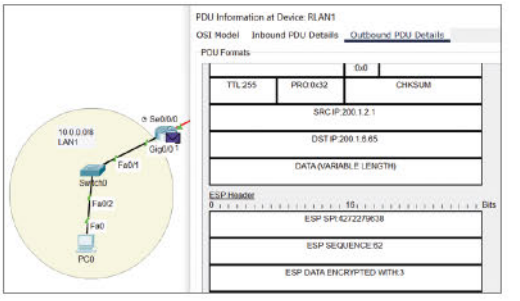


PDU in ingresso su RLAN1 dall'interno

Osserviamo che IP mittente e destinatario sono gli indirizzi privati dei dispositivi sulle due LAN

IP mittente: `10.0.0.1`

IP destinatario: `172.16.0.2`



PDU in uscita da RLAN1 verso l'esterno

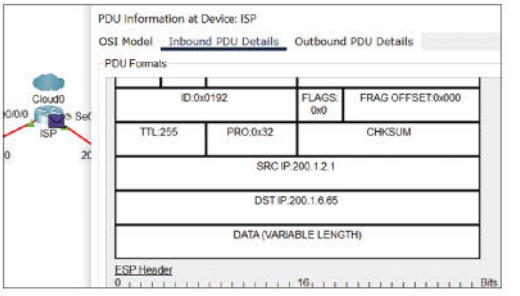
Osserviamo che IP mittente e destinatario sono gli indirizzi pubblici delle LAN e che IPsec è stato attivato.

IP mittente: `200.1.2.1`

IP destinatario: `200.1.6.65`

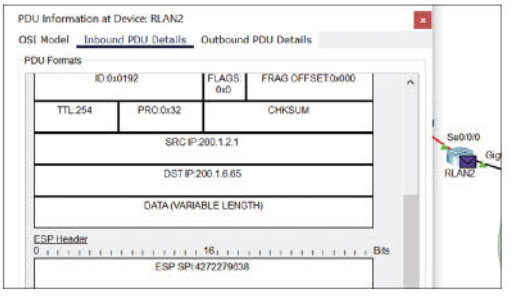
IPsec cripta e incapsula i dati.

Da qui i dati iniziano il loro viaggio nel tunnel in sicurezza.



PDU su ISP

Il PDU transita dal router ISP mantenendo i dati criptati e come indirizzi IP gli indirizzi pubblici delle reti.



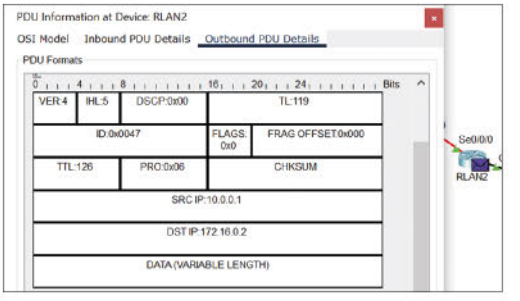
PDU in ingresso su RLAN2 dall'esterno

Osserviamo che IP mittente e destinatario sono gli indirizzi pubblici delle LAN.

IP mittente: `200.1.2.1`

IP destinatario: `200.1.6.65`

Qui termina il tunnel.



PDU in uscita da RLAN2 verso l'interno

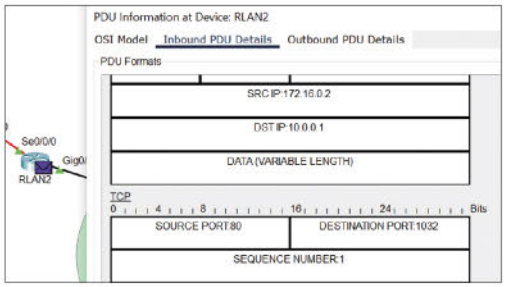
IPSec deincapsula e decripta i dati che in questo modo "fuoriescono dal tunnel" e proseguono il tragitto verso il server web.

Osserviamo che IP mittente e destinatario sono gli indirizzi privati dei dispositivi sulle due LAN.

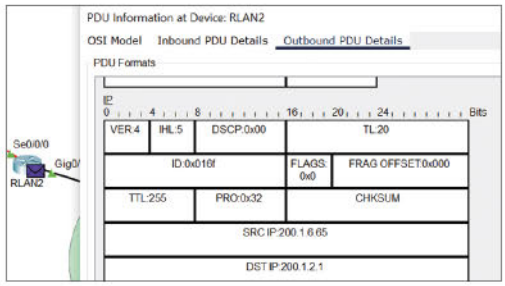
IP mittente: `10.0.0.1`

IP destinatario: `172.16.0.2`

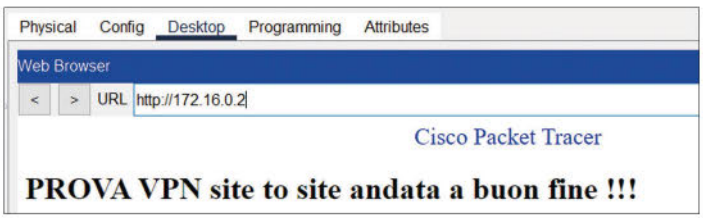
PDU in ingresso su RLAN2 dall'interno
Osserviamo che IP mittente e destinatario sono gli indirizzi privati dei dispositivi sulle due LAN.
IP mittente: `172.16.0.2`
IP destinatario: `10.0.0.1`



PDU in uscita da RLAN2 verso l'esterno
Osserviamo che IP mittente e destinatario sono gli indirizzi pubblici delle LAN e che IPsec è stato attivato.
IP mittente: `200.1.6.65`
IP destinatario: `200.1.2.1`
IPsec cripta e incapsula i dati.
Da qui i dati iniziano il loro viaggio di ritorno nel tunnel in sicurezza.



Infine, osserviamo il buon funzionamento visualizzando la pagina web `index.html` restituita dal protocollo HTTP.



È possibile constatare il funzionamento anche utilizzando il comando `show crypto ipsec sa` (in questo caso a titolo esemplificativo, su RLAN1):

```
RLAN1#show crypto ipsec sa

interface: Serial0/0/0
Crypto map tag: IPSEC-CRYPTOMAP, local addr 200.1.2.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
current_peer 200.1.6.65 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 73, #pkts encrypt: 73, #pkts digest: 0
#pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

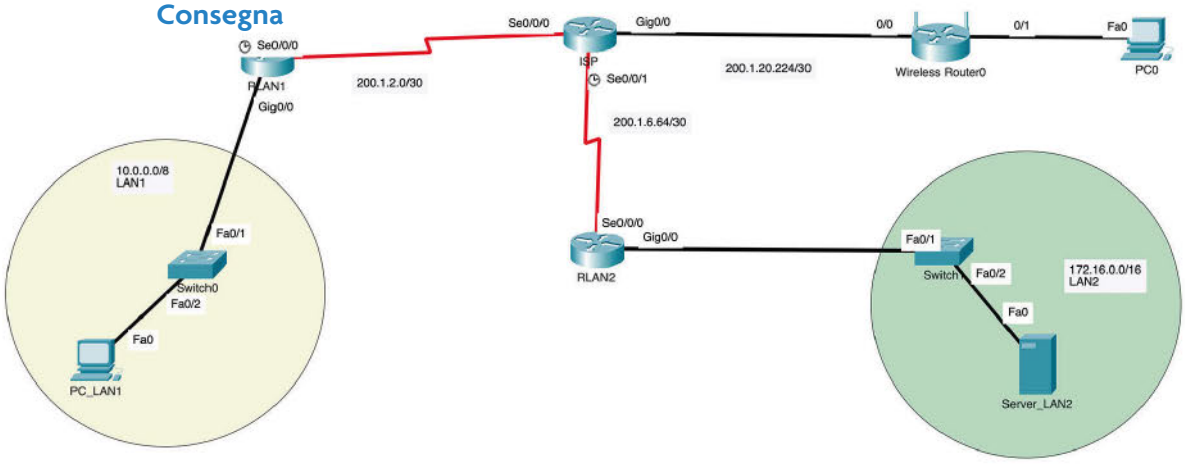
local crypto endpt.: 200.1.2.1, remote crypto endpt.:200.1.6.65
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0xFEA5D056(4272279638)
```

ATTIVITÀ 2
VPN Remote Access

Scenario

Si consideri la rete dell'attività precedente. L'azienda ha stabilito che i lavoratori possono fruire della modalità di lavoro agile da remoto.
I lavoratori devono poter accedere alle risorse aziendali da remoto, in particolare al server web sulla LAN2. Si devono predisporre le misure di sicurezza per tutelare le risorse aziendali.

Consegna



Utilizzando Packet Tracer, realizzare una VPN Remote Access tra la postazione del lavoratore remoto e la LAN1. La trasmissione deve avvenire in modo sicuro.

Passo 1: estensione rete con rete domestica
Aggiungere alla rete dell'attività precedente un router domestico (router del lavoratore) e collegare al router un PC.
Collegare il router domestico al router dell'ISP, configurando l'interfaccia con i seguenti parametri:
IP: `200.1.20.226`
Subnet Mask: `255.255.255.252`

Passo 2: configurare la VPN Remote Access sul router della LAN1
Partiamo dal presupposto che la rete è già stata configurata per funzionare in modalità Site-to-Site (attività precedente). In questa attività aggiungiamo solo quello che serve per l'accesso da remoto, mentre diamo per già definita la policy per la creazione delle SA.
Su router RLAN1 definiamo il pool di indirizzi che possono essere usati da remoto:

```
ip local pool POOL-VPN 10.0.0.100 10.0.0.150
```

Definiamo i parametri (evidenziati in giallo) per la configurazione dei client:

```
crypto isakmp client configuration group lan1
key keyaccess
pool POOL-VPN
exit
```

Definiamo le mappe dinamiche per gli accessi da remoto:

```
crypto dynamic-map MAPPA-DINAMICA 100
set transform-set RLAN1-RLAN2
reverse-route
exit
```

Definiamo ora i parametri per l'autenticazione degli utenti. In particolare, creiamo la lista `accessoremoto` e l'account user: `utente1`, password: `utente1`

```
aaa new-model
aaa authentication login accessoremoto local
aaa authorization network lan1 local
username utente1 password utente1
```

Definizione della mappa statica e collegamento con la mappa dinamica:

```
crypto map IPSEC-CRYPTOMAP client authentication list accessoremoto
crypto map IPSEC-CRYPTOMAP client configuration address respond
crypto map IPSEC-CRYPTOMAP isakmp authorization list lan1
crypto map IPSEC-CRYPTOMAP 30 ipsec-isakmp dynamic MAPPA-DINAMICA
```

Applichiamo la mappa all'interfaccia del router RLAN:

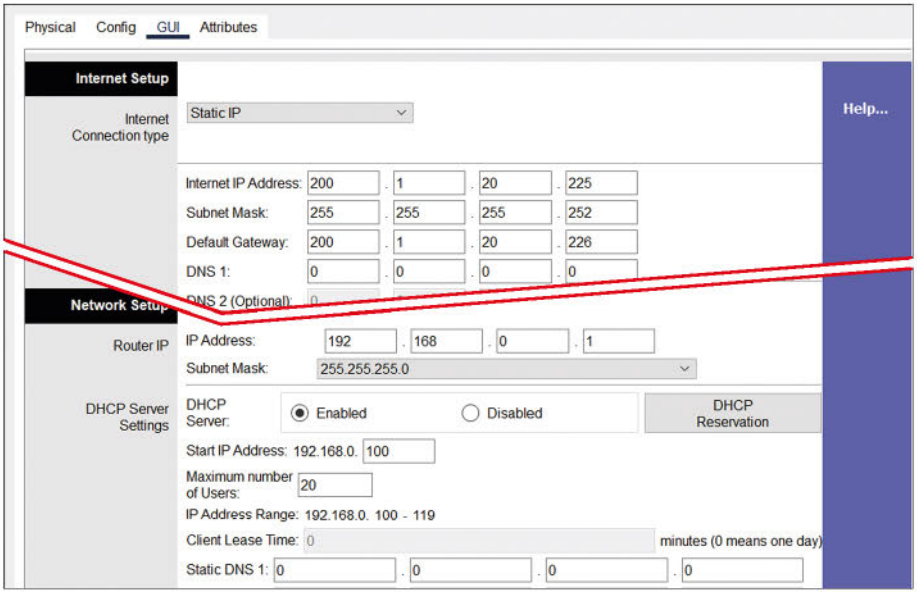
```
interface serial0/0/0
crypto map IPSEC-CRYPTOMAP
exit

copy running-config startup-config
exit
```

Passo 3: configurare il router domestico

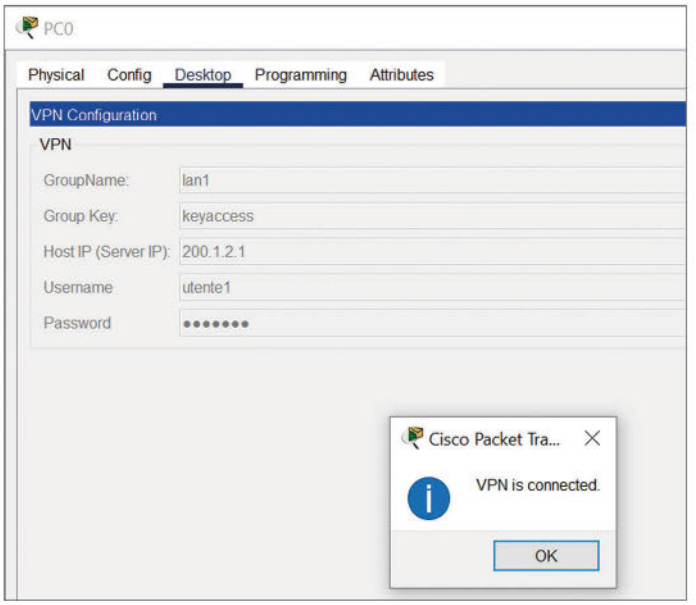
Accedere alle impostazioni del router da GUI e impostare:

- indirizzo IP verso internet `200.1.20.225 255.255.255.252`
- il default gateway: `200.1.20.226` (interfaccia del router ISP)
- Indirizzo IP verso la LAN utente: `192.168.0.1 255.255.255.0` (User default gateway)
- Abilitazione servizio DHCP con il pool di indirizzi da usare

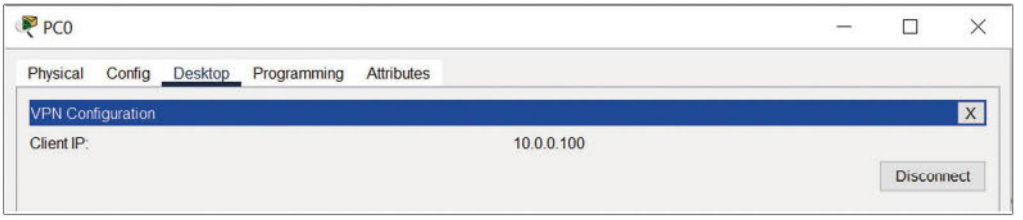


Passo 4: configurazione client VPN sul PC dell'utente remoto

Su PC0 accedere a *desktop* → *VPN* e impostare i parametri (la password è "utente1").

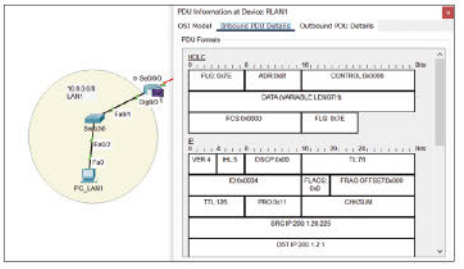


La connessione sicura è stata stabilita. Al PC remoto è stato assegnato IP `10.0.0.100` per accedere alla LAN1 in modalità protetta.



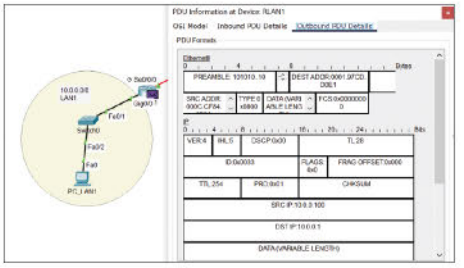
Passo 5: verifica della connessione da remoto alla LAN1

Effettuiamo un accesso da PC0 (dell'utente) a PC1 (sulla LAN1) e osserviamo i PDU in entrata e in uscita dal router RLAN1.



PDU in ingresso al router RLAN1.

PDU in uscita dal router RLAN1 verso PC1. Si può notare che l'indirizzo IP mittente è quello che è stato assegnato al PC remoto per l'accesso in modalità sicura alla LAN.



ATTIVITÀ 3
Studio del protocollo HTTP all'interno di TLS

Scenario

Si consideri la situazione di un utente che visita il sito Facebook (`https://www.facebook.com/` all'indirizzo IP `1.13.86.4`) generando traffico di rete.

Consegna

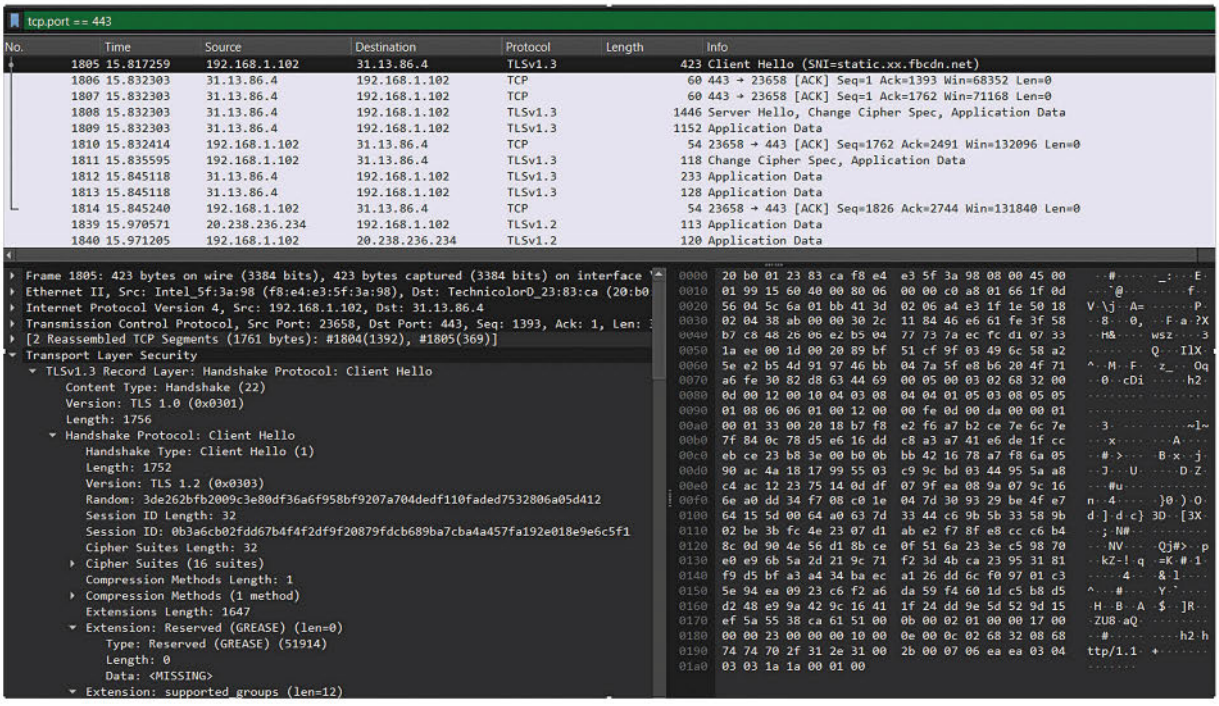
Vogliamo studiare il traffico generato dal protocollo HTTPS, visitando il sito Web che supporta TLS 1.3 in un browser web.

Svolgimento

Passo 1: filtro del traffico sulla porta 443



Passo 2: analisi dei campi di "Client Hello"



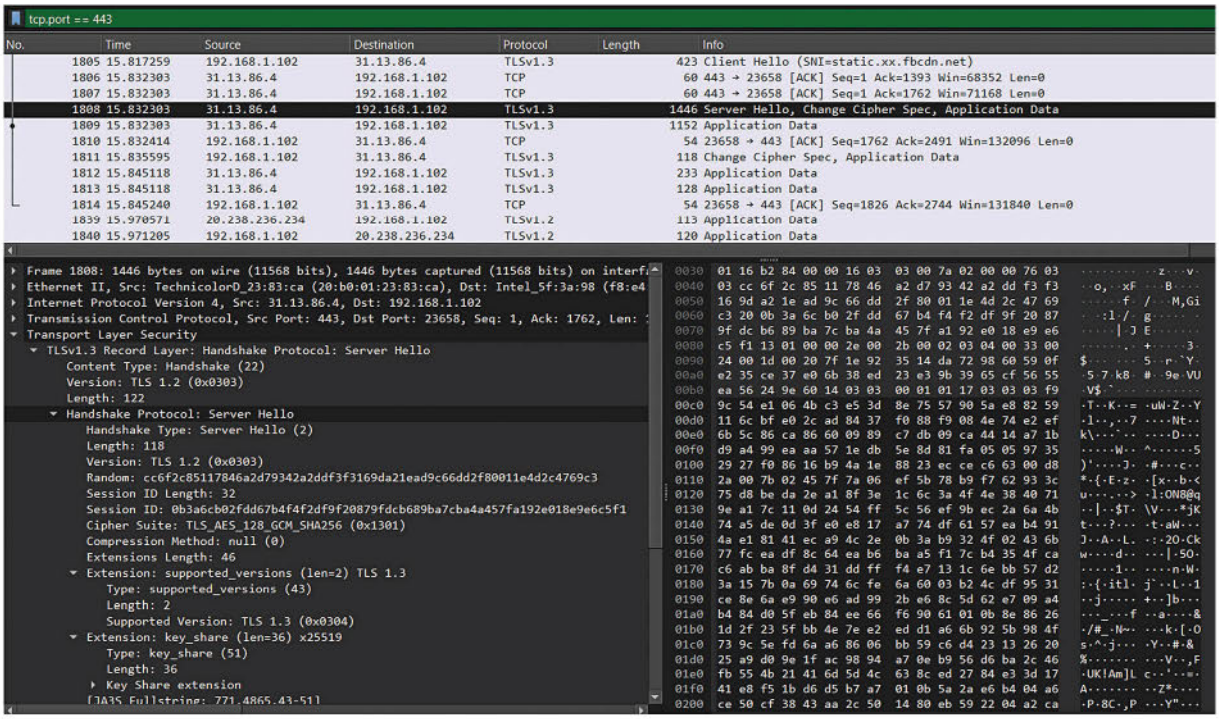
La figura mostra un estratto dei campi principali presenti in "TLSv1.3 Record Layer":

- Ethernet II: livello di Collegamento dati.
- Internet Protocol Version 4: livello di Rete con 'indirizzo IP di origine e di destinazione (31.13.86.4).
- Transmission Control Protocol: livello di Trasporto con porta di origine e di destinazione (443) del protocollo TCP.

- Transport Layer Security: con le informazioni sul protocollo di handshake TLS (Client Hello), tra cui:
  - il tipo di contenuto (22 - handshake);
  - la versione ("TLS 1.0");
  - la lunghezza (1756);
  - il tipo di handshake (Client Hello);
  - la versione ("TLS 1.2");
  - il valore casuale;
  - la lunghezza dell'ID di sessione;
  - l'ID di sessione;
  - la lunghezza delle suite di cifratura;
  - le suite di cifratura;
  - la lunghezza dei metodi di compressione;
  - i metodi di compressione e le estensioni aggiuntive (server name, status request ... pre_shared_key (le chiavi pre-condivise che il client mette a disposizione).

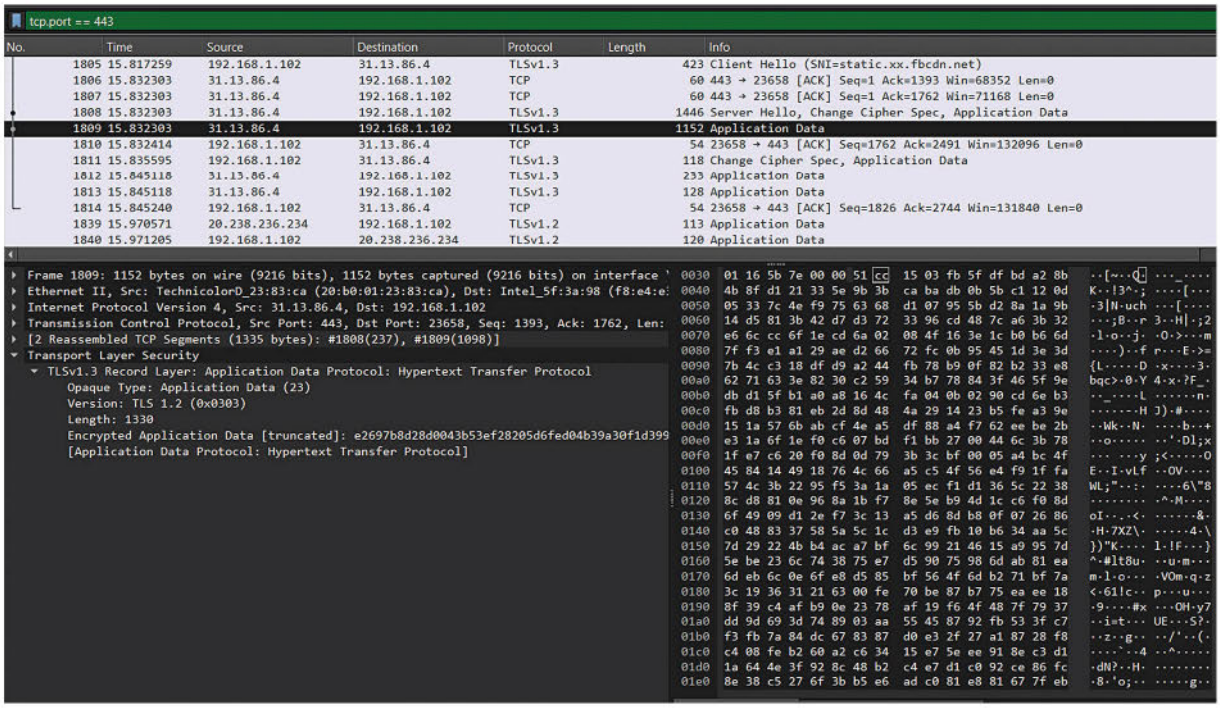
Notiamo che le diverse versioni di TLS che compaiono possono creare confusione. In realtà questo è dovuto al modo in cui il protocollo TLS gestisce la compatibilità con le versioni precedenti, Il client sta dicendo che, pur utilizzando il formato TLS1.3, in questa connessione è in grado di supportare versioni fino a TLS 1.2 e che la versione effettiva di TLS utilizzata per la connessione sarà determinata alla fine della fase di handshake di colloquio con il server.

Passo 3: analisi dei campi di "Server Hello"



Come nel passo precedente il campo Transport Layer Security mostra le informazioni sul protocollo di handshake TLS, tipo di contenuto (Server hello - 2), la versione (1.2), la lunghezza, il tipo di handshake, la versione, il valore casuale, la lunghezza dell'ID di sessione, l'ID di sessione, la suite di cifratura, il metodo di compressione e le estensioni.

Passo 4: analisi dei campi di "Application Data Protocol"



"Application Data Protocol: Hypertext Transfer Protocol" all'interno di Record Layer informa che il tipo di dati contenuti nel record TLS è relativo a «dati applicativi», cioè ai dati effettivamente scambiati tra client e il server. Tali dati sono quelli del protocollo HTTP utilizzato per trasferire la pagina web sul browser.
"Version: TLS 1.2 (0x0303)" indica che la versione di TLS utilizzata per il record "Application Data" è TLS 1.2, come concordato durante la fase di handshake. Di conseguenza i dati applicativi nel record sono crittografati utilizzando il tipo di cifratura e le chiavi stabilite.

ATTIVITÀ 4
Utilizzo di una VPN
Disponibile nell'eBook.

ATTIVITÀ 5
Applicazione di PGP
Disponibile nell'eBook.

SINTESI

VPN E PROTOCOLLI SICURI
Tecniche usate per garantire la sicurezza dei dati in rete in termini di riservatezza e integrità.

VPN (RETE PRIVATA VIRTUALE)
Tecnologia che utilizza la rete pubblica (Internet) per un collegamento sicuro, come se fosse una rete privata.

CLASSIFICAZIONE PER UTILIZZO
- Site-to-Site
- Remote access
- Personal

Site-to-Site
Utilizzata per collegare reti remote come se fossero un'unica rete. Utile per aziende con sedi distaccate.

Remote Access
Utilizzata per consentire a un host l'accesso a una rete privata da remoto. Utile a chi ha la necessità di accedere a risorse aziendali lavorando da remoto.

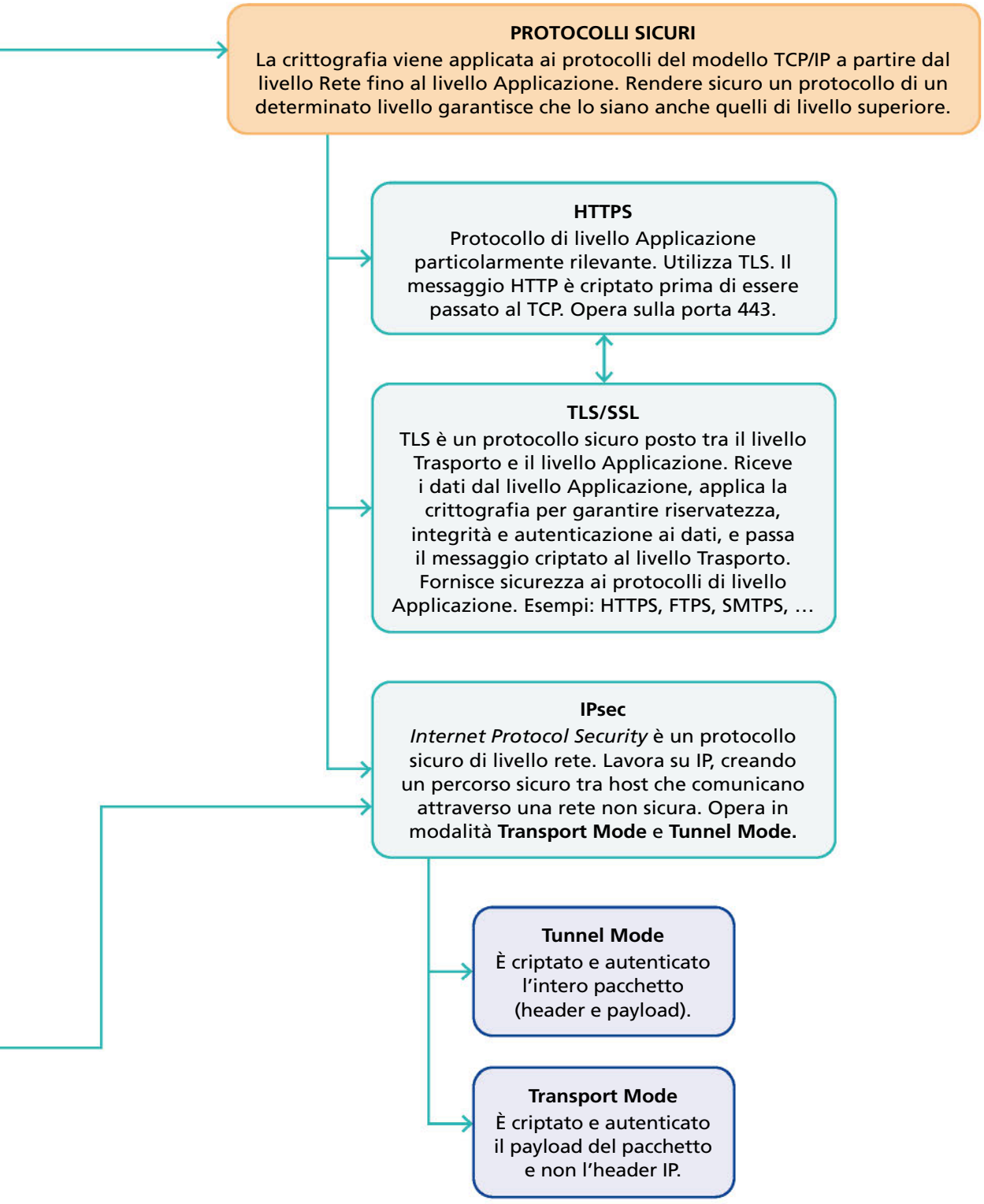
Personal
Utilizzata da utenti privati per accedere a risorse on line con garanzia di privacy.

CLASSIFICAZIONE PER SERVIZIO
- Trusted VPN
- Secure VPN
- Hybrid VPN

Trusted VPN
Ha come obiettivo la **qualità** del servizio. Un ISP crea e gestisce la rete privata, definendo un percorso dedicato su cui viaggiano i pacchetti.

Hybrid
Combina le caratteristiche delle VPN Secure e Trusted.

Secure VPN
Ha come obiettivo la **sicurezza** in termini di **riservatezza**. Si stabiliscono dei "tunnel virtuali" nei quali i dati viaggiano in modo sicuro e protetto anche in una rete pubblica come Internet. Un pacchetto è criptato e incapsulato in un ulteriore pacchetto dal software VPN all'ingresso del tunnel e estratto e decriptato dal software VPN all'uscita del tunnel, quando giunge alla rete di destinazione.


PROTOCOLLI SICURI
La crittografia viene applicata ai protocolli del modello TCP/IP a partire dal livello Rete fino al livello Applicazione. Rendere sicuro un protocollo di un determinato livello garantisce che lo siano anche quelli di livello superiore.
HTTPS
Protocollo di livello Applicazione particolarmente rilevante. Utilizza TLS. Il messaggio HTTP è criptato prima di essere passato al TCP. Opera sulla porta 443.
TLS/SSL
TLS è un protocollo sicuro posto tra il livello Trasporto e il livello Applicazione. Riceve i dati dal livello Applicazione, applica la crittografia per garantire riservatezza, integrità e autenticazione ai dati, e passa il messaggio criptato al livello Trasporto. Fornisce sicurezza ai protocolli di livello Applicazione. Esempi: HTTPS, FTPS, SMTPS, …
IPsec
Internet Protocol Security è un protocollo sicuro di livello rete. Lavora su IP, creando un percorso sicuro tra host che comunicano attraverso una rete non sicura. Opera in modalità Transport Mode e Tunnel Mode.
Tunnel Mode
È criptato e autenticato l'intero pacchetto (header e payload).
Transport Mode
È criptato e autenticato il payload del pacchetto e non l'header IP.

Verifica delle CONOSCENZE

Vero o Falso?

1 Le VPN Site-to-Site collegano in modo sicuro due o più LAN dislocate sul territorio, utilizzando la rete Internet. V F

2 MPLS è un protocollo usato per implementare la trusted VPN. V F

3 La trusted VPN ha un costo basso. V F

4 IPSec è un protocollo di livello applicazione. V F

5 SSL è un protocollo di livello rete. V F

6 HTTPS utilizza SSL. V F

7 HTTPS è un protocollo di livello trasporto. V F

8 La Security Association descrive la connessione sicura usata da IPsec. V F

9 ISAKMP è un protocollo usato per lo scambio delle chiavi in TLS. V F

10 SSL utilizza una chiave di sessione. V F

11 La crittografia può essere utilizzata solo dal livello applicazione per proteggere i dati dell'utente. V F

12 IPsec garantisce autenticazione e riservatezza. V F

13 Il certificato digitale assicura l'autenticazione della chiave pubblica. V F

14 Il protocollo SSL è supportato dai protocolli AH ed ESP. V F

15 HTTPS opera sulla porta 443. V F

16 In IPsec il Tunnel mMode è usato per i collegamenti in cui il protocollo è eseguito sui router. V F

17 HTTPS utilizza IPsec. V F

18 La VPN è usata solo in ambito aziendale. V F

19 La VPN è utile per lo smart working. V F

20 La modalità Transport Mode di IPsec mette al sicuro l'intero pacchetto. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

21 La VPN:

a. è una rete privata che utilizza una rete pubblica
b. è una rete pubblica che sfrutta una rete privata
c. Utilizza collegamenti fisici, sopra una infrastruttura di rete pubblica
d. è usata solo dalle grandi aziende perché è costosa

22 Il protocollo HTTPS utilizza:

a. SSL
b. IPsec
c. SHA
d. PGP

23 In una VPN, un tunnel

a. è usato nella modalità trusted
b. è usato solo tra sedi remote di un'azienda
c. è usato per il trasferimento di dati criptati da un host o da una rete ad un'altra rete
d. è un protocollo di livello Rete

24 Una VPN utilizza:

a. linee dedicate per lo scambio di dati
b. Internet e IPsec per la segretezza dei dati
c. HTTPS
d. l'infrastruttura di Internet e quindi è rischiosa

25 Una Trusted VPN:

a. è meno sicura di una Secure VPN
b. utilizza IPsec e SSL
c. definisce dei percorsi prestabiliti
d. è usata per comodità all'interno di una LAN

Domande per la prova orale

26 Che cosa sono le VPN e quali problemi risolvono?

27 Quali sono gli obiettivi di una VPN ad accesso remoto e quali quelli di una VPN Site-to-Site?.

28 Quali sono le differenze tra i due modelli di VPN, Trusted VPN e Secure VPN? Enumerane le caratteristiche.

29 Quali sono i tre obiettivi fondamentali del protocollo TLS/SSL?

30 Che relazione c'è tra i protocolli HTTP e SSL?

31 Perché SSL utilizza una chiave di sessione?

32 Quali sono le quattro fasi in cui si sviluppa SSL Handshake?

33 Come è gestito l'anonimato dai server proxy, dalle reti VPN e dai firewall?

34 Come è possibile rendere sicuri i protocolli di livello Applicazione?

35 Confronta il protocollo HTTP con il protocollo HTTPS.

36 Siano LAN1 e LAN2 due reti dotate ciascuna di un router R1 e R2 connessi ciascuno a un router di un ISP. Si vuole utilizzare una VPN Site-to-Site per consentire agli host delle due reti di comunicare in modo sicuro.

a. Descrivi le caratteristiche principali di una VPN Site-to-Site.
b. Evidenzia i vantaggi di una VPN Site-to-Site in ambito aziendale.
c. Descrivi la sequenza di operazioni da fare per realizzare il collegamento VPN tra LAN1 e LAN2.
d. Utilizzando Packet Tracer realizza il collegamento.
a. Effettua un test per verificare che il collegamento funziona osservando il contenuto dei PDU in ingresso e in uscita dai router delle LAN.

37 Un'organizzazione si avvale della consulenza di periti che operano sul territorio. I consulenti hanno la necessità di collegarsi alla rete della sede centrale dell'azienda da remoto.

a. Fai una rappresentazione grafica di massima della rete che coinvolge la rete aziendale e le postazioni dei consulenti.
b. Proponi una soluzione adatta a supportare il collegamento sicuro tra consulenti e rete aziendale.
c. Descrivi i passi da fare per attivare il collegamento.

38 Utilizzando Packet Tracer, crea una rete con un server web accessibile dall'esterno.

a. Effettua una richiesta al server web prima utilizzando HTTP e poi utilizzando HTTPS.
b. Osserva i PDU generati usando HTTP e HTTPS e riporta in una tabella le analogie e le differenze riscontrate.
c. Effettua una ricerca sul Web relativa alle VPN disponibili.
d. Riporta in una tabella le informazioni come di seguito.

Nome VPN	Servizi offerti	Sito di riferimento della VPN
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....



Esercizi in più

VPN and secure protocols

Abstract

VPN (*Virtual Private Network*) is virtual network which uses a public network – usually the Internet – to connect remote terminals together as if they belonged to the same local network. This allows to create virtual tunnels in which data travels in a safe and secure way, even in a public network. The main advantage of this method is to guarantee Information secrecy and quality of service, keeping costs low.

Secure tunnels are created thanks to cryptography-based network protocols. Cryptography is indeed used at network, transport and application level to make secure the related protocols.
For example, the IPsec protocol is used at network level, the SSL protocol (which, combined with HTTP, implements HTTPS protocol) is used at transport level. Other protocols at application level which use SSL are PGPand SSH.

Questions

Answer all questions

1 Which are the two VPN models?
2 At what level of the ISO / OSI model is SSL placed?
3 When is it convenient to use a VPN?
4 What are the objectives of PGP?

Choose the correct answer

5 The SSL protocol
- a is used by HTTPS
- b is a network layer protocol
- c ensures confidentiality but not authentication
- d ensures authentication but not confidentiality

6 The IPSec protocol tunnel mode
- a uses dedicated lines
- b uses predefined paths
- c ensures non-repudiation
- d is implemented on client

7 PGP
- a is a secure e-mail protocol
- b is a secure file transfer protocol
- c is a cryptographic algorithm
- d is a session key

8 Secure VPN guarantees
- a connection performance
- b data protection
- c service quality
- d use of a dedicated line

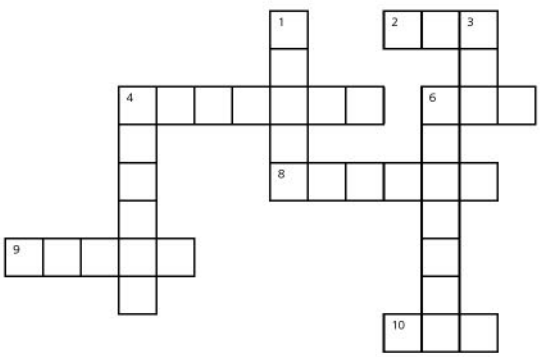
Crosswords

Across

2 Protocol for the definition of SA
4 Working mode of a VPN
6 Technology used to connect remote networks using a public network
8 Working mode of a VPN that uses tunnels
9 Secure protocol at the network layer
10 Secure protocol used by HTTPS

Down

1 Secure application-level protocol for the Web
3 Protocol used by IPsec
4 It is used to securely transmit data over a VPN
6 The «V» of VPN

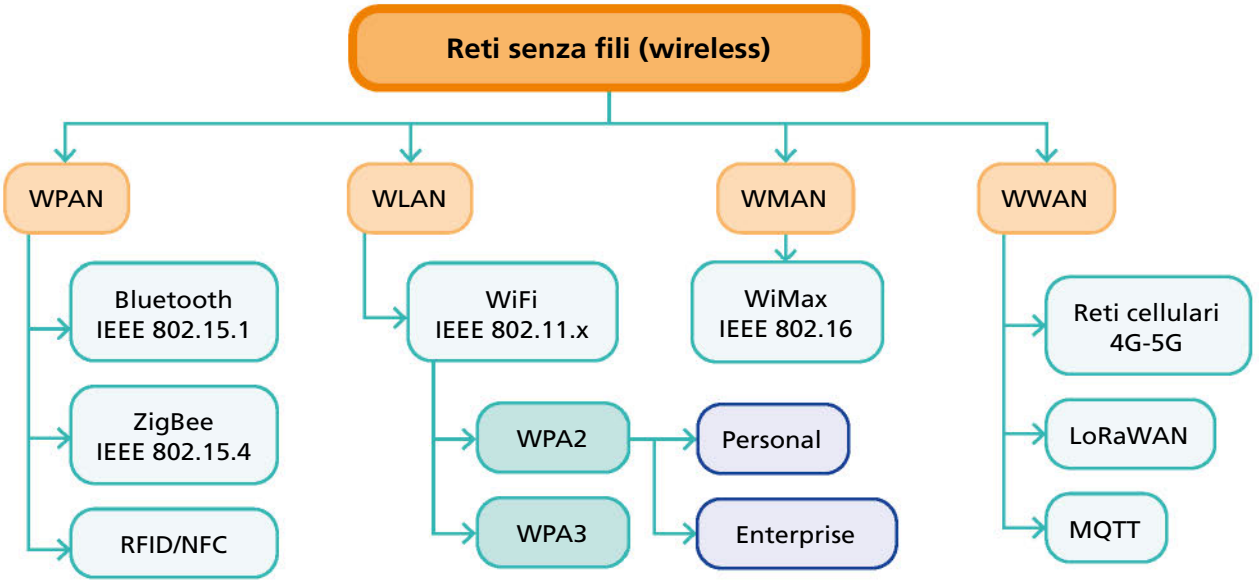




Unità

7

Le reti senza fili



Visione d'insieme

- Protocolli per reti senza fili (wireless).
- Sicurezza per reti WiFi (WLAN).
- Ambiti di utilizzo dei protocolli per reti wireless.

1 Introduzione

C'era un tempo in cui, quando squillava il telefono, ci precipitavamo verso la parete cui era appeso l'apparecchio. Poi il filo si è allungato, permettendoci di portare il telefono sul tavolino e, con una prolunga, fino al divano. Un giorno, siamo stati liberati per sempre dai cavi a cui eravamo legati come a una catena. Ci è stato dato in mano un dispositivo (possiamo ancora chiamarlo telefono?) che è diventato il nostro portafoglio, il nostro lettore musicale, il nostro libro, la nostra banca e il nostro assistente personale. Un cambiamento simile è avvenuto per le reti di dati: il pesante cablaggio ha lasciato il posto, dove possibile, alla leggerezza delle onde radio, trasformando le postazioni fisse e rigide in soluzioni mobili e flessibili.
Ma non è tutto. L'Internet of Things (IoT) ha fatto irruzione nella vita quotidiana, collegando oggetti al mondo digitale attraverso reti wireless. Sensori, lampade, termostati intelligenti e dispositivi indossabili comunicano tra loro e con Internet (Figura 1).
Il 5G, la quinta generazione di tecnologie di telefonia mobile, sta aprendo nuove opportunità. Con velocità teoriche fino a 10 gigabit al secondo e latenze ridotte, il 5G è la spina dorsale per l'IoT. Le reti 5G supportano comunicazioni tra macchine, veicoli autonomi, sensori di monitoraggio ambientale e molto altro, in un mondo sempre più connesso.
Mentre ci godiamo la libertà di connessione senza fili, dobbiamo anche considerare la sicurezza e la privacy. In questa unità, esploreremo le tecniche e i protocolli di sicurezza delle reti wireless.

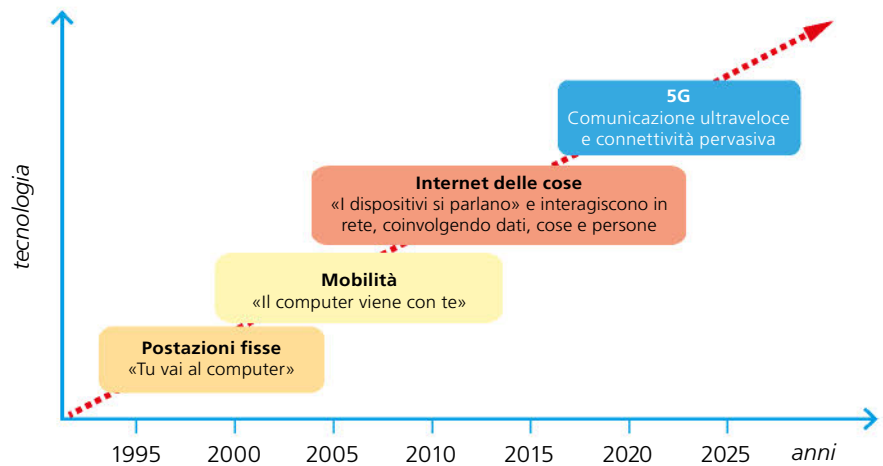
2 Panoramica dei protocolli nelle reti senza fili

Pit Stop

1 Quali sono le caratteristiche per la sicurezza delle reti senza fili?

Le reti senza fili si differenziano in base alle aree coperte e ai servizi offerti. La Figura 2 offre una panoramica, in termini di distanza e velocità, degli standard delle reti senza fili. Tutte le reti senza fili applicano i principi di autenticazione, integrità e riservatezza per proteggere i dati.

- **Autenticazione**: i protocolli di autenticazione spesso richiedono una chiave pre-condivisa o un certificato per accedere alla rete.
- **Integrità**: la garanzia di integrità si basa su meccanismi come l'utilizzo del **CRC** (**C***yclic* **R***edundancy* **C***heck*) e del **Message Digest** (Hash).
- **Riservatezza**: per proteggere la riservatezza dei dati, sono utilizzati algoritmi standard di crittografia, come **AES** (**A***dvanced* **E***ncryption* **S***tandard*).



➜ Fig. 1 L'evoluzione del modo di comunicare dei sistemi intelligenti nel tempo.

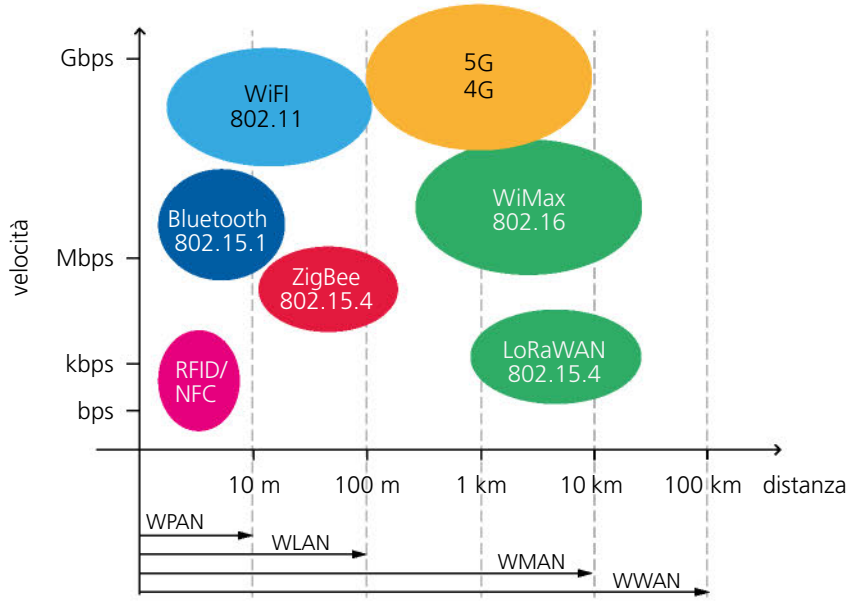


Fig. 2 Grafico qualitativo di comparazione delle distanze-velocità delle diverse tecnologie.

Pit Stop

2 Che cosa sono le reti WIFi e quali sono le loro principali caratteristiche?

La **Tabella 1** sintetizza una classificazione delle reti wireless, concentrandosi su distanze, standard e protocolli di sicurezza.

Tab. 1

Tipo di Rete	Descrizione e Distanze	Standard e protocolli di comunicazione	Protocolli di Sicurezza
WPAN (Wireless Personal Area Network)	• Reti personali. Coprono circa 10 metri. • RFID/NFC: coprono pochi centimetri.	• Bluetooth e Bluetooth Low Energy (BLE): IEEE 802.15.1 • Zigbee: IEEE 802.15.4 • RFID: ISO/IEC 14443 • NFC: ISO/IEC 18092	• Bluetooth: crittografia (AES) per garantire l'autenticazione, l'integrità e la riservatezza dei dati. • ZigBee: crittografia AES per garantire l'autenticazione, l'integrità e la riservatezza dei dati. • RFID e NFC possono utilizzare forme di crittografia.
WLAN (Wireless Local Area Network)	Reti locali senza fili. Arriva fino a circa 100 m.	IEEE 802.11a/b/g/n/ac/ax (Wi-Fi)	WPA2, WPA3 (Wi-Fi Protected Access)
WMAN (Wireless Metropolitan Area Network)	Reti wireless in aree metropolitane. Coprono fino a una cinquantina di km.	WiMAX (IEEE 802.16) e altri standard a banda larga.	Crittografia, come AES, per garantire l'autenticazione, l'integrità e la riservatezza dei dati.
WWAN (Wireless Wide Area Network)	• Reti cellulari per aree vaste (4G, 5G). Una cella 4G arriva a 10 km, una cella 5G a un paio di chilometri. • LoRaWAN (Long Range Wide Area Network). • MQTT (Message Queuing Telemetry Transport).	Standard diversi: GSM, LTE, CDMA.	• Reti di cellulari: crittografia end-to-end. • Dispositivi: autenticazione con SIM, biometrica ecc.
		LoRaWAN: standard gestito dalla LoRa Alliance.	LoRAWAN: crittografia AES per garantire l'autenticazione, l'integrità e la riservatezza dei dati.
		MQTT: ISO/IEC PRF 20922.	MQTT: Scenari di crittografia diversi.

La standardizzazione è importante per sfruttare in pieno il potenziale delle reti senza fili e, in particolare, dell'IoT.
La Tabella 2 cita alcuni esempi di consorzi nati con l'obiettivo di definire standard comuni tra produttori:

Organizzazione/Consorzio	Scopo
Bluetooth Special Interest Group (SIG)	Definisce gli standard Bluetooth, promuovendo l'interoperabilità tra dispositivi wireless.
Wi-Fi Alliance	Stabilisce le regole relative alla tecnologia Wi-Fi.
ETSI (European Telecommunications Standards Institute)	Definisce specifiche e protocolli per l'interoperabilità tra dispositivi e applicazioni IoT.
Open Connectivity Foundation (OCF)	Definisce specifiche aperte per la comunicazione tra dispositivi IoT.
OASIS (Organization for the Advancement of Structured Information Standards)	Lavora allo sviluppo di standard, come LoRaWAN e MQTT.

→ Tab. 2

3 Wi-Fi e la sicurezza

Wi-Fi è una famiglia di protocolli appartenenti alla famiglia WLAN. Le reti Wi-Fi sono state descritte nel Volume 2, Unità 1. Ne ricapitoliamo brevemente le caratteristiche principali.

- **Standard IEEE 802.11**: definiscono l'interfaccia tra un dispositivo wireless e un punto di accesso (AP, *Access Point*).
- **Access Point**: utilizzati per estendere la copertura.
- **Bande di frequenza**: trasmissione su onde radio nelle bande comprese tra **2,4 GHz** e **6 GHz**.
- **Distanza di copertura**: fino a circa **100 metri**; ma questa distanza può variare a seconda dell'ambiente circostante e degli ostacoli presenti.
- **Velocità di trasmissione**: fino a circa **10 Gbit/s**, ma dipende dallo standard Wi-Fi utilizzato.
- **Sono soggette a interferenze** causate da altri dispositivi elettronici e **attenuazioni** causate da muri e altri ostacoli fisici.

Le reti Wi-Fi presentano una **maggiore vulnerabilità rispetto alle reti cablate**, a causa dell'esposizione alle interferenze e al rischio di accesso da parte di malintenzionati che possono attuare attacchi "man-in-the-middle". Per questo motivo è necessario intervenire pesantemente per proteggere i dati trasmessi attraverso le reti con varie metodologie.
La Tabella 3 illustra le caratteristiche dei vari protocolli di sicurezza Wi-Fi, partendo dai protocolli WPA2 e WPA3, che saranno l'oggetto principale della nostra trattazione nei prossimi paragrafi, e arrivando alla rete aperta (l'opzione meno sicura).

Protocollo	Caratteristiche
WPA3	È il protocollo più recente e più sicuro. Utilizza la tecnica di crittografia Simultaneous Authentication of Equals (SAE), che tutela la privacy crittografando le connessioni individuali e offre una protezione contro gli attacchi "man-in-the-middle".
WPA2 Enterprise	Utilizza l'Advanced Encryption Standard (AES) per la crittografia e richiede un server RADIUS per l'autenticazione. È progettato per medie e grandi organizzazioni e fornisce un livello di sicurezza elevato.
WPA2 Personal	Utilizza AES per la crittografia e una chiave pre-condivisa (PSK) per l'autenticazione. È utilizzato nelle reti domestiche o nelle piccole organizzazioni.
WPA	Si appoggia al protocollo Integrity Check Protocol (TKIP) per garantire l'integrità dei dati durante la trasmissione. Offre un livello di sicurezza sufficiente, ma non in linea con le esigenze attuali.
WEP	WEP è il protocollo di sicurezza più antico, ormai obsoleto. Il metodo utilizzato per generare le chiavi crittografiche è stato scoperto e WEP non è più utilizzabile.
Rete aperta	Non ha alcun sistema di sicurezza: chiunque può connettersi alla rete e può vedere i dati che passano "in chiaro".

← Tab. 3

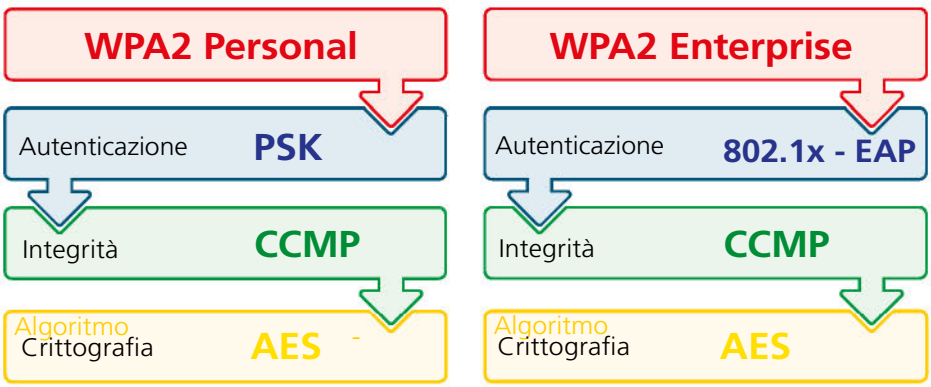
4 WPA2 – Wi-Fi Protected Access II

WPA2 (**W***i-Fi* **P***rotected* **A***ccess II - IEEE 802.11i*) garantisce la sicurezza della rete Wi-Fi tramite (Figura 3):

- **Riservatezza dei dati**. WPA2 utilizza la crittografia **AES** a chiave simmetrica per proteggere i dati. Per ogni connessione, viene generata dinamicamente una nuova chiave di crittografia.
- **Integrità dei dati**: WPA2 utilizza il protocollo **CCMP** (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) per garantire l'integrità dei dati. Questo protocollo combina la cifratura AES con un codice di autenticazione dei messaggi (MAC) per verificare l'integrità dei pacchetti trasmessi.
- **Autenticazione dell'utente**: WPA2 offre due modalità di autenticazione:
  - **WPA2-Personal** (**PSK**): utilizza una password pre-condivisa (Pre-Shared Key) condivisa tra tutti i dispositivi che si connettono alla rete;
  - **WPA2-Enterprise**: richiede un server RADIUS per l'autenticazione.

Pit Stop

3 Elenca i nomi dei principali protocolli per la sicurezza delle reti WiFi.



Pit Stop

4 Quali sono gli obiettivi della sicurezza del protocollo WPA2?

5 Quali sono le modalità in cui opera WPA2?

← Fg. 3 Caratteristiche del protocollo WPA2.

notabene

La lunghezza della PSK deve essere compresa tra 8 e 63 caratteri. La sicurezza di WPA2-PSK dipende dalla segretezza di PSK.

Modalità Personal

La modalità **WPA2-PSK** (**W***i-Fi* **P***rotected* **A***ccess* **2** *con* **P***re-***S***hared* **K***ey*), chiamata anche WPA2 Personal, prevede una serie di passaggi tra un dispositivo, ad esempio un Personal Computer, e un punto di accesso (AP *Access Point*).

- **Associazione iniziale**:
  - il PC individua l'identificatore della rete (SSID) trasmesso dall'AP;
  - l'utente seleziona la rete e inserisce la **password pre-condivisa** (**PSK-PreSharedKey**) nel PC, che è comune a tutti i dispositivi che si connettono in rete;
  - utilizzando la PSK e l'identificatore della rete (SSID), il PC crea un **Pairwise Master Key** (**PMK**);
  - l'AP verifica la PSK e accetta la richiesta di associazione.
- **4-Way Handshake**: il client e l'AP eseguono un handshake a quattro vie per generare una chiave di sessione a 128 bit, detta Pairwise Transient Key (PTK).
  - **Fase 1**: l'AP invia un "nonce" (un numero casuale utilizzato una sola volta) al PC.
  - **Fase 2**: il PC risponde con il suo nonce e calcola la chiave PTK.
  - **Fase 3**: l'AP conferma PTK e invia il suo nonce al PC.
  - **Fase 4**: il PC conferma il nonce dell'AP.
- **Crittografia dei dati**:
  - il PTK è utilizzato per cifrare i dati della comunicazione tra il PC e l'AP;
  - è utilizzato l'**Advanced Encryption Standard** (**AES**) per garantire la sicurezza;
  - il PTK viene rigenerato periodicamente per garantire la sicurezza.
- Ora il PC può trasmettere i dati in rete in **modo sicuro**.

Pit Stop

6 Quando è utilizzata la modalità Personal di WPA2?

7 Che cosa signifca "pre-shared"?

8 Come avviene l'autenticazione WPA2 in modalità Personal?

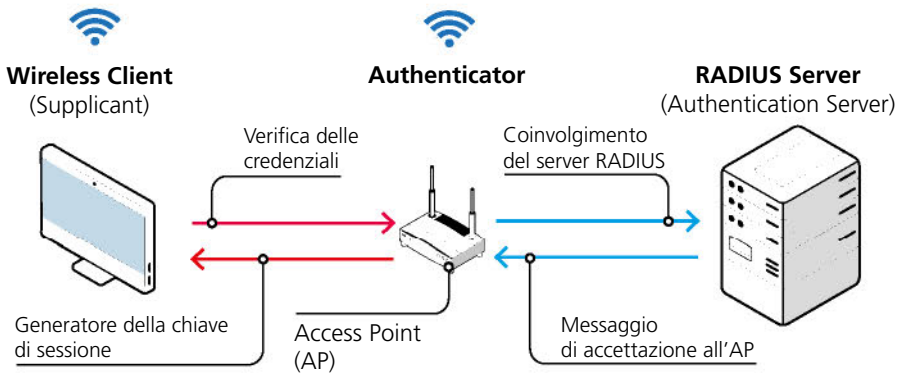
Modalità Enterprise

notabene

Per il funzionamento generale di un server RADIUS si veda l'approfondimento relativo.

La **modalità WPA2-Enterprise** prevede un processo di autenticazione più complesso rispetto alla modalità WPA2-PSK e coinvolge anche un **server di autenticazione**: il **server RADIUS** (**R***emote* **A***uthentication* **D***ial-***I***n* **U***ser* **S***ervice*), che verifica le credenziali del client e decide se accettare o rifiutare l'accesso.
L'autenticazione WPA2-Enterprise con **EAP** (**E***xtensible* **A***uthentication* **P***rotocol*) tra un PC (o qualsiasi client wireless), un Access Point e un server RADIUS avviene attraverso una serie di passaggi (Figura 4):

- **Verifica delle credenziali**:
  - il PC invia una richiesta di accesso all'Access Point (AP) per connettersi alla rete Wi-Fi;
  - l'AP risponde, avviando il processo di autenticazione;
  - il PC invia le proprie credenziali (nome utente e password) all'AP.
- **Coinvolgimento del server RADIUS**:
  - l'AP inoltra le credenziali del PC al server RADIUS;
  - il server RADIUS, che possiede un database con tutti gli utenti ammessi, verifica le credenziali e, se sono corrette, invia un messaggio di accettazione all'AP.
- **Generazione della chiave di sessione**:
  - dopo l'autenticazione, il PC e l'AP negoziano una chiave di sessione;
  - la chiave di sessione (**Pairwise Transient Key – PTK**) è generata dinamicamente utilizzando il **Master Session Key** (**MSK**), che varia a seconda del tipo di autenticazione EAP negoziato (ad esempio, **EAP-TLS**);



← **Fig. 4** Quando un client wireless richiede l'accesso a una risorsa LAN, il punto di accesso (AP) richiede l'autenticazione al server RADIUS.

  - durante questo processo, avviene il **4-Way Handshake** tra il client e l'AP per stabilire una connessione sicura e scambiare informazioni necessarie per creare la chiave di sessione.
- **Crittografia dei dati**:
  - la chiave di sessione (PTK) viene utilizzata per cifrare e decifrare i dati trasmessi sulla rete.
- Ora il PC può trasmettere i dati in rete in **modo sicuro**.

5 WPA3 (Wi-Fi Protected Access III)

WPA3 è stato introdotto nel 2018 per **migliorare la sicurezza delle reti Wi-Fi** rispetto a WPA2. Da allora, il protocollo WPA3 è stato supportato da Windows 10, macOS (dalla versione 10.15), Android (10 e successivi) e iOS (dalla versione 13). Tuttavia, molti produttori di dispositivi di accesso wireless implementano ancora una modalità "mista" WPA2/WPA3 per garantire la compatibilità con dispositivi più datati. Di seguito elenchiamo le caratteristiche principali di WPA3.

- **L'autenticazione** è realizzata con protocollo **Simultaneous Authentication of Equals** (**SAE**) che comprende le seguenti fasi (Figura 5):
  - **Fase di Commit**:
    - da Client ad AP: il messaggio di "commit" contiene un numero casuale generato dal client;
    - da AP a Client: il messaggio di "commit" contiene un numero casuale generato da AP e un numero derivato da questo numero casuale e dalla password della rete.
  - **Fase di Confirm**:
    - da Client ad AP. Il client invia un messaggio di conferma ad AP che contiene una prova che il client conosce la password di autenticazione (la chiave pre-condivisa) che è utilizzata per accedere alla rete Wi-Fi.
  - **4-Way Handshake**:
    - dopo l'autenticazione, i dispositivi scambiano ulteriori informazioni per generare una chiave segreta condivisa;
    - questa chiave segreta viene utilizzata per crittografare tutti i dati trasmessi sulla rete.
- La semplificazione del processo di connessione alla rete Wi-Fi dei dispositivi IoT, che non possiedono un'interfaccia, è attuata tramite la crittografia a chiave pubblica (**Easy Connect**). Con Wi-Fi Easy Connect un utente può semplicemente scansionare un QR code specifico del dispositivo IoT per connetterlo alla rete in modo sicuro.

notabene

In realtà il processo di autenticazione che abbiamo appena descritto è una semplificazione di quello reale, che coinvolge ulteriori dettagli e protocolli. Inoltre, ci sono diversi metodi EAP disponibili in WPA2-Enterprise, tra cui EAP-TLS.

Pit Stop

9 Quando è utile usare WPA2 in modalità Enterprise?

10 Come avviene la fase di autenticazione WPA2 in modalità Enterprise?

11 Qual è il ruolo di un Server RADIUS?

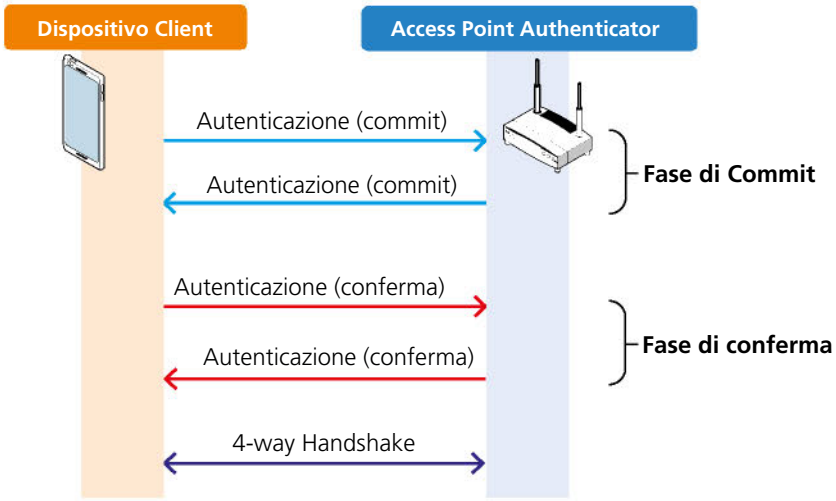
notabene

I numeri casuali servono ad aumentare la sicurezza durante l'autenticazione, perché introducono un elemento di imprevedibilità che rende più difficile a un attaccante decrittare i dati.

notabene

Sulla modalità PMF
Vedi Approfondimento: *L'attacco KRACK e il passaggio a WPA3*.

- La crittografia è a 128 bit (in **modalità WPA3-Personal**) e 192 bit (in **modalità WPA3-Enterprise**).
- La modalità **PMF** (**P***rotected* **M***anagement* **F***rames*) impedisce agli attacchi di disconnettere i client dalla Wi-Fi e monitorare la riconnessione.



➜ **Fig. 5** Diagramma semplificato del flusso di informazioni tra il dispositivo utente e l'Access Point nel processo di autenticazione SAE.

6 RFID e NFC

La tecnologia **RFID** (**R***adio* **F***requency* **I***dentification*) è utilizzata per rilevare le informazioni relative a un oggetto, persona, animale, sia fermi sia in movimento, tra cui l'identificatore univoco, la posizione e le caratteristiche. Gli elementi di un sistema RFID sono (Figura 6):

- **RFID Tag**: memorie che contengono dati. Possono essere passivi (alimentati dall'energia dell'onda radio emessa dal lettore) o attivi (con alimentazione autonoma). Ogni tag è composto da un transponder, che identifica l'oggetto a cui è assegnato un determinato impulso radio. È costituito da un microchip con antenna.
- **RFID Reader**: dispositivo per leggere o scrivere i dati da o sul tag. Legge il segnale inviato dal tag ed è caratterizzato da una antenna che genera un impulso elettromagnetico che permette al tag di attivarsi. Decodifica il segnale ricevuto dal tag per ottenere i dati memorizzati. Si interfaccia con il software.
- **Sistema di gestione dei dati**: per l'elaborazione e lo storage dei dati.

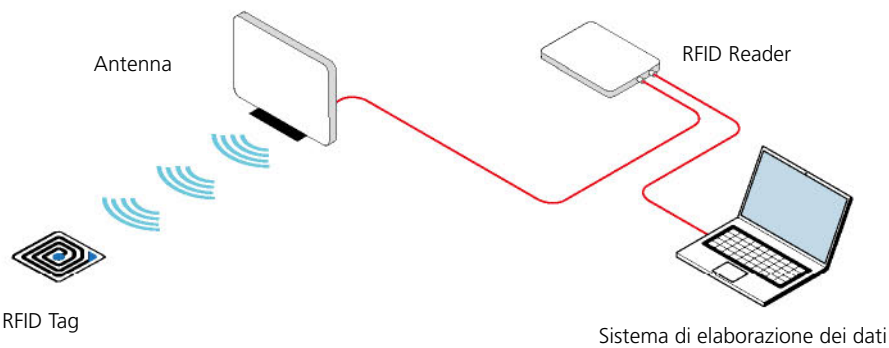
Pit Stop

12 Che cos'è WPA3?

13 In che cosa si differenzia WPA3 da WPA2?

14 Che cos'è un sistema RFID?

15 Quali sono le componenti di un sistema RFID?



➜ **Fig. 6** Elementi di un sistema RFID.

La trasmissione dati tra RFID Tag e RFID Reader è **wireless contactless** (senza contatto). Utilizza diverse frequenze per la trasmissione di dati, e la distanza di lettura varia in base alla frequenza e alla potenza dell'antenna del lettore. Di solito, la distanza di lettura è di qualche centimetro (con frequenze dell'ordine dei 100 kHz), ma in alcuni casi può arrivare fino a un centinaio di metri con frequenze di circa 900 MHz.
L'RFID si concentra principalmente sui livelli Fisico e di Collegamento dati:

- Il **livello Fisico** gestisce la comunicazione tra i dispositivi utilizzando onde radio. Questo include la trasmissione e la ricezione di segnali radio tra il tag RFID e il lettore RFID.
- Il **livello di controllo dell'accesso al mezzo** (**MAC**) controlla l'accesso al mezzo dei dispositivi RFID per evitare collisioni. Un esempio di questo è il protocollo ALOHA, in cui i dispositivi RFID trasmettono i dati senza sincronizzazione. Se si verifica una collisione (cioè, due o più tag trasmettono allo stesso tempo), i dispositivi ritrasmettono in momenti casuali.
- **Livelli superiori al MAC**: alcuni dispositivi RFID possono implementare livelli superiori al MAC, come il livello Rete, che gestisce la comunicazione tra i dispositivi su una rete più ampia, il livello Trasporto, che rende la trasmissione affidabile dei dati tra i dispositivi, e il livello Applicazione , che si interfaccia alle applicazioni che utilizzano la tecnologia RFID.

notabene
Tag è il termine per definire l'etichetta a radiofrequenza (RFID).

Pit Stop
16 Che cos'è un sistema NFC?

La tecnologia RFID consente il monitoraggio e il controllo di qualsiasi cosa sia dotata di etichetta a radiofrequenza.
Vari sono gli ambiti di utilizzo, tra i quali citiamo:

- gestione del magazzino e logistica;
- tracciabilità delle fasi di approvvigionamento di prodotti (supply chain);
- sistemi di monitoraggio;
- sistema anti-contraffazione e anti-taccheggio;
- identificazione di animali domestici;
- sistema di raccolta rifiuti;
- ambito sanitario.

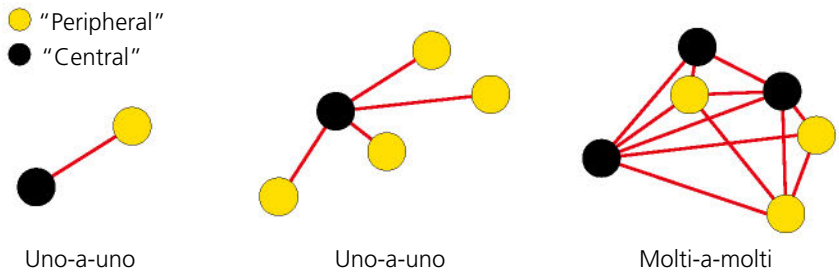
Rispetto a un codice a barre o a un QR code (Figura 7), un tag RFID ha le seguenti caratteristiche: è un oggetto fisico che contiene un circuito integrato, ha più resistenza nel tempo, rileva più dati contemporaneamente, richiede alimentazione, necessita di hardware e software più costosi. A differenza dei codici a barre, o QR code, i tag RFID possono essere letti anche se non sono direttamente visibili o allineati con il lettore.
La **tecnologia NFC** (**N***ear* **F***ield* **C***ommunication, Comunicazione di prossimità*), deriva da RFID. Fornisce connettività wireless bidirezionale, fino a un **massimo di 10 cm**, ma si riduce a 4 cm per garantire una connessione stabile. Funziona a una frequenza **radio di 13,56 MHz**. Per utilizzare l'NFC, un dispositivo deve avere un chip NFC integrato. Questo può essere presente direttamente nel dispositivo o su una SIM o scheda SD.
Le applicazioni più comuni riguardano i pagamenti contactless con gli smartphone o le carte di credito, il trasferimento di file per condividere immagini, video o contatti e l'accesso con il cellulare per accedere a un edificio o registrarsi su un volo.



→ **Fig. 7** Tag RFID, codice a barre e codice QR per identificare un oggetto.

7 Bluetooth

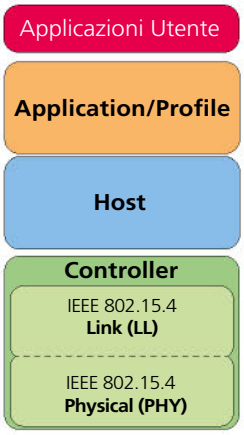
Bluetooth è una tecnologia utilizzata per le reti Wireless Personal Area Network (WPAN). È spesso impiegata in dispositivi di uso quotidiano come smartwatch, tracker fitness, sistemi indossabili (wearable) e per fornire informazioni in musei e negozi.
La prima specifica Bluetooth risale al 1999. Nel 2010 è stato introdotto Bluetooth Low Energy (BLE) per dispositivi a basso consumo energetico. Nel 2022 è stata rilasciata la versione Bluetooth 5.3.
La maggior parte dei dispositivi Bluetooth comunica utilizzando diverse topologie di rete (**Figura 8**):



➜ **Fig. 8** Le topologie di Bluetooth.

- **Uno-a-uno** (punto-punto): è la topologia più comune, utilizzata da molti dispositivi wireless in cui un dispositivo ha un ruolo "Central" e chi si collega ha il ruolo "Peripheral", come altoparlanti e cuffie che si collegano a uno smartphone.
- **Uno-a-molti**: è la topologia in cui il Central può connettersi a più dispositivi (Peripheral) contemporaneamente. Ad esempio, un telefono cellulare può essere collegato a più auricolari Bluetooth. Una rete formata da un dispositivo Bluetooth LE Central e uno o più dispositivi Peripherals prende il nome di "piconet". Una rete "scatternet" è formata da più piconet collegate tra loro.
- **Molti-a-molti** (rete mesh): è la topologia in cui più dispositivi Bluetooth comunicano tra loro fino a comprendere un'area geografica ampia e contenente un gran numero di dispositivi. La topologia mesh disponibile su Bluetooth Low Energy (BLE) è utilizzata spesso per sistemi di controllo e monitoraggio. Nelle reti mesh, alcuni dispositivi possono agire come Central, mentre altri come Peripheral.

L'architettura del protocollo Bluetooth è costituita da tre livelli sovrapposti (**Figura 9**):



- **Controller**: comprende i livelli più bassi, basati su IEEE 802.15.4, cioè il Physical Layer (PHY), che gestisce la modulazione del segnale di trasmissione, e il Link Layer (LL), che è responsabile dell'accesso al mezzo CSMA (Carrier Sense Multiple Access with Collision Avoidance) e della trasmissione affidabile dei dati.
- **Host**: adatta il formato delle trame tra i livelli (comprende il Logical Link Control and Adaptation Protocol).
- **Application**: fa da interfaccia con le applicazioni Bluetooth.

➜ **Fig. 9** Architettura semplificata dei livelli di Bluetooth. Il livello Fisico utilizza bande di frequenza comprese tra 800 MHz e 2400 MHz.

La parola a... Harald I (Bluetooth)



Nella Cattedrale di Roskilde, antica prima capitale vichinga, riposa Harald I, il primo re di Danimarca. Accanto al suo nome, è inciso il soprannome Blåtand, che in antico scandinavo significa "dente blu": in inglese, Bluetooth, proprio come l'omonima tecnologia moderna che collega i dispositivi tra loro. Questo curioso legame deriva dal fatto che Harald, che visse tra il 911 e il 986 d.C., compì imprese straordinarie, tra cui l'unificazione delle terre di Danimarca, Svezia e Norvegia sotto un unico regno. In maniera analoga, la tecnologia Bluetooth mira a connettere numerosi tipi di dispositivi.
Immaginiamo le parole di Harald oggi: «*Popoli tutti, ascoltatemi! Le nostre terre sono frammentate, divise da tribù e rivalità. Ma io vedo un futuro migliore. È giunto il momento di unificare le terre in modo che le spade non si rivolgano l'una contro l'altra, ma vengano usate per costruire ponti che uniscano i nostri destini.*»
Ci piace pensare che le parole di Harald "Bluetooth" continuino a ispirare la nostra tecnologia moderna, alimentando la visione di un mondo unito e collaborativo.

In cima allo stack si innestano le **applicazioni Bluetooth**, come ad esempio quelle per la lettura dei dati da sensori, per il controllo di dispositivi smart o per la gestione di dispositivi indossabili.
Bluetooth garantisce la sicurezza dei dati attraverso l'autenticazione dei dispositivi e la riservatezza.
Utilizza un processo di accoppiamento per **autenticare i dispositivi** prima di stabilire una connessione. Il processo comprende:

- la scoperta dei dispositivi;
- una richiesta di accoppiamento che comporta l'invio di una chiave pubblica;
- la conferma dell'utente;
- uno scambio di chiavi che porta alla generazione di una chiave di sessione condivisa.

La chiave di sessione viene utilizzata per **crittografare i dati** durante la comunicazione. Per quanto riguarda l'**integrità dei dati**, utilizza il **Message Integrity Code** (**MIC**), un valore hash che viene calcolato e trasmesso insieme ai dati per rilevare eventuali alterazioni del messaggio trasmesso.

notabene

Message Integrity Code (MIC) è un valore hash del messaggio che viene allegato al messaggio stesso.

8 ZigBee

ZigBee si basa sullo standard **IEEE 802.15.4**, progettato per le comunicazioni a bassa potenza e a corto raggio.
Per la sua semplicità è utilizzato soprattutto per soluzioni domotiche (smart home), per le operazioni di misurazione dei consumi (smart metering) e per la gestione di distribuzione dell'energia (smart grid).

Pit Stop

17 Che cos'è il Bluethoot?

18 Quali sono le caratteristiche di Bluetooth?

19 Che cos'è Zigbee?

La struttura di una rete ZigBee supporta diverse topologie: a stella, ad albero e a maglia (mesh). Nelle reti a stella, ogni rete ha un dispositivo che fa da coordinatore e da nodo centrale. Sia le topologie ad albero, sia le topologie mesh, consentono l'uso dei router ZigBee per estendere le comunicazioni a livello di rete (**Figura 10** e **Tabella 4**).

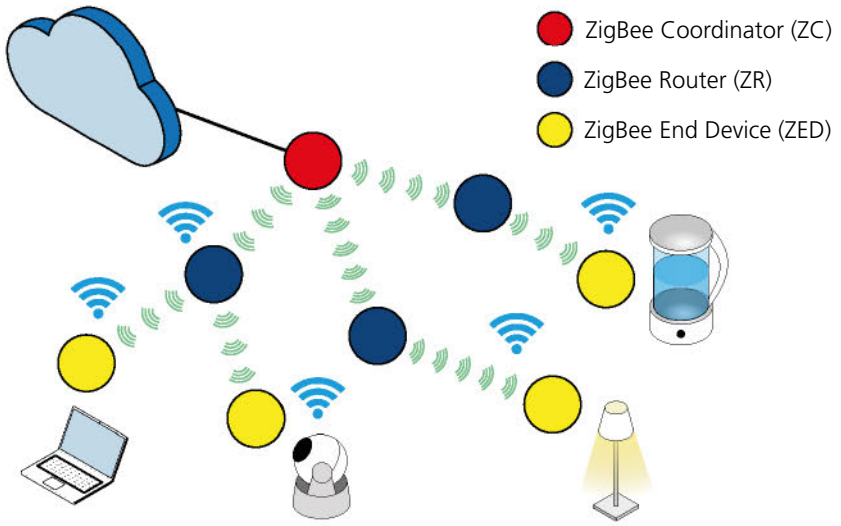
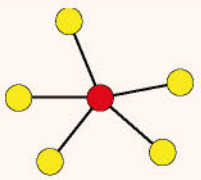
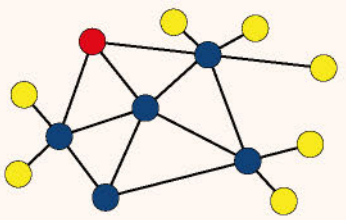
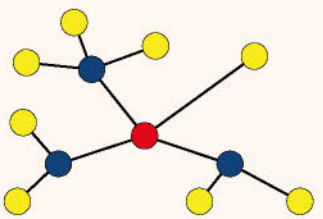


Fig. 10 Un esempio di struttura di rete ZigBee con sistema centrale di coordinamento, router e dispositivi finali. ZigBee è progettato per essere più semplice ed economico di altre reti wireless personali, come Bluetooth o Wi-Fi.

Tab. 4

Topologia delle reti ZigBee	
• **ZigBee Coordinator**: inizializza la rete, gestisce i vari nodi e le informazioni. • **ZigBee Router**: instrada i messaggi tra i vari nodi della rete. • **ZigBee End device**: nodi che posseggono solo le funzionalità minime per interagire con Coordinator e Router.	
	• **Star** (**stella**): gli "*end device*" si collegano direttamente al coordinatore. È semplice e facile da implementare.
	• **Mesh** (**maglia**): diversi router sono collegati al coordinatore per permettere ai nodi di comunicare tra loro. Questa topologia garantisce la ridondanza dei percorsi e l'instradamento automatico verso altri nodi in caso di guasti. È utile nelle situazioni in cui è richiesta affidabilità.
	• **Tree** (albero): in una topologia ad albero la rete è costituita da un coordinatore centrale (radice) a cui si collegano: router e dispositivi terminali. Ogni end device è in grado di comunicare solo con il router o con il coordinatore.

L'architettura del protocollo ZigBee 3.0 è costituita da una pila di livelli (Figura 11). Esaminiamo i singoli livelli in dettaglio.

- **Livello fisico**: questo strato gestisce le operazioni di modulazione e demodulazione dei segnali e utilizza 3 bande di frequenza comprese tra 800 MHz e 2400 MHz.
- **Livello MAC**: è responsabile della trasmissione affidabile dei dati accedendo a reti diverse con accesso al mezzo CSMA (Carrier Sense Multiple Access with Collision Avoidance) che, periodicamente, trasmette anche i frame beacon per sincronizzare la comunicazione. Il campo FCS (Frame Check Sequence) presente nella trama MAC assicura il controllo degli errori (Tabella 5).
- **Livello Rete** (**Network**): sfrutta le varie potenzialità del canale radio IEEE 802.15.4, occupandosi della gestione dei dispositivi con la connessione e la disconnessione alla rete e il routing tra i nodi. In particolare, la trasmissione dei messaggi avviene attraverso i nodi della rete scegliendo il percorso migliore. L'applicazione dello standard AES (Advanced Encryption Standard) sui frame trasmessi e ricevuti applica la sicurezza.
- **Livello Applicazione** (**Application Framework**). Fornisce due servizi:
  - **APS** (**Application Object**): permette il discovery dei nodi nella rete;
  - **ZDO** (**ZigBee Device Object**): si occupa della classificazione di un nodo, per esempio coordinator, delle sue funzionalità e della scelta della metodologia di sicurezza più efficace.
- **Applicazioni Utente**. Sopra l'Application Framework ci sono le applicazioni Utente. Queste applicazioni utilizzano i servizi forniti dall'Application Framework per comunicare con altri dispositivi nella rete. Le applicazioni possono essere molto diverse tra loro, a seconda delle specifiche esigenze del dispositivo o del sistema. Ad esempio, un'applicazione potrebbe gestire un sensore di temperatura, mentre un'altra potrebbe controllare un interruttore di luce.

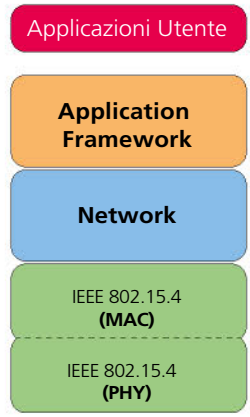


Fig. 11 I livelli dello stack ZigBee 3.0.

ZigBee garantisce l'autenticazione, la riservatezza e l'integrità.

- **Autenticazione dei dispositivi**. Una "chiave di collegamento" (**Link Key**), pre-condivisa dal dispositivo con il coordinatore di rete, permette di autenticare i dispositivi all'interno della rete.
- **Riservatezza dei messaggi**. Utilizza la crittografia AES, con una "chiave di rete" (**Network Key**), condivisa tra tutti i dispositivi.
- **Integrità dei dati**. Il **Message Integrity Code** (**MIC**), un valore di hash calcolato utilizzando la chiave Network Key, consente di rilevare eventuali alterazioni del messaggio trasmesso.

Pit Stop

20 Quando conviene usare Zigbee?

21 Quali sono gli obiettivi di sicurezza garantiti da Zigbee?

notabene

La prima specifica di ZigBee risale al 2004, migliorata nel 2007 con ZigBee PRO e ZigBee 2007. Dal 2014 ZigBee 3.0 ha unificato le versioni precedenti aggiungendo reti mesh e livelli di sicurezza, insieme a un framework applicativo.

Ottetti 2	1	0/2	0/2/8	0/2	0/2/8	variabile	2
Frame Control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame Check Sequence

Tab. 5 La trama 802.15.4 con i campi di controllo, gli indirizzi sorgente e destinazione e FCS per il controllo degli errori.

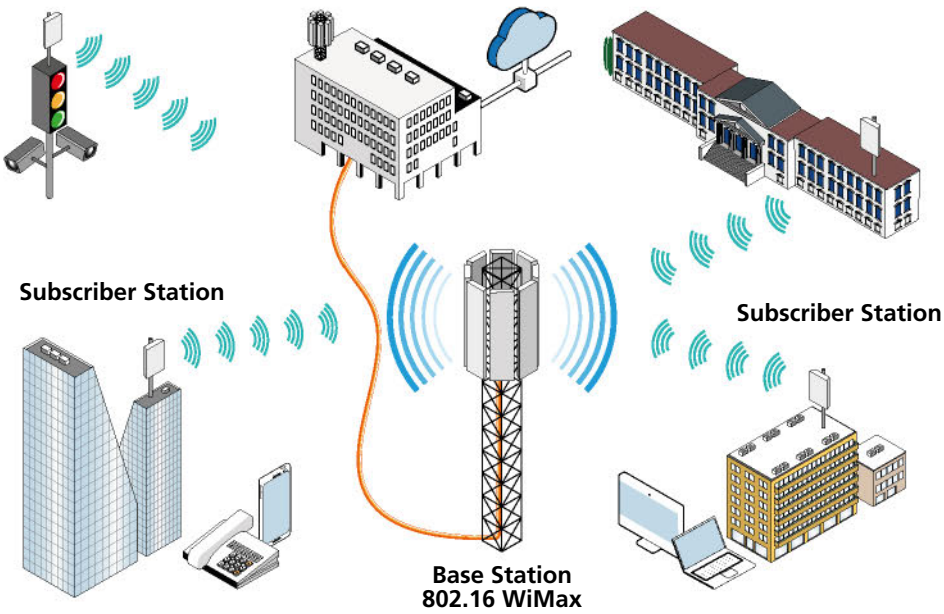
9 WiMAX

WiMAX (*Worldwide Interoperability for Microwave Access*) è una tecnologia appartenente alla famiglia WMAN, definita dallo standard IEEE 802.16, che consente l'accesso senza fili a Internet ad alta velocità in aree extraurbane o dove la fibra ottica non arriva. Le reti WiMAX adottano una topologia Punto-Multipunto (PMP), in cui una Base Station (BS, Stazione Base), l'antenna principale, comunica con diverse Subscriber Station (SS). Le SS sono i dispositivi finali, che di solito comprendono un'antenna con cui collegarsi alla BS, installati presso il cliente (Figura 12). L'accesso a una stazione base WiMAX è simile all'accesso a un Access Point di una rete Wi-Fi, ma con una copertura maggiore, che può arrivare fino a qualche decina di chilometri.

Pit Stop

22 Che cos'è WiMax?

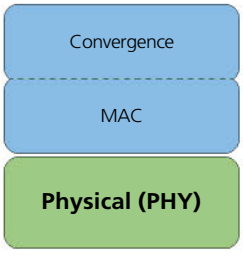
23 Quando conviene usare WiMax?



➜ **Fig. 12** Topologia Punto-Multipunto (PMP).

L'architettura WiMAX è divisa in strati, che si sovrappongono parzialmente ai primi due livelli del modello TCP/IP (Figura 13):

- **Physical Layer**: converte le trame MAC gestendo la codifica e la decodifica dei segnali radio. Specifica la banda di frequenza (sotto i 10 GHz) e il tipo di modulazione.
- **MAC Layer**: costituisce l'interfaccia tra il livello di Convergenza e il livello Fisico. Controlla l'accesso al mezzo con CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) delle trame dati.
- **Convergence Layer**: accetta unità di dati di protocollo (PDU) dal livello superiore e le converte in trame per il livello MAC.



↑ **Fig. 13** I livelli della pila del protocollo WiMax 802.16.

A livello rete, WiMAX supporta il protocollo IP, consentendo l'accesso a Internet e la comunicazione tra dispositivi.
Per proteggere le comunicazioni, WiMAX utilizza:

- l'algoritmo di crittografia AES (Advanced Encryption Standard) per la riservatezza;
- algoritmi di hash come SHA-1 o SHA-256 per l'integrità dei dati;
- chiavi pre-condivise o certificati digitali per l'autenticazione dei dispositivi.

10 LoRaWAN

Il protocollo **LoRaWAN** (*Long Range Wide Area Network*) è parte della famiglia LPWAN (Low Power Wide Area). È un protocollo open source definito dalla LoRa Alliance, un'organizzazione che promuove questa tecnologia. È caratterizzata da un copertura a lungo raggio (dai 5 km delle aree urbane, ai 40 km delle aree rurali) che permette la trasmissione su reti wireless a bassa potenza.
L'architettura comprende i livelli Fisico e Collegamento dati.

- Il **Physical Layer** (**PHY**) impiega la modulazione **LoRa** (*Long Range*), che opera su frequenze senza licenza. In Europa, la banda di frequenza è compresa tra 863 MHz e 870 MHz.
- Il **Data Link Layer** (**MAC**) ha diverse funzioni:
  - stabilisce la connessione tra il gateway e il dispositivo;
  - formatta le trame MAC con l'intestazione e con l'aggiunta del codice di integrità del messaggio (MIC) al campo dati.

La struttura della rete comprende (Figura 14):

- **nodi finali**, che includono i sensori, che comunicano i dati a un gateway;
- **gateway**, che fa da concentratore e ponte tra i dispositivi finali e il Network Server. Riceve i dati dai nodi finali e li invia al Network Server;
- **Network Server**, che supporta il protocollo LoRaWAN, garantendo l'efficienza e la sicurezza della rete. Riceve i dati dal gateway e li invia all'Application Server;
- **Application Server** , l'applicazione che elabora i dati per analizzarli e inviare notifiche agli utenti finali o ad altre applicazioni.

Garantisce l'integrità e la riservatezza dei messaggi utilizzando due chiavi diverse:

- **Integrità dei messaggi**. Utilizza la chiave **NwkSKey** (*Network Session Key*) per calcolare il Message Integrity Code (MIC) dei messaggi inviati dal dispositivo al Network Server. Questo permette al Network Server di verificare che il messaggio non sia stato alterato durante la trasmissione.
- **Riservatezza dei messaggi**. Utilizza la chiave **AppSKey** (*Application Session Key*), per cifrare i dati tra il dispositivo e l'Application Server, utilizzando la crittografia AES-128.

Pit Stop

24 Che cos'è LoRaWAN?

25 Quando conviene usare LoRaWAN?

26 Quali sono gli obiettivi di sicurezza realizzati da LoRaWAN?

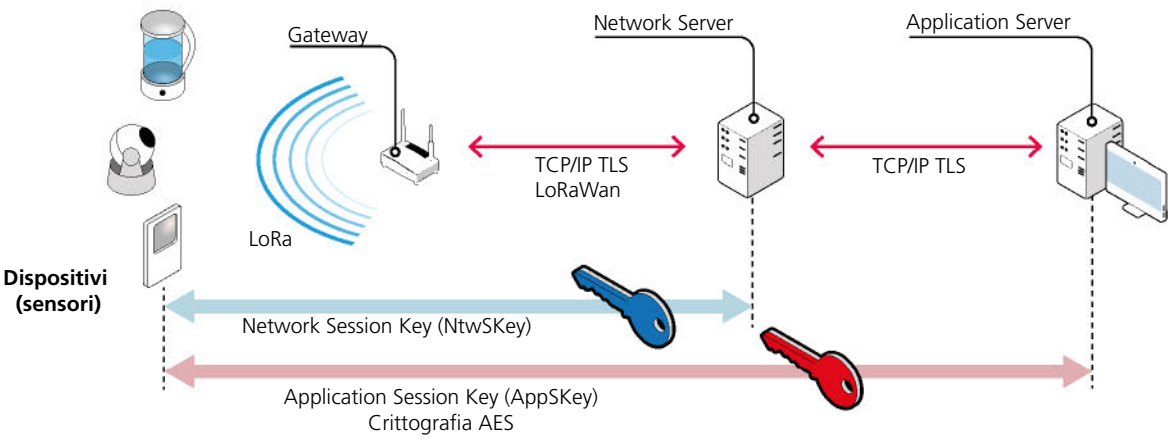


Fig. 14 Schema di un tipo di collegamento che utilizza LoRaWAN per trasmettere i dati su un server in Internet.

All'interno delle reti con dispositivi IoT, è spesso utilizzato il **gateway**, che facilita la comunicazione tra dispositivi con interfacce diverse e l'accesso a reti esterne. Anche il **router** permette la connessione di reti interne con quelle esterne. Tuttavia ognuno ha caratteristiche proprie, utili in contesti diversi, come mostrato nella Tabella 6 che confronta le funzioni di un router con quelle di un gateway LoRaWAN.

notabene

Con il termine "backhaul" ci si riferisce al collegamento di rete tra i dispositivi di livello inferiore e i sistemi di livello superiore. In LoRaWAN, il backhaul indica il collegamento tra i gateway e il Network Server.

Fig. 15 a. Un esempio di gateway interno; b. un esempio di gateway esterno.

a



b



Tab. 6

Router	Gateway LoRaWAN
• **Gestisce il traffico dei pacchetti** IP tra i dispositivi di una LAN e Internet. • Individua il **percorso migliore** per il transito dei pacchetti in Internet. • Può implementare **regole di sicurezza** e filtraggio dei pacchetti. • Fornisce funzionalità di **NAT** per consentire a più dispositivi di condividere un indirizzo IP pubblico. • Non è specificamente progettato per l'aggregazione di dati da interfacce diverse.	• **Gestisce il traffico da dispositivi con interfacce diverse**, aggregando i dati e convertendo protocolli • Riceve i messaggi dai dispositivi finali (come sensori e attuatori) tramite la modulazione LoRa e li **inoltra al network server**. • Si differenzia a seconda dell'ambito di utilizzo: – **Indoor**: adatto per spazi interni come uffici o case (Figura 15a). – **Outdoor**: coprono aree esterne più vaste rispetto ai gateway interni, sia urbane che rurali. Sono montati su torri cellulari o alti edifici (Figura 15b). • Comunica con il Network Server tramite: – **una rete dedicata a LoRaWAN**, senza passare attraverso Internet. Questo collegamento (backhaul) può essere realizzato tramite diverse tecnologie, come la fibra ottica, il WiFi, Ethernet o le reti cellulari (4G/5G). – **Internet**: invia i dati al router della rete locale a cui è connesso, che a sua volta instrada i dati attraverso la connessione Internet fino al Network Server. • Può lavorare in **collaborazione con altri gateway** in modo da coprire un'area geografica più ampia con maggiore affidabilità.

11 MQTT

MQTT (**M***essage* **Q***ueuing* **T***elemetry* **T***ransport*) è un protocollo open-source di **livello Applicazione** che opera sopra il livello Trasporto dello stack TCP/IP: TCP garantisce la consegna affidabile dei dati, mentre IP gestisce il collegamento alla rete. MQTT non richiede un protocollo specifico a livello di collegamento dati, ma può utilizzare Ethernet, Wi-Fi, Zigbee o Bluetooth a seconda del contesto. Si basa su un'**architettura di tipo publish/subscribe** in cui i dispositivi possono "pubblicare" informazioni, e altri dispositivi possono "sottoscriversi" per ricevere queste informazioni secondo un processo che coinvolge quattro componenti principali:

- **Publisher**:
  - è un client che pubblica messaggi su specifici "argomenti" (topic) su un nodo intermedio chiamato broker;
  - può inviare un argomento alla volta e non deve preoccuparsi che gli abbonati siano online quando pubblica un messaggio;
- **Subscriber**:
  - è un client che riceve i messaggi a cui è interessato;
  - si iscrive a uno o più argomenti specifici per ricevere i messaggi pubblicati su quei topic;
  - gli abbonati possono iscriversi a più argomenti contemporaneamente;

notabene

Originariamente creato da IBM, è ora supportato dal consorzio OASIS, che promuove lo sviluppo e l'adozione di standard aperti per la comunicazione tra dispositivi IoT.

Comprendi con l'analogia

La comunicazione tra insegnanti e studenti è analoga a quella tra gateway e nodi finali della rete LoRaWAN



Gli **studenti** sono i **nodi finali** nella rete LoRaWAN. Ognuno di loro ha qualcosa da dire all'insegnante (trasmette dati). L'insegnante rappresenta il **gateway** LoRaWAN. È il punto centrale di comunicazione e ascolta gli studenti .

La conversazione

La conversazione tra studenti e insegnante avviene in modo asimmetrico: più studenti cercano, nello stesso momento, di comunicare con l'insegnante, ma l'insegnante non può ascoltarli tutti contemporaneamente e può non sentire delle domande. Allo stesso modo, i nodi finali trasmettono i loro messaggi via radio contemporaneamente, ma il gateway può riceverne solo uno alla volta. Se un messaggio non viene ricevuto dal gateway, i dati contenuti in quel messaggio andranno persi. Per garantire una copertura adeguata, potrebbe essere necessario aumentare il numero di gateway.

I gateway multipli

Immaginiamo due insegnanti in laboratorio. Quando uno studente parla, entrambi gli insegnanti possono ascoltarlo. Questo è vantaggioso perché se un insegnante si distrae, la comunicazione non va persa.
Pensiamo ora a due gateway. Quando un nodo finale trasmette un messaggio, entrambi i gateway lo ascoltano. Questo è vantaggioso perché almeno uno dei gateway riceverà il messaggio, aumentando l'affidabilità della rete. Inoltre, la ridondanza fa sì che se un gateway fallisce o è fuori servizio, l'altro gateway possa ancora ricevere i messaggi.

Duplicazione di messaggi

La richiesta di uno studente può essere duplicata se entrambi gli insegnanti la recepiscono. Tuttavia questo è superato dal fatto che entrambi gli insegnanti hanno in mente chiaramente il tempo in cui la richiesta è stata fatta; un messaggio potrebbe essere duplicato se è ricevuto da entrambi i gateway. Per gestire questa situazione, i gateway includono informazioni di timestamp nei messaggi ricevuti, consentendo al server di identificare e gestire le duplicazioni.

Ricevuta di consegna

Dopo aver trasmesso il messaggio, non c'è alcuna conferma di ricevimento da parte dell'insegnante (o del gateway). Tuttavia, gli studenti possono richiedere all'insegnante (o al gateway) una ricevuta di consegna (come chiedere all'insegnante la consegna di una verifica) per assicurarsi che il messaggio sia stato ricevuto.

- **Broker**:
  - è il nodo intermedio responsabile della ricezione dei messaggi dai publisher e dell'inoltro agli abbonati;
  - gestisce anche le richieste dei client per la connessione, la disconnessione, la sottoscrizione e l'annullamento della sottoscrizione;
- **Topic**:
  - MQTT instrada i messaggi in base agli argomenti;
  - più abbonati possono iscriversi allo stesso argomento, e il broker inoltrerà tutti i messaggi su quell'argomento a questi abbonati;
  - più editori possono inviare messaggi allo stesso argomento, e il broker instraderà questi messaggi nell'ordine in cui vengono ricevuti ai client sottoscritti;
  - la sintassi di un topic è simile a quella di un URL con una barra che separa i livelli. Ad esempio, un argomento potrebbe essere "sensore/1/temperatura".

Pit Stop

27 Che cos'è un gateway?

28 Che differenza c'è tra router e gateway?

29 Che cos'è MQTT?

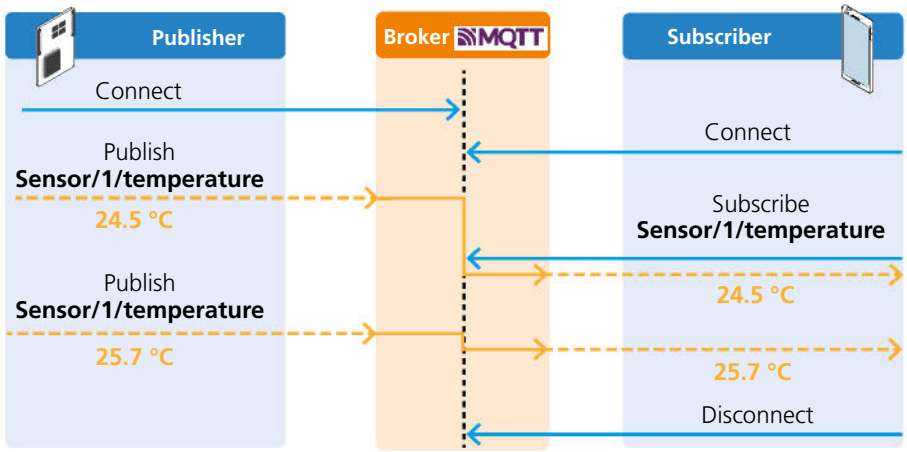


Fig. 16 Esempio di architettura MQTT publish-subscribe.

Nell'esempio mostrato nella **Figura 16**, un termostato intelligente (publisher) pubblica la temperatura. Un dispositivo (subscriber) si mette in ascolto per ricevere il valore della temperatura. Il dispositivo può essere semplicemente un'applicazione software che mostra i dati.

MQTT ha altre caratteristiche che lo rendono adatto per IoT, tra cui:

- **Qualità del servizio** (**QoS**): offre tre livelli di QoS per garantire la consegna dei messaggi.
  - **QoS 0**: il messaggio viene inviato una volta senza alcuna garanzia di consegna.
  - **QoS 1**: il mittente conserva il messaggio finché non riceve dal destinatario la conferma di avvenuta ricezione.
  - **QoS 2**: questa modalità è la più affidabile perché garantisce che ogni messaggio venga consegnato una sola volta. Il processo prevede un doppio rimbalzo tra mittente e destinatario:
    - il mittente invia un messaggio al destinatario (broker);
    - il broker conferma il messaggio;
    - il mittente, ormai sicuro che il messaggio è stato ricevuto, lo segnala al broker e lo estrae dalla sua coda di invio;
    - il broker conferma il messaggio.
- **Persistenza dei messaggi**: il broker MQTT conserva i messaggi fino a quando non sono consegnati a tutti i dispositivi (subscribers). In questo modo il broker si assicura che nessun messaggio vada perso a causa di interruzioni temporanee.
- **Messaggi di testamento** (Will): sono inviati dal broker MQTT come notifica a tutti i dispositivi quando uno di essi si disconnette.

La **sicurezza** riveste un elemento importante nei sistemi IoT. È perciò necessario adottare alcune misure precauzionali con i dispositivi che utilizzano MQTT:

- **Autenticazione e Autorizzazione**: i dispositivi che richiedono l'accesso al broker MQTT devono utilizzare username, password e certificati per autenticarsi e verificare l'autenticità del broker.
- **Trasporto Sicuro** (**TLS/SSL**); la comunicazione tra i dispositivi e il broker utilizza TLS/SSL.
- **Topic**: i permessi di lettura e scrittura dei topic vanno limitati e controllati.

Pit Stop

30 Quando conviene usare MQTT?

- **Firewall**: l'accesso al broker MQTT va riservato solo ai dispositivi autorizzati.
- **Segmentazione di Rete**: la rete IoT va isolata dalle altre reti.
- L'attività dei broker va **monitorata**.
- L'**aggiornamento dei dispositivi** va fatto in modo costante.

12 Reti mobili 5G

Il **5G** rappresenta la quinta generazione della tecnologia cellulare nell'ambito della telefonia mobile (Figura 17). Si basa sull'insieme di tecnologie e standard definiti dall'ente di standardizzazione **3GPP**. 5G permette l'ottimizzazione nell'uso delle risorse grazie ad alcune tecniche innovative:

- L'utilizzo di numerose antenne (Figura 18) che coprono aree di territorio di ridotta dimensione ("**small cells**").
- **La possibilità di dirigere** i segnali 5G in una direzione specifica verso un singolo dispositivo (Beamforming, Figura 19).
- La creazione di reti dedicate virtuali con funzionalità specifiche (**Network slicing**).

notabene

3GPP (*Third Generation Partnership Project*) è un ente, originariamente creato da IBM e ora supportato dal consorzio OASIS, che produce standard per le telecomunicazioni cellulari come LTE (4G) e 5G.

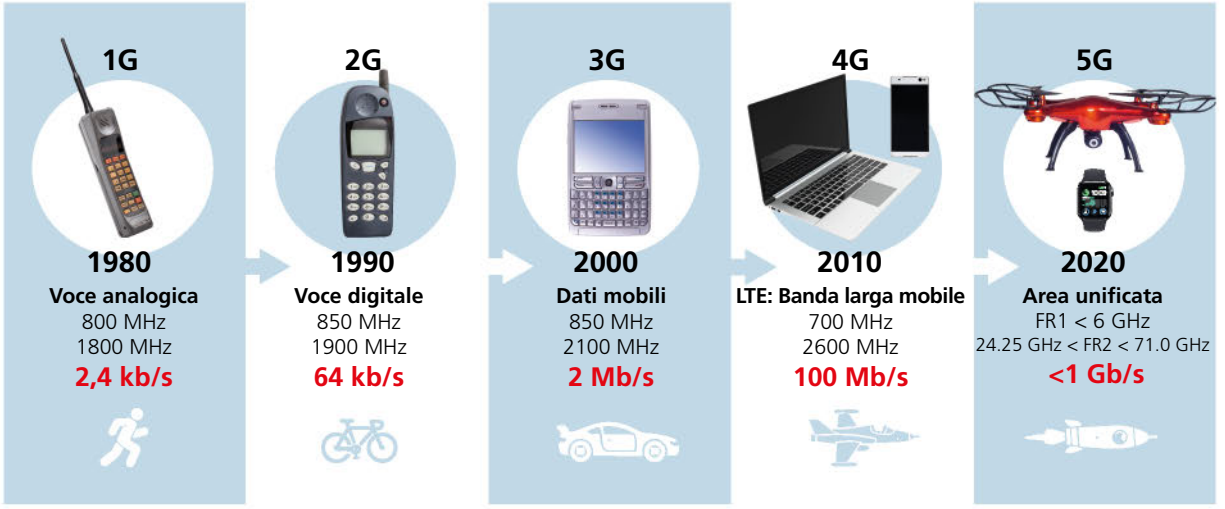


Fig. 17 Confronto tra generazioni per le trasmissioni cellulari: anno di introduzione, utilizzo, banda di frequenza indicativa. velocità (bit/s) e relativa analogia con le velocità dei mezzi di trasporto nella vita quotidiana.

Le bande di frequenza per il 5G New Radio (**5G NR**) sono suddivise in due gruppi principali:

- **Frequency Range 1** (**FR1**), che utilizza bande di frequenza inferiori a 6 GHz, con una copertura che va da alcune centinaia di metri a diversi chilometri.
- **Frequency Range 2** (**FR2**) ,che utilizza bande di frequenza che vanno da 24,25 GHz a 71,0 GHz. Queste bande consentono trasmissioni veloci, ma hanno una portata limitata, che va da alcune decine di metri a qualche centinaio di metri.

notabene

Il 4G necessita di grandi torri cellulari ad alta potenza, mentre il 5G utilizza un gran numero di piccole stazioni cellulari, perché le frequenze delle onde radio usate possono viaggiare solo su brevi distanze e sono sensibili alle interferenze.



Fig. 18 Torre con antenne 5G.

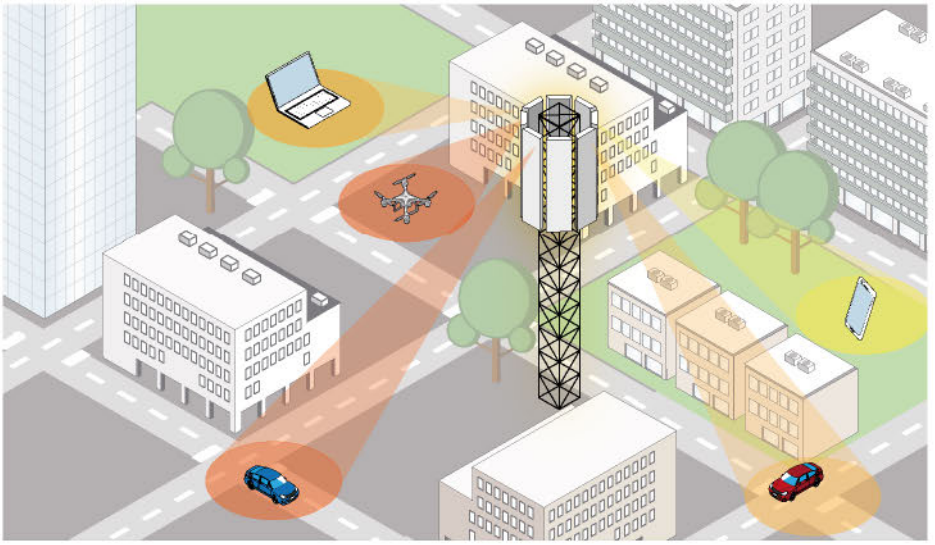


Fig. 19 Il beamforming del 5G indirizza il fascio di onde radio emesso dalla stazione base verso il dispositivo dell'utente. Il numero di connessioni può arrivare al milione per km².

A titolo di confronto, il Wi-Fi utilizza bande di frequenza intorno ai 2,4 GHz, con una portata di circa 100 metri, e ai 5 GHz, con una portata di circa 50 metri. Per le sue caratteristiche, il 5G si configura come il "sistema nervoso della società digitale", progettato per collegare virtualmente tutti e tutto, inclusi macchine, oggetti e dispositivi. In particolare, grazie al basso tempo di latenza (1 ms) e al numero di pacchetti persi (1 su 100 milioni), è fondamentale per la **gestione delle applicazioni critiche**, come la guida autonoma, la telemedicina e la chirurgia a distanza.

Le reti di dati basate su telefonia cellulare costituiscono un'ottima soluzione per IoT (Figura 20) in quanto sono erogabili solo da operatori mobili e sfruttano frequenze licenziate, con il vantaggio di evitare interferenze di terzi.

Pit Stop

31 Cosa sono 4G e 5G?

32 Quando conviene usare tecnologia 4G e 5G?

33 Che differenza c'è tra 4G e 5G?

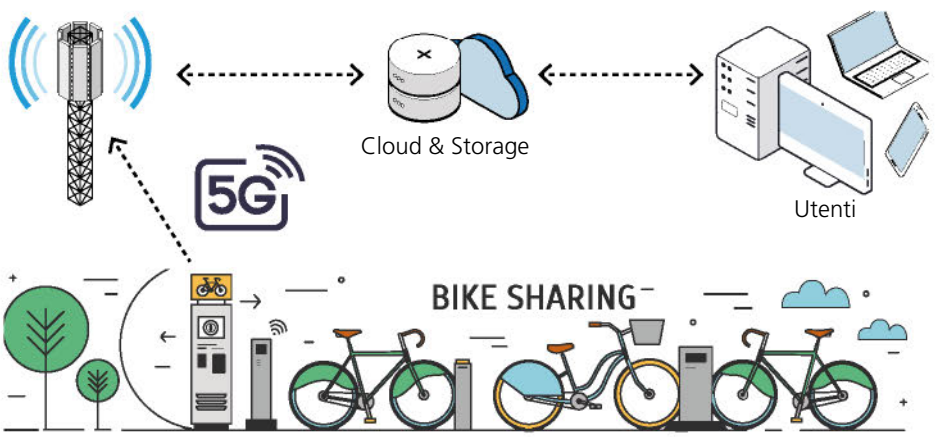


Fig. 20 Un esempio applicativo con 4G/5G.

Approfondimento - Tecnologia 1

L'attacco KRACK e il passaggio a WPA3

Nel 2017, un gruppo di ricercatori ha scoperto una vulnerabilità nel protocollo di sicurezza WPA2, ampiamente utilizzato per proteggere le reti Wi-Fi. Questo protocollo si basa su un sistema di autenticazione a chiave pre-condivisa (PSK). Tuttavia, durante l'handshake iniziale (4-way handshake) tra un dispositivo client e un Access Point, è emersa una falla che poteva essere sfruttata dagli attaccanti.
L'attacco Key Reinstallation Attacks (KRACK) mirava proprio a questa fase di handshake. L'attaccante si inseriva tra il dispositivo client e l'Access Point utilizzando una tecnica di "man in the middle". Sfruttando una vulnerabilità nell'implementazione dei protocolli di cifratura, l'attaccante riusciva a sostituire la chiave di cifratura dell'utente con una chiave molto più semplice, costituita da una stringa di zeri. Questo consentiva all'hacker di decifrare facilmente i dati in transito, anche se il sito web utilizzava HTTPS (**Figura 1**).
Anche la copertura di SSL/TLS, utilizzata per proteggere le comunicazioni tra il browser e i server Web, poteva essere bypassata tramite una tecnica chiamata SSLstrip. In questo caso, l'attaccante costringeva il browser a comunicare con server non controllati, consentendo l'intercettazione e la manipolazione del traffico tra l'utente e il sito Web, anche se quest'ultimo era protetto da HTTPS.
L'attacco KRACK ha evidenziato la necessità di migliorare la sicurezza delle reti Wi-Fi. Per affrontare queste vulnerabilità, è stato introdotto WPA3 che, tra le sue caratteristiche, possiede la modalità PMF (*Protected Management Frames*) che assicura che i messaggi scambiati tra dispositivi e Access Point provengano da fonti legittime.

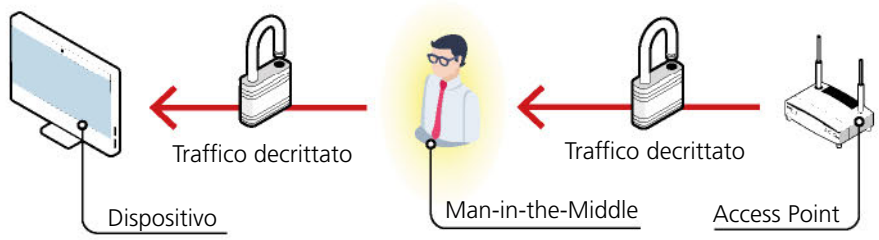


Fig. 1 La reinstallazione della chiave consente agli aggressori di intercettare e decifrare i dati trasmessi tra il dispositivo e l'AP.

Approfondimento - Tecnologia 2

Il protocollo RADIUS

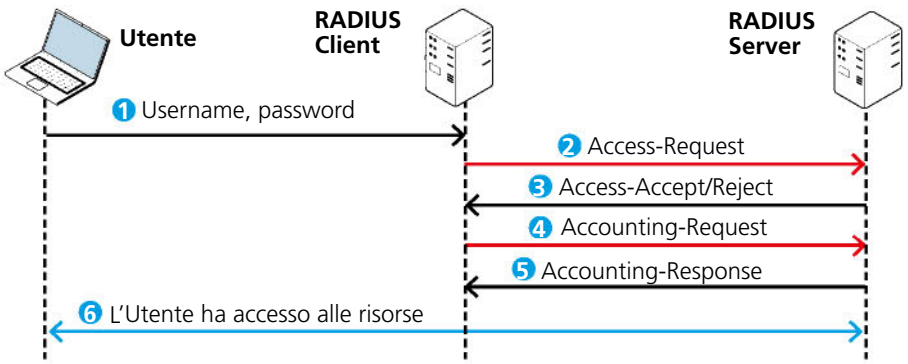
Il protocollo RADIUS (Remote Authentication Dial-in User Service, RFC 2866) ha lo scopo di fornire servizi di autenticazione, autorizzazione e accounting per la comunicazione client-server. Il suo funzionamento è mostrato nella **Figura 2**.

1. L'**accesso a un server RADIUS** da parte di un dispositivo (ad esempio, un PC) avviene tramite un **server NAS** (*Network Access Server*) che agisce da intermediario tra il client e il server RADIUS.

Il server NAS, identificato come RADIUS client, è il dispositivo a cui si connettono gli utenti remoti. Esso interroga il server RADIUS per lo stato di autenticazione, i profili utente e le autorizzazioni.

2. Quando il server NAS riceve le richieste di autenticazione dal dispositivo, come login e password, le comunica al server RADIUS per la verifica (**Access-Request**).
3. Se le credenziali sono valide, il server NAS riceve un messaggio di **Access-Accept** dal server RADIUS. In caso contrario, il server RADIUS invia un messaggio di Access-Reject, negando l'accesso.
4. Se l'accesso è consentito, il client RADIUS invia un pacchetto di richiesta di avvio (**Accounting-Request**) al server RADIUS.
5. Il server RADIUS restituisce il messaggio di conferma (**Accounting-Response**)
6. L'utente accede alle risorse di rete.

I messaggi del protocollo RADIUS utilizzano la porta UDP 1812 per l'autenticazione e la porta UDP 1813 per l'accounting.
Un **Network Access Server** (**NAS**) è un server specializzato che offre dei servizi per il controllo dei dispositivi che si collegano a una rete, come limitare l'accesso a un dispositivo o a una rete, autenticare le credenziali di un client appoggiandosi a un altro dispositivo che sa come gestire le credenziali



→ **Fig. 2** Accesso alle risorse di rete tramite l'autenticazione di un server RADIUS, passando da un server NAS.

Approfondimento - Tecnologia 3

Indirizzi IP per sistemi mobili

Quando utilizziamo un dispositivo mobile, come un telefono cellulare, per collegarsi a Internet si presentano due scenari.

- **Un dispositivo mobile si connette alla rete Wifi** di una LAN, come quella di casa o dell'ufficio. In questo caso riceve **un indirizzo IP privato** assegnato dinamicamente dal router tramite il server DHCP. Quando il dispositivo si collega ad Internet, utilizza l'indirizzo IP pubblico del router, condiviso da tutti i dispositivi connessi alla stessa rete Wi-Fi, e assegnato dal provider di servizi Internet.

- **Il dispositivo mobile si disconnette dalla rete Wi-Fi** e passa alla connessione dati mobili, come 4G o 5G. In questo caso gli viene assegnato un nuovo indirizzo IP pubblico dal provider di servizi Internet mobile. Questo indirizzo IP può essere dinamico e cambiare ad ogni connessione. Il servizio DHCP del provider gestisce l'assegnazione dinamica degli indirizzi IP ai dispositivi collegati. Inoltre, il provider potrebbe utilizzare la tecnica del NAT per condividere lo stesso indirizzo IP tra diversi utenti.

Approfondimento - Salute

L'esposizione delle persone ai campi elettromagnetici

L'esposizione delle persone e dell'ambiente ai campi elettromagnetici è un argomento importante e delicato. In particolare il 5G, che opera nella banda di spettro delle microonde da 3 GHz a 300 GHz, ha sollevato preoccupazioni riguardo ai potenziali danni che potrebbe causare. Secondo il documento *Statement on emerging health and environmental issues* – 2018 del Comitato Scientifico sui Rischi Sanitari Ambientali ed Emergenti (SCHEER) della Commissione Europea, «l'esposizione ai campi elettromagnetici [delle reti 5G] che potrebbe influenzare l'uomo rimane un'area controversa e gli studi non hanno prodotto prove chiare dell'impatto su mammiferi, uccelli o insetti. La mancanza di prove chiare per informare lo sviluppo di linee guida sull'esposizione della tecnologia 5G lascia aperta la possibilità di conseguenze biologiche impreviste».
Tuttavia occorre considerare alcuni fattori importanti:

1. **Fonti di esposizione alle onde elettromagnetiche**:
   - **sorgenti fisse ambientali**: antenne radio-TV, stazioni radio base per la telefonia cellulare e impianti WiFi. Queste sorgenti generano un livello di fondo di radiazione a RF su tutto il territorio.
   - **Apparati ad uso personale**: telefoni cellulari, laptop e altri dispositivi wireless. Le onde elettromagnetiche da queste sorgenti sono di bassa intensità.
   - **Sorgenti domestiche o d'uso comune**: forni a microonde, antifurti, telepass e telecomandi. Queste sorgenti emettono campi a radiofrequenza di breve durata e non comportano significativi livelli di esposizione.
2. **Caratteristiche Importanti**:
   - la penetrazione delle onde millimetriche utilizzate nel 5G è limitata dagli edifici.
   - La profondità di penetrazione nel corpo umano varia con la frequenza. All'aumentare della frequenza si riduce la profondità di penetrazione del campo elettromagnetico nel corpo umano (circa 10 cm per le frequenze radiofoniche e 1-5 cm per la telefonia mobile e il WiFi) e, di conseguenza, l'assorbimento di energia interesserà solo i tessuti superficiali.
   - I campi elettromagnetici del 5G non sono radiazioni ionizzanti e non interagiscono direttamente con il DNA e non causano mutazioni che favoriscono i tumori.
   - **Temperatura Corporea**. L'intensità dei segnali del 5G non induce aumenti significativi della temperatura corporea.

notabene

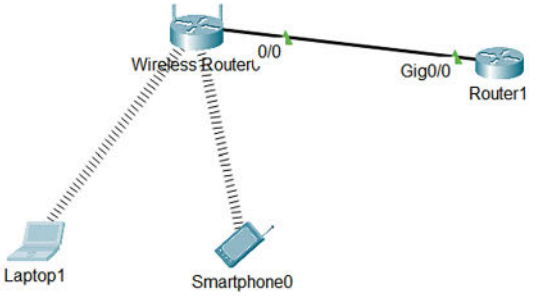
Per ulteriori approfondimenti si faccia riferimento al documento emesso dall'Istituto Superiore di Sanità "Radiazioni a radiofrequenze e tumori: sintesi delle evidenze scientifiche" del 2019.

Laboratorio

ATTIVITÀ 1
WLAN con WiFi e protocollo WPA2 Personal (PSK)

Scenario

Consideriamo la situazione di una semplice rete domestica, come rappresentato in figura, con un router wireless a cui sono collegati dei dispositivi, in questo caso un laptop e uno smartphone.
I dispositivi sono collegati al router domestico in modalità wireless e utilizzano il protocollo WiFi.



Consegna

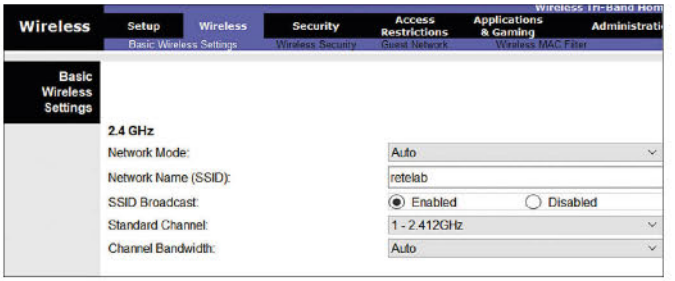
Utilizzare WPA2 per l'accesso sicuro alla rete e all'autenticazione del client, in modalità Personal con chiave pre-condivisa (WPA2-PSK) .

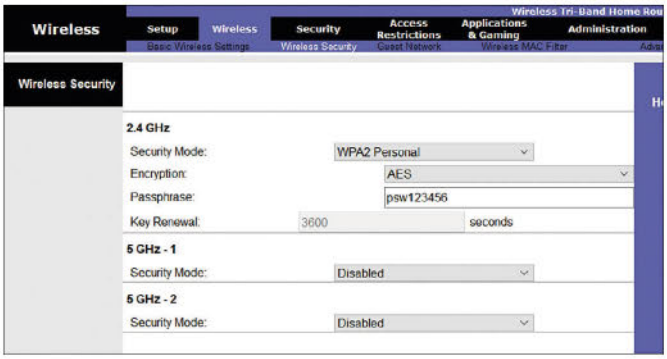
Svolgimento

Passo 1: progettazione della rete
Predisporre i dispositivi come nella figura.

Passo 2: configurazione router

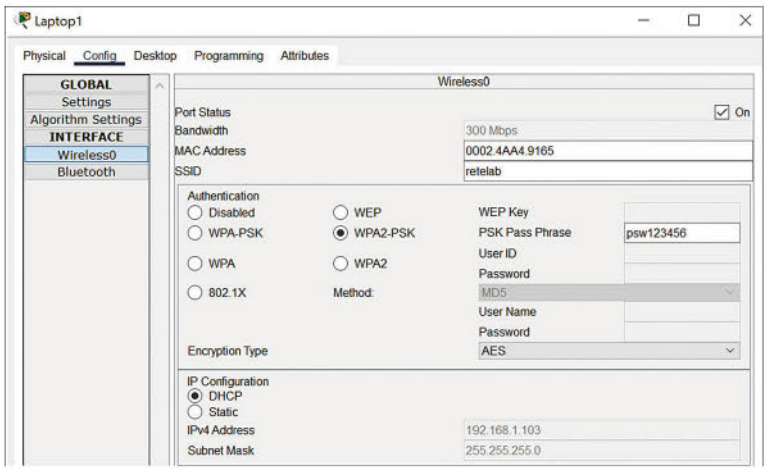
- Assegnare al router indirizzo 192.168.1.1 lato LAN e indirizzo 200.1.15.1 lato Internet.
- Attivare il servizio DHCP per i dispositivi della LAN.
- Selezionare la modalità GUI, Wireless e assegnare come SSID il nome "retelab".
- Selezionare Wireless Security e impostare WPA2 Personal, crittografia AES, password: psw123456. È questa la chiave pre-condivisa che dovrà essere usata da tutti i dispositivi che vogliono collegarsi alla rete.





Passo 3: configurazione dei dispositivi

Configurare ora i dispositivi impostando i parametri come nella figura. A titolo di esempio mostriamo la configurazione del laptop.



Osserviamo che il collegamento è avvenuto con successo.

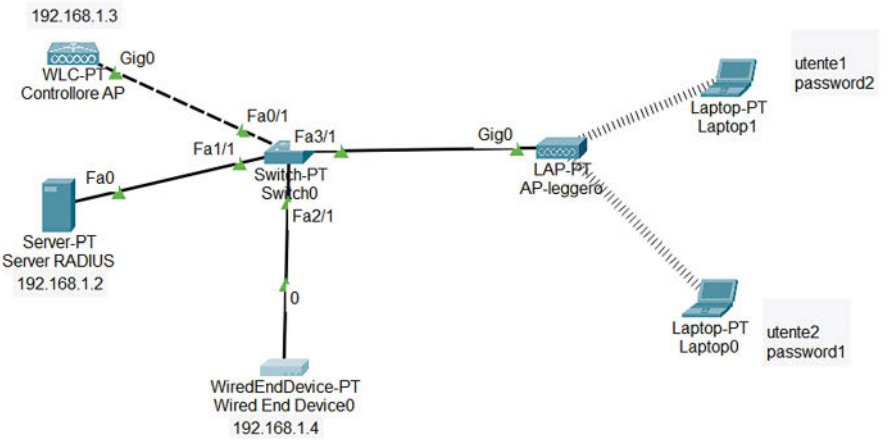
Proviamo ora a inserire una password errata o una SSID errata in uno dei dispositivi e osserviamo che il collegamento non si attiva. Infatti, WPA2 PSK (Personal) per l'autenticazione utilizza SSID e password.

ATTIVITÀ 2

WLAN con WiFi e protocollo WPA2 Enterprise con WLC

Scenario

Consideriamo una rete aziendale, più complessa di quella dell'attività precedente, che necessita di identificazione e autenticazione degli utenti che vogliono collegarsi a una delle reti wireless aziendali.
La situazione è rappresentata nella figura seguente.



Per consentire l'identificazione e l'autenticazione tramite userid e password di un utente, utilizziamo un server di autenticazione (AAA) RADIUS.
In una rete di una azienda (ma anche di una scuola!) che ha necessità di coprire una vasta area con rete WiFi, potrebbero essere necessari tanti Access Point e potrebbero essere definite varie SSID, con la relativa complessità di gestione.
Per questo motivo introduciamo un ulteriore apparato di rete, un **WLC** (**W***ireless* **L***AN* **C***ontroller*), che si occupa della gestione di tutti gli Access Point e delle reti WiFi collegate. In questo modo si possono usare Access Point "stupidi", chiamati "leggeri", che hanno particolari configurazioni e dipendono dal controller.

Consegna

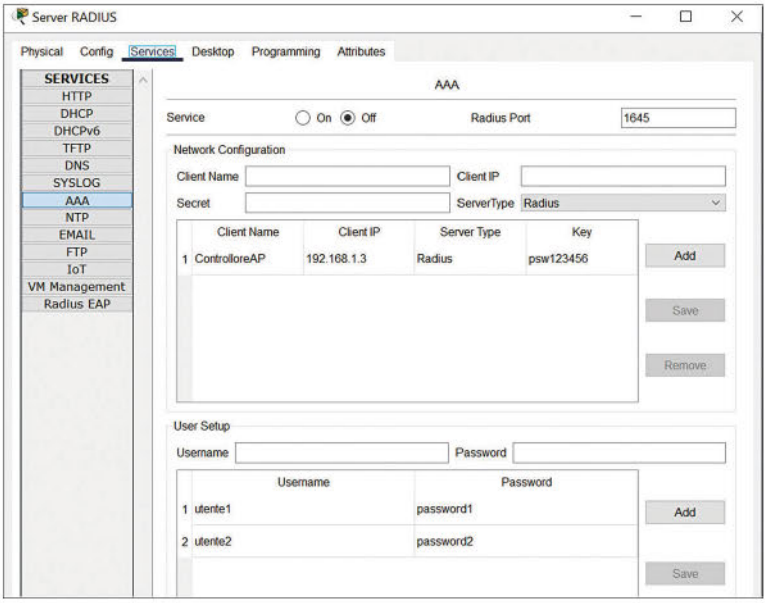
Utilizzare WPA2 per l'accesso sicuro alla rete e all'autenticazione del client, in modalità Enterprise con server RADIUS di autenticazione.

Svolgimento

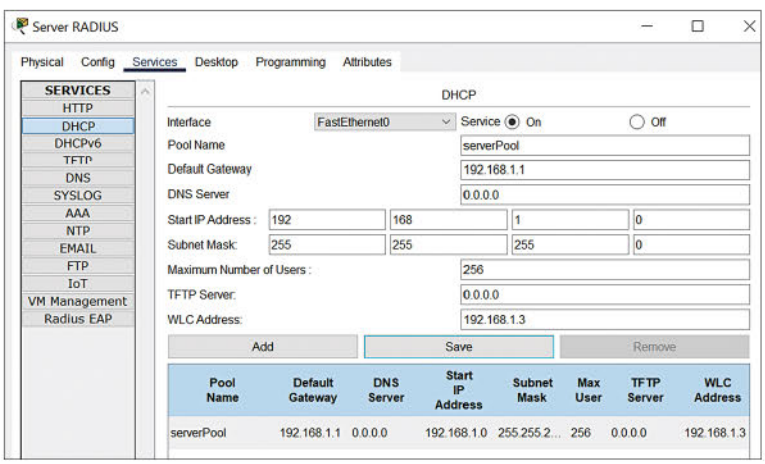
Passo 1: progettazione della rete
Predisporre i dispositivi come nella figura.

Passo 2: configurazione server RADIUS
Configurare il server RADIUS:
indirizzo IP statico: `192.168.1.2`
default gateway: `192.168.1.1`
Subnet Mask: `255.255.255.0`

Configurare il servizio AAA sul server RADIUS collegandolo al controller WLC, impostando una password condivisa (con il controller) e inserire due account (userid e password) da assegnare poi agli utenti.

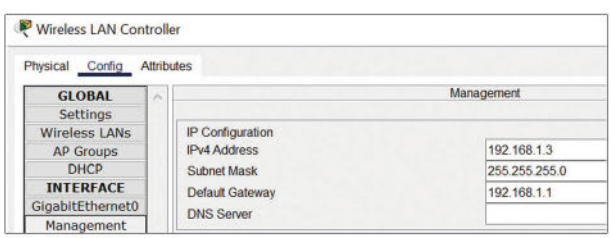


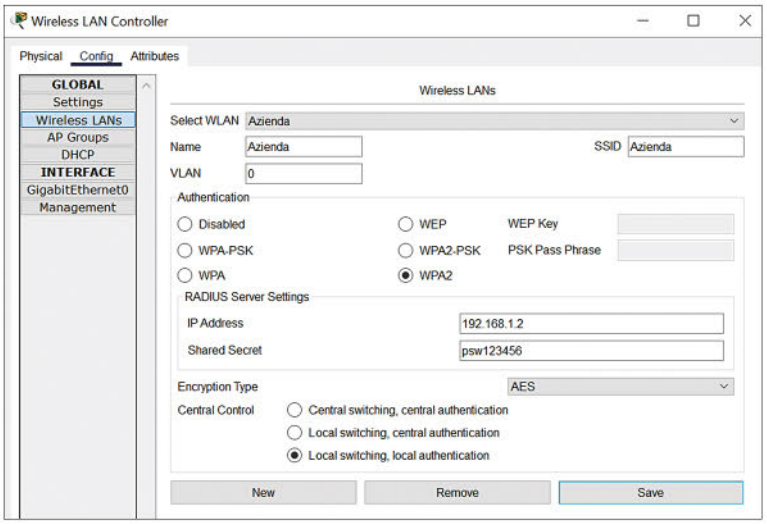
Abilitare e impostare il servizio DHCP.



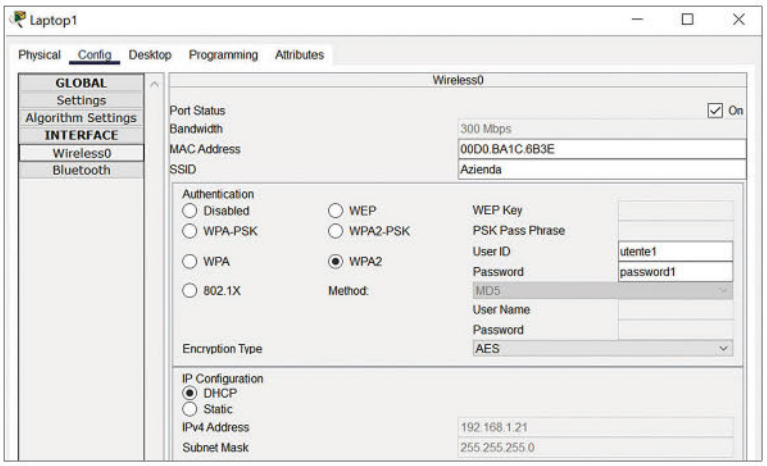
Passo 3: configurazione del controllore degli Access Point

Configurare il controller assegnando un IP statico `192.168.1.3` e impostando la password pre-condivisa con il server RADIUS, come nella figura.





Passo 4: configurazione dei dispositivi utente
A titolo di esempio, configuriamo laptop1 utilizzato da `utente1`, come nella figura.



Passo 5: verifica del funzionamento
Osserviamo che i laptop sono collegati alla rete (graficamente si vede il simbolo del segnale wireless) e testiamo il funzionamento facendo un ping da laptop1 a un generico dispositivo di rete con `IP 192.168.1.4`.

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=27ms TTL=128
Reply from 192.168.1.4: bytes=32 time=31ms TTL=128
Reply from 192.168.1.4: bytes=32 time=6ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 31ms, Average = 17ms
```

SINTESI

RETI SENZA FILI (WIRELESS)
Utilizzano onde radio per trasmettere. Vantaggi: flessibilità e mobilità. Svantaggi: sicurezza. Si differenziano in base all'area di copertura, alla velocità di trasmissione e ai servizi offerti. Necessitano di autenticazione, integrità, riservatezza.

WPAN
Wireless Personal Area Network – area di copertura da pochi cm a 10 m.

BLUETOOTH IEEE 802.15.1
Per trasmissione dati a corto raggio. Usato nelle reti personali e nelle applicazioni IoT. Utilizza AES.

RFID-NFC
RFID: tecnologie a corto raggio (fino a pochi cm) per rilevare informazioni relative a un oggetto, persona, animale.

ZIGBEE IEEE 802.15.4
Per comunicazioni a bassa potenza e a corto raggio. Usato per domotica, misurazione dei consumi, gestione di distribuzione dell'energia.

WLAN
Wireless Local Area Network – area di copertura fino a 100 m.

WIFI IEEE 802.11X
Per reti locali. Ottima copertura in ambienti interni, alta velocità di trasmissione, consumo energetico elevato, costi elevati su larga scala. Non adatto per il settore industriale.

WPA2
Protocollo per la sicurezza reti WiFi. Garantisce autenticazione, riservatezza e integrità dei dati. Utilizza AES per la crittografia. Lavora in modalità Personal e Enterprise.

Personal
Il dispositivo e l'access point hanno una chiave (password) pre-condivisa (pre-shared).

Enterprise
Per autenticare l'utente è utilizzato un server RADIUS.

WPA3
Aumenta la sicurezza rispetto a WPA2 in fase di autenticazione.

WMAN
Wireless Metropolitan Area Network – area di copertura fino a circa 50 km.

WIMAX IEEE 802.16
Wireless a banda larga, usata per collegare reti locali a Internet. Utilizza antenne installate da un ISP.

WWAN
Wireless Wide Area Network – area di copertura nell'ordine delle decine di km.

RETI CELLULARI 4G-5G
A medio raggio fino ad una decina di km per collegamenti veloci a sistemi remoti e per IoT.

MQTT
Protocollo open source di livello Applicazione che opera sopra il livello Trasporto dello stack TCP/IP. Non richiede un protocollo specifico a livello di collegamento dati.

LORAWAN
A lungo raggio (dai 5 km ai 40 km) per la trasmissione su reti wireless a bassa potenza. Garantisce l'integrità e la riservatezza dei dati.

Verifica delle CONOSCENZE

Vero o Falso?

1 Per proteggere una rete wireless è possibile effettuare il filtraggio degli IP tramite l'Access Point. V F

2 WEP è usato per l'autenticazione nelle reti wireless. V F

3 EAP è usato per l'autenticazione. V F

4 Un server RADIUS è usato per l'autenticazione. V F

5 Una rete wireless è più vulnerabile di una rete cablata. V F

6 LoRaWAN è un protocollo wireless a corto raggio usato nelle PAN. V F

7 WPA2 in modalità standard utilizza una chiave pre-condivisa. V F

8 ZigBee garantisce l'autenticazione, la riservatezza e l'integrità dei dati. V F

9 Il server Radius è usato per l'autenticazione. V F

10 Nelle reti IoT gateway e router hanno le stesse funzioni. V F

11 WPA2 in modalità Enterprise ha una fase di autenticazione più complessa rispetto alla modalità Standard. V F

12 ZigBee è un protocollo usato nelle PAN. V F

13 ZigBee supporta la topologia a bus. V F

14 Bluetooth ha un'area di copertura fino a 1 km. V F

15 MQTT è un protocollo adatto alle WWAN. V F

16 5G utilizza un gran numero di piccole stazioni cellulari. V F

17 5G è adatto a IoT industriale e automazione. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

18 In una rete wireless:
- a possono essere usati algoritmi di cifratura la cui sicurezza dipende anche dalla lunghezza delle chiavi
- b la riservatezza dei dati non può mai essere garantita perché una wireless è vulnerabile
- c tutta la gestione della sicurezza è affidata all'Access Point
- d o si garantisce l'autenticazione o la segretezza

19 Un server RADIUS:
- a è usato per il backup dei dati
- b ha una funzione di proxy server
- c è usato per l'autenticazione degli utenti
- d controlla i flag ACK e SYN di un segmento TCP

20 Il protocollo WPA2 garantisce
- a riservatezza, integrità e autenticazione
- b riservatezza, integrità e, solo in modalità Enterprise, autenticazione
- c riservatezza, integrità e, solo in modalità Standard, autenticazione
- d autenticazione con un server RADIUS in modalità Standard

21 Il protocollo ZigBee
- a è usato per le trasmissioni a lungo raggio
- b è usato nella domotica
- c è particolarmente usato in telemetria
- d non garantisce la riservatezza dei dati

22 Il protocollo LoRaWAN
- a è una evoluzione di Bluetooth
- b utilizza celle telefoniche
- c è a lungo raggio e bassa potenza
- d non utilizza la crittografia

Domande per la prova orale

23 Quali sono i principali standard per la trasmissione wireless?

24 Come si possono classificare gli standard wireless in base all'area di copertura?

25 Come è realizzata la sicurezza dell'accesso a una rete WiFi?

26 Che differenza c'è tra "wireless" e "WiFi"?

27 Quali sono le principali caratteristiche di WEP, WPA2 e WPA3?

28 Che differenza c'è tra la modalità Personal e la modalità Enterprise di WPA2?

29 Qual è il ruolo di un server di autenticazione e quando si usa?

30 Quali sono le principali caratteristiche di ZigBee?

31 Quali sono le principali caratteristiche di LoRaWAN?

32 Quali sono le principali caratteristiche di MQTT?

33 Quali sono le principali caratteristiche di 5G?

34 Utilizzando Cisco Packet Tracer, progettare una rete domestica con i seguenti requisiti:
- utilizzo di un router domestico (wireless router);
- collegamento dei dispositivi (1 laptop, 1 desktop, 1 smart phone) tramite WiFi;
- autenticazione tramite protocollo WPA2 pre-shared.

35 Utilizzando Cisco Packet Tracer, progetta una rete domotica con i seguenti requisiti:
- utilizzo di un home gateway;
- collegamento dei dispositivi (1 laptop, 1 smart phone, 1 lampada intelligente) tramite WiFi;
- autenticazione tramite protocollo WPA2 pre-shared.

36 Fai una ricerca sul Web per recuperare informazioni relative alla tecnologia RFID e riporta i risultati in una tabella come di seguito:

Esempio di utilizzo	Dati da rilevare	Come programmare il tag
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....

37 Riporta in una tabella la differenza tra tecnologia NFC e Bluetooth.

38 Un'azienda vuole commercializzare sistemi per la gestione di una serra intelligente. La serra deve essere installata in un ambiente domestico. Degli appositi sensori rilevano dati relativi all'ambiente e li trasmettono ad un sistema centralizzato in cloud. In questo contesto definisci con uno schema grafico la rete e discuti i protocolli utilizzati.



Esercizi in più

Wireless networks

Abstract

Wireless networks are becoming increasingly widespread due to their flexibility and ease of use. In particular, they are increasingly used in the IoT sector, both for home automation and in business and industrial contexts. However, wireless networks are more vulnerable and subject to interference compared to wired networks, which is why wireless protocols must ensure client authentication, data confidentiality, and integrity. Wireless protocols are classified based on coverage area, transmission speed, and power consumption. A primary classification includes protocols for WPANs (RFID/NFC, Bluetooth, ZigBee), WLANs (WiFi), WMANs (WiMax), and WWANs (5G, LoRaWAN, MQTT). These protocols are widely used in IoT. In LAN networks that use WiFi, secure access must be ensured by using the WPA2 protocol, which guarantees data confidentiality, integrity, and client authentication. It operates in two modes that differ in how they perform authentication: Personal mode and Enterprise mode. The WPA3 protocol adds further security to the authentication phase.

Questions

Answer all questions

1 What is WPA2 used for?

2 When is it advisable to use the LoRaWAN protocol and why?

3 What are the characteristics of the 5G standard?

4 What are the most commonly used protocols in home automation?

Choose the correct answer

5 A RADIUS server
- a is used by WEP for data privacy in a wireless network
- b is used for authentication in a LAN
- c is a particular firewall
- d acts as an access point

6 Among the short-range wireless technologies are:
- a LoRaWAN
- b WiFi
- c RFID and Bluetooth
- d WiMax

7 MQTT
- a requires a specific data link layer protocol
- b is a Physical layer protocol
- c is an encryption algorithm
- d is an Application layer protocol

8 About home automation, the following is used:
- a the 4G protocol
- b the ZigBee protocol
- c the WiMax protocol
- d a RADIUS server

Crosswords

Across

2 Protocol used in home automation

4 Authentication server used by WPA2

6 Application-level WWAN protocol

7 Networks used for 5G

9 Very short-range technology

10 Protocol for WLAN

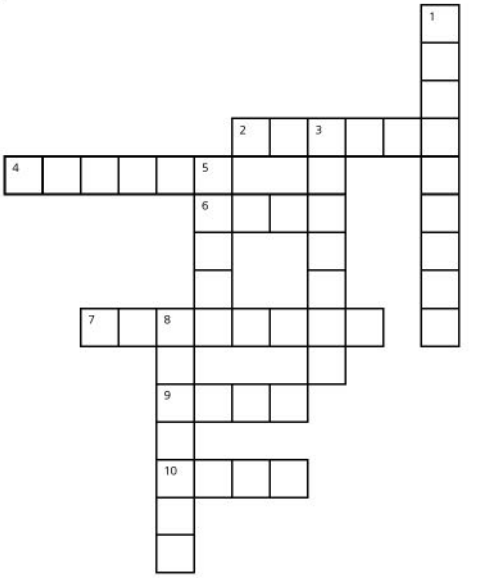
Down

1 Protocol for WPAN

3 IoT device similar to a router

5 This is how 5G cells are

8 WWAN protocol with sensors, gateways, network server, and application server



Verifica delle COMPETENZE

Tema 2

1 Esponi le soluzioni studiate per garantire la protezione di una rete locale aziendale, anche in presenza di server collegati a Internet.

2 Esponi le misure che devono essere attuate in ambito aziendale per garantire la sicurezza e la protezione dei dati trattati da un sistema informatico.

3 Quali sono le principali minacce per il Web?

4 Dopo aver detto che cos'è la crittografia, precisa quali problemi risolve e specifica la differenza tra crittografia a chiave privata e crittografia a chiave pubblica.

5 Descrivi, con l'aiuto di un disegno, il formato di IPsec Tunnel Mode (con ESP) e il modo con cui SSL imbusta i dati che provengono dal livello superiore e li invia al TCP.

IPSec Tunnel mode
SSL (imbustamento)

6 Dai la definizione di attacco APT e spiega sinteticamente i passi servendoti di un elenco puntato.

7 Alice vuole inviare segretamente a Bob il messaggio «I feel like I'm knockin' on heaven's door». Per Alice è molto importante che nessun altro legga il messaggio e che Bob possa essere sicuro che sia stata proprio lei a inviarlo. Decide, perciò, di usare la crittografia asimmetrica. Disegna uno schema, con la legenda relativa e il tipo di chiavi usate, che illustri il processo di spedizione del messaggio da parte di Alice e di quello di ricezione da parte di Bob.

8 Che cosa si intende per "caratteristica biometrica" e quali tra le seguenti non vengono usate per l'autenticazione dei soggetti?

- pianta del piede;
- iride dell'occhio;
- timbro della voce;
- forma dell'orecchio;
- impronta digitale;
- chimica della saliva;
- timbro della voce;
- immagine del volto.

9 Cita le caratteristiche fondamentali di una VPN e le tipologie principali. Fai un disegno che mostri un esempio di caso reale di un collegamento da casa ad azienda.

10 Bruno vuole procedere a un acquisto online di calzettoni da calcio tramite il sito di Anna. Il server di Anna può rispondere digitando sia `http://www.nomesito.com` sia `https://www.nomesito.com`. Descrivi sinteticamente le fasi che avvengono per i due protocolli.

HTTP
HTTPS

11 Esponi il significato di DMZ e disegna uno schema che rappresenta i componenti principali con le relative connessioni.

12 Completa la seguente tabella:

nome	Funzione, significato, caratteristiche principali
Buffer Overflow	
Backdoor	

13 Descrivi le tipologie di firewall esistenti.

14 Fornisci una panoramica sintetica delle tecniche di autenticazione degli utenti e spiega che cosa sono i "certificati" elettronici (chi li usa, chi li emette, la necessità del loro utilizzo).

15 Che cosa hanno in comune i protocolli SSL e PGP? Fai un confronto.

16 Cita (e spiega sinteticamente) almeno due attacchi per ogni livello: Fisico, Datalink, Rete e Trasporto.

---

17 Dopo aver esaminato l'episodio della divulgazione delle vulnerabilità "Meltdown" e "Spectre" del gennaio 2018, compila la tabella seguente.

Scenario incidente	IOC	Effetto e criticità	Modalità di attacco con analisi dettagliata della minaccia	Protezione e prevenzione	Fonti di riferimento e materiale
Data, Ente interessato, informazioni di base	Elenco indicatori della minaccia	Gravità, identità delle vittime, materiale sottratto, impedimento servizio...	Processo di analisi	Azioni correttive per eradicare il problema e fare in modo che non si presenti più in futuro	CVE …

18 Il vostro responsabile vi ha informato di una vulnerabilità (CVE-2014-0160) che impatta i server web con HTTPS. Dopo aver controllato il web server della vostra azienda, rilevate che esso sta utilizzando OpenSSL versione 1.0.1c. La ritenete un'informazione valida? Discutete come potete intervenire nel caso specifico.

19 Un progettista della vostra azienda si deve recare all'estero per una conferenza e vi chiede di utilizzare il PC portatile che utilizzerà in viaggio per poter accedere a informazioni riservate della vostra Intranet aziendale. Disegnate lo schema (con relativa spiegazione) che illustri il modo con cui il progettista accede al server aziendale dal proprio PC portatile.

20 "Incident Response LifeCycle" è un modello per la gestione degli incidenti informatici. L'analogia che segue applica il ciclo di vita agli eventi di previsione, prevenzione e lotta attiva agli incendi boschivi. Utilizzare l'analogia relativa alla difesa degli incendi per declinare i passi del modello Incident Response LifeCycle relativo alla sicurezza di un sistema informatico.

Difesa incendi	Sicurezza informatica ("Incident Response LifeCycle")
0. Prevenire incendi nel mio campo di mais	0. Prevenire gli attacchi informatici alla rete della mia scuola
1. Preparazione: compro un estintore e preparo vasche d'acqua piovana	1. .....
2. Rilevamento: segni di fuoco o fumo	2. .....
3. Risposta: utilizzo acqua ed estintori	3. .....
4. Mitigazione: il problema erano le sterpaglie. Le taglio	4. .....
5. Ripristino/Bonifica: faccio un muretto di contenimento	5. .....
6. Lezione appresa: non sottovalutare la pericolosità dell'erba secca in caso di incendio. Ne tengo conto per il futuro	6. .....

Orientamento al lavoro

ORIENTAMENTO STEM Tema 2

Sicurezza Informatica

Contesto

Il settore della sicurezza informatica, in tutti i suoi aspetti, di una multinazionale che opera nel campo aerospaziale e della difesa e che comprende clienti pubblici e privati sia nazionali sia esteri.

Intervista a

Andrea Minigozzi, che attualmente ricopre il ruolo di Team Leader della sezione Cyber Threat Intelligence dell'unità di di prevenzione e gestione degli incidenti di sicurezza informatica (CERT) di Leonardo S.p.A., azienda internazionale operante nei settori dell'aerospazio e della difesa. Approccia il mondo della sicurezza informatica nel 1999, alle porte del Millenium Bug, al quale riesce però a sopravvivere. Da allora ha avuto la fortuna di maturare esperienze in svariati ambiti della galassia Cyber Security.

Qual è il mercato oggi e qual è la previsione per i prossimi anni?

Il mercato della Cyber Security è sicuramente in forte espansione in tutti i settori, data la sempre crescente presenza di elementi vulnerabili ad attacchi informatici: basti pensare al mondo dell'Internet delle cose (IoT). Credo che nel prossimo futuro il trend sarà sempre positivo, anche grazie alla spinta delle nuove normative europee che dal 2018 impongono alle aziende una gestione più attenta e responsabile delle minacce informatiche (vedasi le direttive GDPR e NIS).

Qual è la figura professionale richiesta in quest'ambito?

La galassia della Cyber Security è costellata di figure professionali di diversa entratura, in quanto richiede competenze diverse in ambiti diversi. Ci sono figure estremamente tecniche in ambiti come Malware Analysis, Digital Forensics, Penetration Testing, Code Review ecc., così come profili meno tecnici in ambiti quali Analisi del Rischio, Audit, Resilience e altri prettamente manageriali come la Security Governance. Tutte queste persone concorrono alla sicurezza digitale dell'Azienda, andando a coprire tutte le fasi del ciclo PDCA (*Plan, Do, Check, Act*). I profili con alte competenze tecniche sono sicuramente quelli più ricercati, in quanto in grado di aggredire direttamente la minaccia cibernetica.

Che tipo di formazione deve avere questa figura professionale?

Nel mondo della sicurezza informatica credo che le competenze siano al secondo posto, perché sul gradino più alto del podio deve esserci l'attitudine. Se non si ha attitudine e "Lateral Thinking", le competenze tecniche non saranno mai espresse nel pieno del loro potenziale. Personalmente sono un Perito Informatico, che ha avuto la fortuna di vivere un periodo storico dove l'approccio alla sicurezza informatica stava nascendo e le community erano composte quasi esclusivamente da appassionati mossi da curiosità e tanta voglia di imparare. La vera spinta emotiva era la curiosità e quel modo diverso di approcciare il problema tecnico, di confrontarsi con altri senza fini commerciali o professionali ma "solo" per condividere conoscenze. Era passione pura.
Se a un candidato manca l'attitudine e la passione pura, potrà diventare un buon tecnico, ma sicuramente non un ottimo player nel mondo della Cyber Security. Detto questo, oggi esistono vari corsi di laurea e master che trattano temi inerenti alla Sicurezza Informatica fornendo solide basi agli studenti, così come diverse organizzazioni forniscono training e certificazioni specifici (per esempio SANS Institute, ISC2, Ec-Council, ecc.). Questi percorsi dovranno però essere sempre complementari alla curiosità e all'attitudine del singolo.

Ci racconti un po' la sua esperienza, la sua storia, il rapporto con colleghi.

Ho iniziato la mia attività in azienda nel 2000, come dipendente dell'allora Agusta S.p.A., operante nel settore elicotteristico a livello internazionale, e negli anni ho vissuto i profondi cambiamenti dell'azienda che, in diverse fasi, è diventata l'odierna Leonardo. Agli inizi della mia esperienza lavorativa i temi della Sicurezza Informatica erano appannaggio di pochi, e anche il mio ufficio era composto da sole due persone. Successivamente, negli anni, i cambiamenti dello scenario tecnologico, la diffusione dirompente di dispositivi sempre più pervasivi (i portatili prima, smartphone e tablet successivamente) e la crescente volatilità delle informazioni

hanno ampliato notevolmente la superficie d'attacco e i rischi associati alle attività Cyber. Con la nascita del CERT di Leonardo ho avuto la fortuna di confluire in un gruppo di persone con capacità tecniche eccezionali e tanta passione per quello che fanno. Trovarmi ogni giorno a operare in un contesto strategico ad alta tecnologia, con persone da cui c'è sempre da imparare e accomunate dalla mia stessa passione per la Cyber Security è un privilegio, una fortuna, un onore. La trasversalità è l'altra delle caratteristiche intrinseche della Cyber Security e lo deve essere anche delle persone che ci lavorano: devono interessarsi, anche fuori dall'ambito lavorativo, di altri temi, contaminarsi con altre discipline STEM (Science, Technology, Engineering, Mathematics) applicando il paradigma della Cyber Security ai più svariati campi come i "big data": io per esempio sono pilota di droni, un mio collega è un information designer, un altro è un maker appassionato di stampanti 3D, e tutti insieme creiamo delle singolari alchimie che, come ogni gruppo affiatato, rendono unico il CERT Leonardo.

Qual è stata la cosa più bella della sua esperienza lavorativa?

Uno dei momenti più belli è stata la nascita del CERT Leonardo, dove ho potuto rincontrare persone con le quali avevo già condiviso momenti "digitali" in passato, durante le ore spese in BBS prima e su Internet poi. Persone che, come me, da vere appassionate di sicurezza informatica (in un'epoca che potremmo definire l'alba della Cyber Security in Italia, sul finire degli anni Novanta) hanno avuto la fortuna di convertire la passione in lavoro: non esistevano università e i tanti esperti di oggi, eravamo dei pionieri. Non sono mancate le difficoltà: spesso non si era del tutto capiti, superare la sindrome del sottoscala e del garage, lo stereotipo che ci ha consegnato la filmografia di genere non aiutava in azienda. Sono uscito da quel cliché ponendomi in maniera diversa: dal ragazzo che porta solo brutte notizie e spende senza produrre nulla, da un centro di costo quindi, a un valore per l'azienda.

È contento del suo lavoro? Rifarebbe la stessa scelta?

Assolutamente sì. Credo che operare nel settore della Cyber Security in un contesto come quello di Leonardo sia motivo di orgoglio e soddisfazione, in grado di offrire sfide e scenari dove le competenze tecniche e le skill delle persone diventano fondamentali per il raggiungimento degli obiettivi.

Sfida finale

ORIENTAMENTO STEM

Tema 2

Fiutare i pacchetti SSH con Wireshark

Scenario

Siete i responsabili della sicurezza e volete controllare il collegamento tra un terminale remoto (nel nostro caso l'applicazione PuTTY in esecuzione su un PC con Sistema Operativo Windows) e un sistema Raspberry Pi presente in in rete locale.

Obiettivi

- **Scoprire l'indirizzo IP di un dispositivo collegato a una rete locale, utilizzando appositi tool.**
- **Intercettare i pacchetti che viaggiano in rete.**
- **Utilizzare il protocollo SSH.**
- **Verificare che i pacchetti sono criptati.**

Consegna

Utilizzare Wireshark per fiutare (*sniffing*) i pacchetti che vengono inviati dal vostro terminale a Raspberry Pi, assicurandovi che i dati siano crittografati e non interpretabili da terzi.

Traccia

Passo 1: scoprire l'indirizzo IP di Raspberry Pi

La prima cosa da fare è individuare l'indirizzo IP di Raspberry Pi presente nella vostra rete locale e verificare se ha la porta 22 (SSH – *Secure SHell*) aperta e disponibile (su Raspberry Pi deve essere stato abilitato il servizio SSH).

Il consiglio è quello di utilizzare il tool Zenmap (le Figure 1 e 2 forniscono un esempio come traccia).

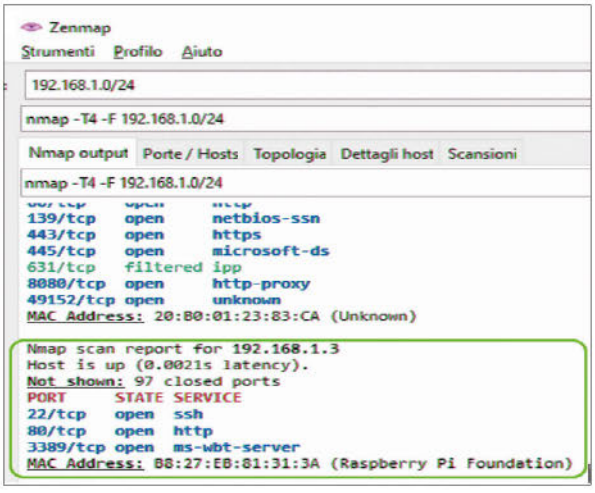


Fig. 1 È stato individuato l'indirizzo di Raspberry Pi con la porta 22 (SSH) aperta.

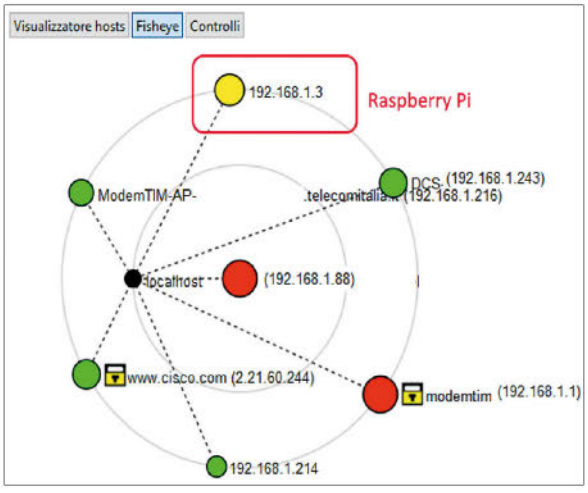


Fig. 2 La topologia della rete.

Passo 2: preparazione e cattura dei dati

- Far partire Wireshark (in modalità promiscua) filtrando i soli pacchetti SSH.

- Aprire una sessione PuTTY come in **Figura 3**.
- Entrare, da remoto, nel sistema Raspberry Pi con le credenziali e digitare il comando di visualizzazione dei file in cartella (**Figura 4**).

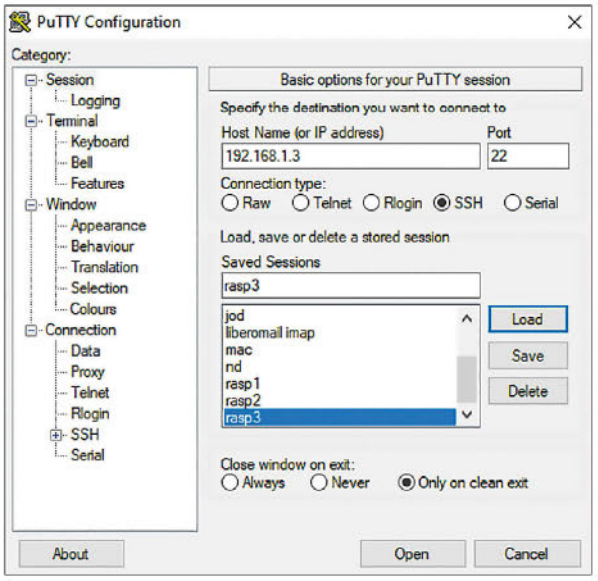


Fig. 3 La sessione SSH con PuTTY. SSH è un protocollo sicuro che sostituisce Telnet per accessi a un server remoto. SSH cripta la sessione di login, impedendo di accedere alla password, e può essere usato per cifrare (con codifica a 128 bit) i dati di protocolli non sicuri che, altrimenti, sarebbero mostrati in chiaro.

```
pi@raspberrypi ~ $
pi@raspberrypi ~ $ ls -l
total 60
drwxr-xr-x 2 pi pi  4096 Jun 22  2018 arm
drwxr-xr-x 5 pi pi  4096 Oct  4  2018 Desktop
drwx------ 2 pi pi  4096 Dec 29  2018 Downloads
-rw-r--r-- 1 pi pi 20480 Jul  1  2016 provaio.tar
drwxr-xr-x 2 pi pi  4096 Oct  4  2018 prove
-rw-r--r-- 1 pi pi 20480 Jul  1  2016 proveshell.tar
drwxrwxr-x 2 pi pi  4096 Jan  1  1970 python_games
pi@raspberrypi ~ $
```

Fig. 4 Il comando `ls -l`.

Passo 3: verifica dei pacchetti

Visualizzare i pacchetti su Wireshark e verificare che i dati sono crittografati (**Figura 5**).

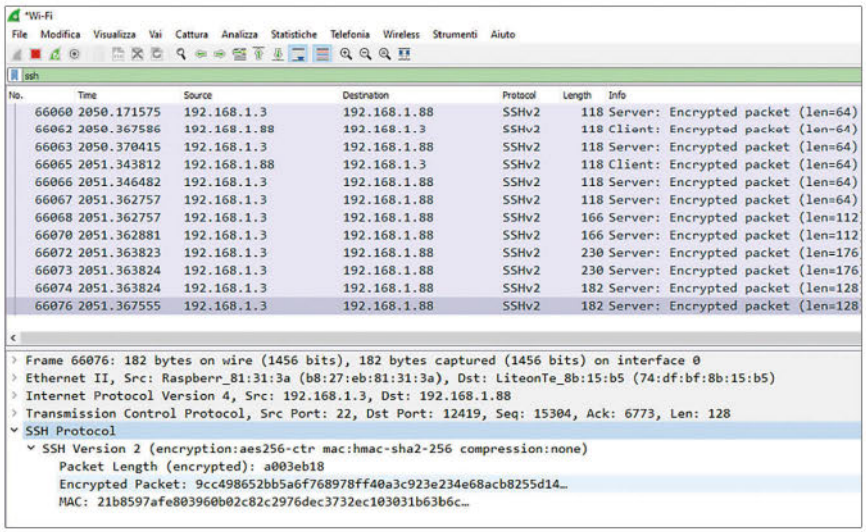


Fig. 5 Analisi di un pacchetto SSH inviato dal server (`192.1681.13`) come risposta al client.

Considerazione sull'analisi dei pacchetti di dati catturati

In ambiente Windows, la cattura dei dati non viene effettuata direttamente da Wireshark, ma dall'applicazione **Winpcap**; il traffico acquisito può essere salvato in un file con estensione `.pcap`. Si tratta di un formato compatibile con altre applicazioni in grado di analizzare i dati in un momento differito.
È possibile inoltre trovare in rete numerose librerie per Python, come Scapy o Pyshark, che, importate nel

programma, permettono di analizzare i dati di un file con estensione `.pcap` catturato con Wireshark. Ad esempio, consideriamo il programma seguente (`testpcap.py`) che importa la libreria `scapy` e la applica al file `test1ws.pcap` per mostrare i pacchetti SSH:

```
from scapy.all import rdpcap
# Carica il file .pcap
packets = rdpcap('test1ws.pcap')
# Filtra e mostra i pacchetti SSH (porta 22) (i primi due pacchetti)
for i, packet in enumerate(packets[:2]):
    if packet.haslayer('TCP') and packet['TCP'].dport == 22:
        print(f"Packet {i+1}:")
        packet.show()
        print("\n" + "............." + "\n")
    else:
        print("Non trovato pacchetto SSH\n  .............")
```

- `from scapy.all import rdpcap`: importa la funzione `rdpcap` dal modulo `scapy.all`, che serve per leggere `file .pcap`.
- `packet.haslayer('TCP')`: controlla se il pacchetto dati appartiene al livello trasporto (TCP).
- `packet['TCP'].dport == 22`: controlla se la porta di destinazione (`dport`) del pacchetto TCP è la 22, utilizzata per SSH.

notabene

Nella sezione online è presente un esempio di "sniffer" realizzato in linguaggio C che utilizza un raw socket (`sock_raw = socket(AF_INET, SOCK_RAW, IPPROTO_TCP)`) che riceve tutti i tipi di dati in entrata e li mostra a video.

File aggiuntivi
Codice completo pronto per l'esecuzione

Interroghiamo l'Intelligenza Artificiale

Tema 2

Tu e un tuo compagno o una tua compagna scegliete 5 domande dall'elenco.

Successivamente, lavorando individualmente, interrogate l'AI usando due chatbot diverse. Ciascuno conserva le schermate con le risposte e riassume le risposte ottenute. Infine, confrontate le risposte. Le chatbot hanno dato risposte analoghe? Oppure ci sono state differenze? Quando tu e il tuo compagno o la tua compagna avete riassunto le risposte della chatbot, avete considerato come importanti gli stessi concetti?

1. Cos'è la sicurezza informatica e quali sono i suoi obiettivi principali?
2. Quale sarà l'impatto dell'Intelligenza Artificiale nell'ambito della sicurezza informatica nel corso del prossimo anno?
3. Quali sono i principali tipi di minacce alla sicurezza di un sistema informatico?
4. Spiega l'importanza degli aggiornamenti software per la sicurezza.
5. Cos'è il social engineering e quali sono le sue implicazioni sulla sicurezza?
6. Qual è il ruolo della crittografia nella sicurezza informatica?
7. Spiega la differenza tra crittografia simmetrica e asimmetrica.
8. Confronta gli Algoritmi Crittografici Comuni come RSA, AES, 3DES , ECC. Quali offrono un livello di sicurezza superiore? In quale contesto?
9. Qual è il ruolo delle funzioni hash nella sicurezza informatica?
10. Spiega il concetto di Firma Digitale e come garantisce autenticità e integrità.
11. Cos'è una VPN e come garantisce la sicurezza delle comunicazioni?
12. Spiega la differenza tra un tunnel VPN e una connessione non protetta.
13. Come si distinguono i protocolli sicuri (ad esempio HTTPS, SSH) da quelli non sicuri (ad esempio HTTP, FTP)?
14. Spiega come il protocollo SSL è stato sostituito da TLS e perché.
15. Come funzionano i protocolli di autenticazione basati su chiavi (ad esempio RSA)?
16. Qual è il ruolo di un IDS (*Intrusion Detection System*) in un sistema di sicurezza?
17. Spiega la differenza tra IDS e IPS (*Intrusion Prevention System*).
18. Cos'è un SIEM (*Security Information and Event Management*) e a cosa serve?
19. Come può l'Intelligenza Artificiale migliorare il SIEM automatizzando l'analisi dei dati e identificando comportamenti anomali?
20. In che modo l'Intelligenza Artificiale può essere utilizzata per difendersi dallo spam o dalle fake news?
21. In che modo l'Intelligenza Artificiale può migliorare le capacità del SOC automatizzando la rilevazione delle minacce?
22. In che modo il concetto di DMZ (*Demilitarized Zone*) si è evoluto con l'avvento del Cloud?

Tema 3

Cloud Computing e IoT

Unità

8 I data center
9 Il Cloud Computing
10 IoT – Internet of Things

Prerequisiti

- Architettura di un sistema di elaborazione
- Architettura di un sistema operativo
- Architettura di rete
- Physical Computing

Conoscenze

- Reti geografiche
- Reti e protocolli di rete wireless
- I data center e la loro evoluzione
- Dal data center fisico al data center virtuale
- Soluzioni per la continuità del servizio
- Il Cloud Computing
- Container e microservizi
- IoT: architettura, ambiti di utilizzo, sicurezza

Abilità

- **Comprendere** i servizi offerti da un data center
- **Installare**, **configurare** e **gestire** reti in riferimento alla privacy, alla sicurezza e all'accesso ai servizi
- **Comprendere** i problemi legati alla continuità del servizio
- **Conoscere** i diversi protocolli di rete wireless

Competenze

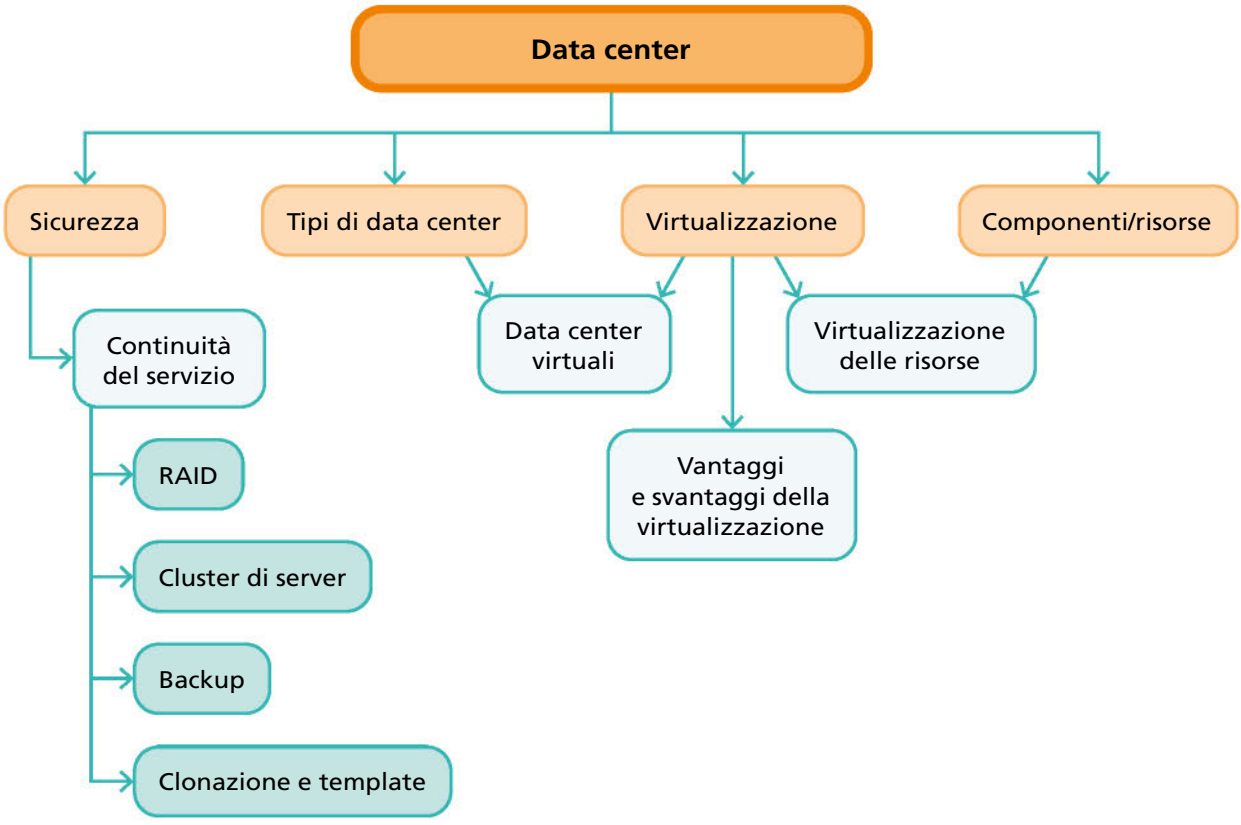
- **Scegliere** dispositivi e strumenti in base alle loro caratteristiche funzionali
- **Gestire** progetti secondo le procedure e gli standard previsti dai sistemi aziendali
- **Scegliere** la soluzione migliore relativamente alla distribuzione di risorse
- **Progettare** l'architettura di un sistema informatico scegliendo gli opportuni protocolli
- **Utilizzare** i servizi in Cloud Computing
- **Gestire** piccoli sistemi IoT con microcontrollori in locale e in Cloud



Unità

8

I data center



Visione d'insieme

- I data center.
- La virtualizzazione.
- Come garantire la continuità del servizio.

1 Introduzione

È il Black Friday, periodo più critico dell'anno per il commercio online. Il sito web di Centaurus, uno dei maggiori rivenditori online, è assediato da clienti ansiosi di approfittare delle offerte. Il data center che ospita il sito web è ormai al limite con i server che lavorano a pieno ritmo per far fronte all'enorme aumento del traffico.
Ma proprio quando sembra che il sistema stia per collassare, entra in gioco la virtualizzazione. In un batter d'occhio, il data center crea nuove istanze di server virtuali, distribuendo il carico di lavoro e prevenendo pericolosi sovraccarichi. Nel frattempo i clienti, ignari, non notano alcuna differenza: le pagine del sito web si caricano rapidamente e le transazioni vengono elaborate senza intoppi.
Tutto procede bene, ma improvvisamente accade l'irreparabile: uno dei server principali si arresta. Tuttavia, grazie alle funzioni di Fault Tolerance e al Disaster Recovery, il sito web rimane operativo. In pochi secondi, le funzioni del server in blocco sono trasferite a un altro server: la perdita di dati è sventata e i tempi di inattività sono ridotti al minimo indispensabile.
Grazie alla tecnologia avanzata del data center, il Black Friday è un successo!
I data center, che sono i luoghi in cui le aziende conservano e gestiscono tutte le loro informazioni digitali, un tempo erano visti principalmente come strumenti per migliorare la produzione. Ora la prospettiva è cambiata e sono diventati fondamentali e strategici nell'economia digitale, con un'attenzione particolare al cliente e ai suoi bisogni. Le strutture fisiche sono meno importanti rispetto alla gestione delle informazioni. Questo cambiamento ha portato i data center a dover fornire servizi veloci e affidabili, sfruttando le ultime innovazioni come la virtualizzazione e l'Intelligenza Artificiale.
In questa unità esploreremo l'evoluzione dei data center (dal mainframe al cloud) e le loro componenti principali (i server, lo storage e il network). Parleremo della virtualizzazione, di come ha rivoluzionato i data center, dei suoi vantaggi e delle problematiche. Discuteremo la continuità del servizio e gli elementi base per garantirla, come Fault Tolerance, Disaster Recovery, Business Continuity, RAID, la gestione di un cluster di server, le funzioni di migrazione, il backup e le repliche del data center virtuale.

2 I data center

Un data center (o Centro di Elaborazione Dati, CED) è lo spazio fisico che ospita le infrastrutture tecnologiche utilizzate da un'azienda per l'elaborazione, la memorizzazione e la condivisione delle informazioni. È il punto nevralgico dei sistemi IT (*Information Technology*) aziendali, necessari per il funzionamento dei processi aziendali informatizzati e integrati tra loro.
In un data center ci sono le risorse informatiche necessarie per:

- eseguire applicazioni web;
- eseguire le applicazioni aziendali interne per la contabilità, l'amministrazione, la gestione delle risorse umane, la gestione del magazzino, la pianificazione delle risorse aziendali (ERP - Enterprise Resource Planning) e per la gestione dei database;
- gestire la comunicazione interna ed esterna: desktop virtuali, servizi di comunicazione e collaborazione, e-mail, condivisione file, gestione dei rapporti con il cliente (CRM - Customer Relationship Management);
- supportare la business intelligence, i Big Data, l'Intelligenza Artificiale e l'apprendimento automatico.

Pit Stop

1 Che cos'è un data center?

Evoluzione dei data center: dal mainframe al cloud

I data center sono nati all'inizio degli anni Quaranta del secolo scorso (Figura 1). L'ENIAC (Electronic Numerical Integrator and Computer) fu uno dei primi calcolatori elettronici digitali, con una potenza di calcolo straordinaria per l'epoca (1946). Occupava una superficie di 180 metri quadrati e pesava 30 tonnellate. In quel periodo la gestione e la manutenzione dell'hardware dei computer erano complesse. I primi sistemi informatici richiedevano un gran numero di componenti di grandi dimensioni, collegate tra loro con un cablaggio complesso. Questi sistemi, chiamati **mainframe**, consumavano una grande quantità di elettricità e richiedevano sistemi di raffreddamento per evitare il surriscaldamento. Per gestire questi computer, le aziende posizionavano tutto l'hardware un unico locale chiamato **data center**.

Tra il 1950 e il 1960, i data center si presentavano ancora come ambienti incredibilmente complessi e primitivi, con decine di metri di cavi usati per collegare i dispositivi. Negli anni Settanta venne progettato il primo microprocessore Intel 4004, programmabile. Nel decennio seguente arrivarono i primi personal computer e, infine, negli anni Novanta del Novecento, gli utenti iniziarono a interfacciarsi con **Internet**, gettando le basi per i data center attuali.

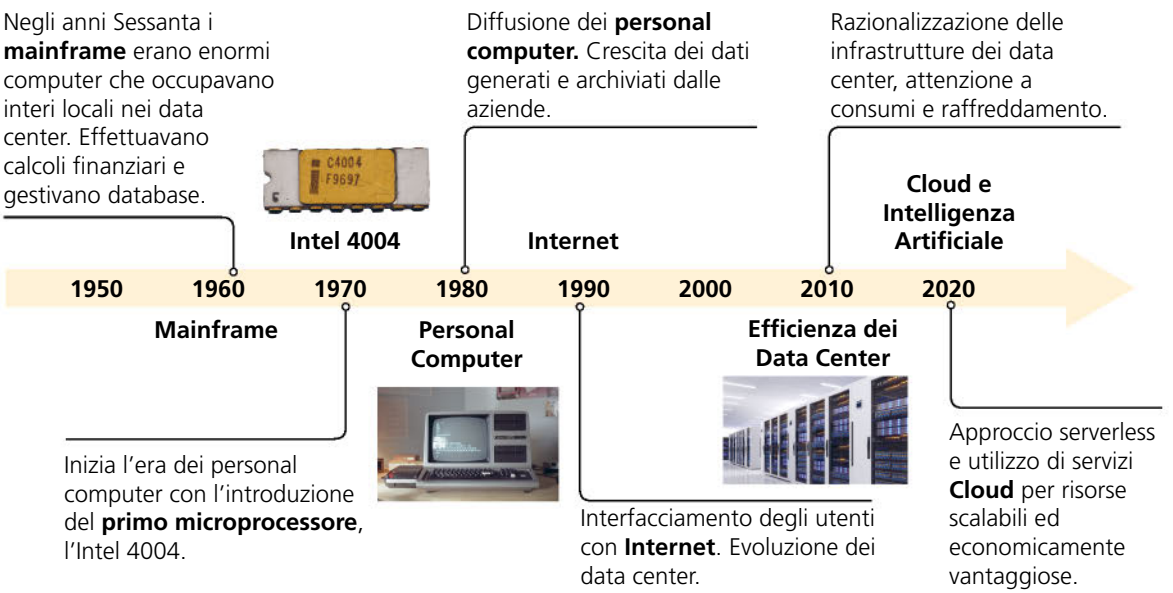
Nel corso del tempo, le innovazioni della tecnologia hardware hanno consentito di ridurre le dimensioni e i requisiti di potenza dei computer. Allo stesso tempo, tuttavia, i sistemi informatici sono diventati più complessi. Ad esempio:

- la quantità di dati generati e archiviati dalle aziende è aumentata in modo esponenziale.
- La tecnologia di **virtualizzazione** ha separato il software dall'hardware sottostante.
- Le innovazioni nel campo delle reti hanno reso possibile l'esecuzione di applicazioni su hardware remoto.

Pit Stop

2 Quali sono i passi fondamentali dell'evoluzione dei data center?

Fig. 1 La linea del tempo dell'evoluzione dei Data Center.



notabene

Il modello serverless consente agli sviluppatori di sviluppare le applicazioni senza gestire l'infrastruttura dei server necessari per l'esecuzione delle applicazioni.

Oggi la tendenza è quella di liberare il cliente da qualsiasi legame con l'hardware (approccio **serverless**) e di affidarsi a un fornitore di servizi in **cloud** che mascheri ogni problematica legata alle strutture fisiche. L'azienda si appoggia al cloud per ottenere le risorse necessarie a realizzare il sistema informativo aziendale, sotto forma di servizi software facili da richiedere, scalabili in funzione delle esigenze crescenti dell'azienda ed economicamente vantaggiosi, liberandosi, una volta per tutte, dalla costosa manutenzione dell'hardware. Il futuro prossimo appartiene al cloud computing e all'Intelligenza Artificiale.
Nei data center si stanno affermando progressivamente i seguenti modelli, che analizzeremo nella prossima unità dedicata al cloud computing:

- **as a Service** (**aaS**): offre servizi e risorse tramite Internet, consentendo agli utenti di accedere a funzionalità specifiche senza dover gestire l'infrastruttura sottostante.
- **On Demand**: prevede l'accesso immediato alle risorse quando necessario.
- **Pay Per Use**: consente agli utenti di pagare solo per le risorse effettivamente utilizzate.

Componenti principali di un data center

Le risorse informatiche di un data center si dividono in tre categorie (Figura 2):

- Calcolo e RAM (Compute).
- Memorie per l'archiviazione (Storage).
- Rete (Network).

La sicurezza del data center è fondamentale. Infatti questi componenti archiviano e gestiscono dati e applicazioni critiche (business-critical) che sono vitali per l'azienda e la loro interruzione potrebbe causare gravi danni.
Per supportare le componenti hardware e software, è necessaria un'infrastruttura "intelligente" che comprende (Figura 3):

- sottosistemi di alimentazione;
- gruppi di continuità (UPS - Uninterruptible Power Supply);
- generatori di riserva;
- sistemi di ventilazione e di raffreddamento;
- sistemi antincendio;
- sistemi di sicurezza degli edifici.

Infrastruttura di calcolo: i server

L'infrastruttura di calcolo comprende i dispositivi di calcolo veri e propri, cioè i computer dotati di CPU e memoria RAM per l'esecuzione del software. Questi computer sono i server e si distinguono dai computer degli utenti che hanno il ruolo di client.
Sui server fisici sono attivi software server, come HTTPD e altri, per la gestione delle applicazioni lato server.

Pit Stop

3 Quali sono le componenti fondamentali di un data center?

4 Quali sono le componenti di supporto di un data center?

5 Quali sono le principali applicazioni (servizi) in esecuzione sui server?



➜ **Fig. 2** Risorse di un Data Center.

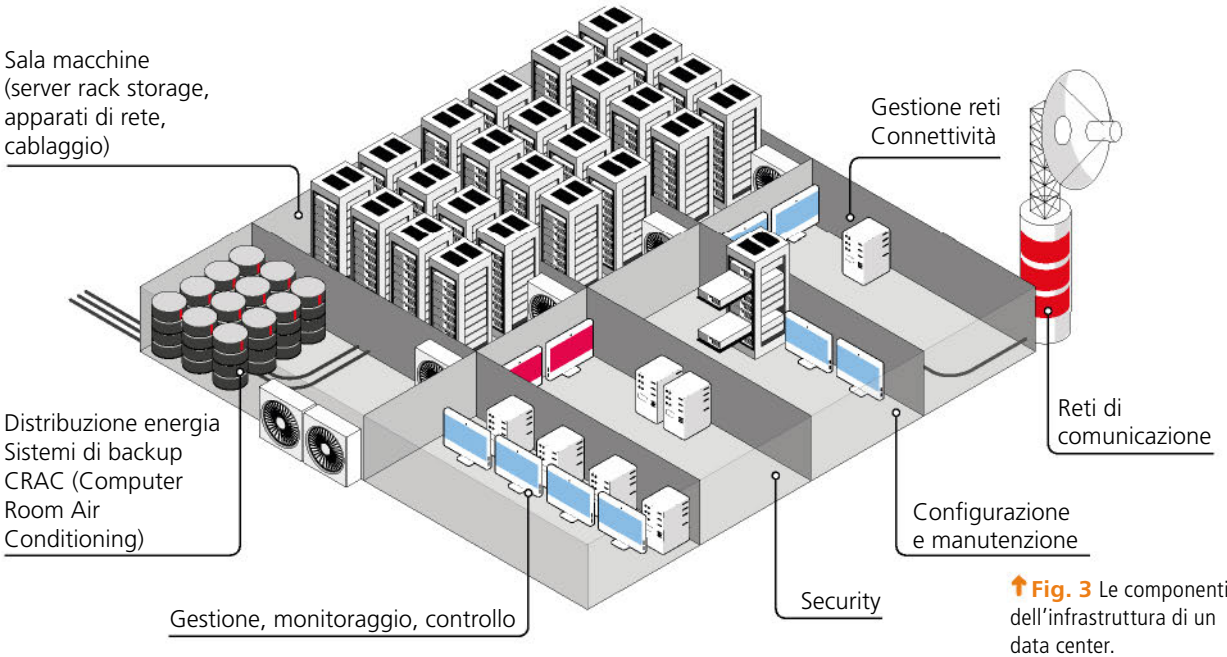


Fig. 3 Le componenti dell'infrastruttura di un data center.

La **Figura 4** descrive i tipi principali di server fisici, ognuno con caratteristiche specifiche, che li rendono adatti a diverse applicazioni e ambienti. Nella **Tabella 1**, invece, sono descritti i tipici servizi (applicazioni lato server) usati in una rete aziendale.



Tower Server
È un computer simile a un desktop dotato di un software specifico. È usato come server web, server DHCP, server DNS, o altro server di rete.



Rack Server
Hanno un design piatto e rettangolare e possono essere impilati in un armadio (rack). L'armadio possiede degli spazi per il passaggio dei cavi e alloggiamenti per le ventole di raffreddamento. Ogni server è un'unità indipendente con un proprio sistema di alimentazione, raffreddamento e connettività. I rack server sono utilizzati nei data center.



Blade Server
Sono compatti, modulari e scalabili. Privi di un sistema di alimentazione e raffreddamento indipendente, dipendono dal blade enclosure in cui sono installati e che fornisce le risorse hardware per il loro funzionamento. La loro flessibilità d'uso li rende adatti alla distribuzione dei carichi di lavoro, alla gestione dei dispositivi di rete e di storage, alle applicazioni business-critical e all'hosting di siti web. Sono dotati di hot-swap (cioè i componenti, come i dischi, possono essere rimossi e sostituiti senza dover spegnere il sistema) per ridurre efficacemente i tempi di inattività. Sono usati nei data center di grandi dimensioni.

Fig. 4 I principali tipi di server fisici.

notabene

In base al contesto occorre distinguere un server fisico (macchina fisica, hardware) da un'applicazione software lato server. Su un server fisico possono essere in esecuzione una o più applicazioni.

Pit Stop

6 Quali sono i principali tipi di server fisici?

La **Tabella 1** fornisce una sintesi dei server comunemente utilizzati in rete con i protocolli che specificano i servizi offerti.

Server	Servizi	Principali protocolli coinvolti
Web Server	Hosting e distribuzione di contenuti web (pagine HTML, filmati, ecc.) ai client, come i browser, attraverso demoni HTTP (HTTPD).	HTTP (*HyperText Transfer Protocol*) e HTTPS (*HTTP Secure*) che è la versione sicura di HTTP e che utilizza SSL/TLS per crittografare i dati trasmessi tra il server e il client.
Mail Server	Invio e ricezione di e-mail..	SMTP(S), IMAP/POP3, MAPI (*Messaging Application Programming Interface*), un protocollo che consente agli utenti di accedere alla propria cassetta postale utilizzando client di posta come Outlook.
FTP Server	Trasferimento di file (upload e download) tra client e server e gestione delle directory sul server.	FTP (*File Transfer Protocol*) e FTPS (*FTP Secure*) che aggiunge un livello di sicurezza utilizzando SSL/TLS.
DHCP Server	Assegnazione dinamica della configurazione di rete (indirizzi IP e subnet mask, default gateway, indirizzo server DNS) ai dispositivi in una rete.	DHCP (*Dynamic Host Configuration Protocol*).
Application Server	Esecuzione di diversi tipi di applicazioni lato server, tra cui le applicazioni web, la gestione delle sessioni utente, l'accesso ai database, l'autenticazione degli utenti.	L'interazione tra client e application server può avvenire tramite REST (*Representational State Transfer*).
AAA Server - RADIUS Server	Autenticazione, autorizzazione e accounting.	I server AAA possono utilizzare protocolli di autenticazione come SAML e OAuth per fornire il Single Sign-On (SSO), oltre al protocollo RADIUS.
DBMS Server	Gestisce database.	Utilizzano il linguaggio SQL per database relazionali e altre tecnologie per database non relazionali, come NoSQL.
DNS server	Traduce ("risolve") i nomi di dominio in indirizzi IP.	DNS (*Domain Name System*).
Active directory server	Gestisce un archivio centralizzato in un ambiente Windows, per le risorse di rete. Gestisce utenti, gruppi, dispositivi.	LDAP (Lightweight Directory Access Protocol) e Kerberos.
File Server	Fornisce spazio di archiviazione condiviso in rete. Un File Server può funzionare sia come NAS (*Network Attached Storage*) per piccole organizzazioni, sia come SAN (*Storage Area Network*) per data center o grandi organizzazioni.	SMB/CIFS (*Server Message Block/Common Internet File System*) e NFS (*Network File System*) sono protocolli che consentono agli utenti di accedere ai file su un server remoto come se fossero locali.
Proxy Server	Filtraggio e memorizzazione nella cache delle richieste web. Miglioramento della sicurezza e della privacy.	SOCKS (*Socket Secure*), un protocollo utilizzato dai proxy per instradare il traffico di rete tra il client e il server.
VPN Server	Crea connessioni sicure e criptate tra client e server.	I server VPN possono utilizzare vari protocolli per creare connessioni sicure. OpenVPN è un software che utilizza SSL/TLS. IPsec (*Internet Protocol Security*) è un protocollo che garantisce sicurezza a livello di rete ed è spesso utilizzato con L2TP (*Layer 2 Tunneling Protocol*). PPTP (Point-to-Point Tunneling Protocol) è uno dei protocolli VPN storici, ma è meno sicuro rispetto alle alternative più recenti.
Game Server	Coordinamento e gestione dei giochi e dei giocatori online.	
Print Server	Centralizzazione e gestione della stampa di documenti su una rete.	I print server utilizzano protocolli come SMB (*Server Message Block*), CIFS (*Common Internet File System*) e IPP (*Internet Printing Protocol*) per condividere da remoto file e stampanti.

Tab. 1 I server comunemente utilizzati in rete con i protocolli che specificano i servizi offerti.

Infrastruttura di archiviazione: lo storage



Fig. 5 La sostituzione di un disco in un array RAID in un SAN.

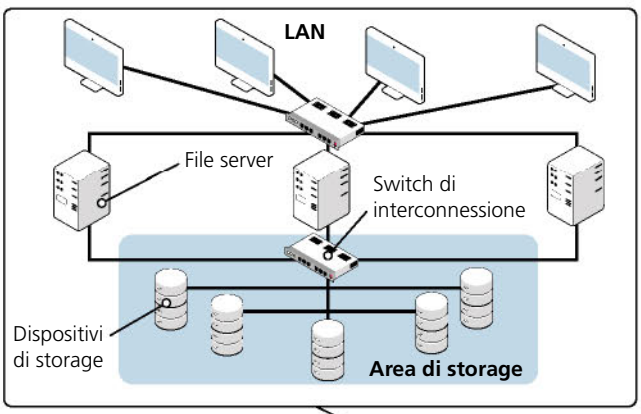
Lo storage è lo spazio di memoria di massa su cui archiviare i dati. Per lo storage sono utilizzati principalmente due sistemi:

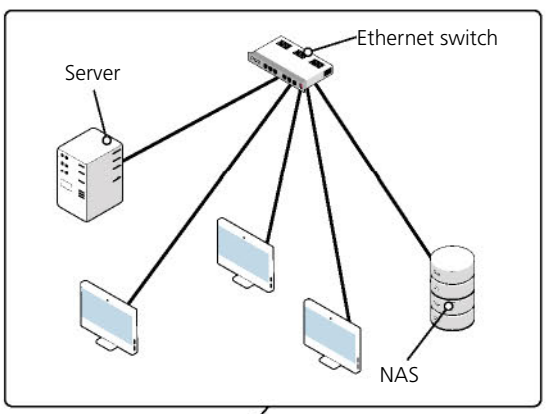
- Reti **SAN** (**Storage Area Network**). Una rete SAN è una rete ad alta velocità, **separata dalla LAN e collegata a essa tramite server dedicati**, che fornisce uno spazio di archiviazione condiviso a più computer e server. Consente scalabilità, elevata disponibilità e una gestione centralizzata dello storage con la possibilità di applicare un'unica policy per la sicurezza, la protezione dei dati e il disaster recovery. L'obiettivo di questa architettura è di spostare in rete il carico di lavoro per la gestione dello storage. Per garantire la sicurezza dei dati in termini di disponibilità, riservatezza e integrità, si utilizzano array di dischi (RAID, Figura 5). Le reti SAN usano una tecnica di archiviazione chiamata **archiviazione a blocchi**: I dati vengono suddivisi in segmenti e memorizzati in blocchi separati, ciascuno con un indirizzo univoco per migliorare la ricerca e velocizzare il loro recupero. Quando un'applicazione richiede i dati, i blocchi vengono recuperati, riassemblati e forniti all'utente o all'applicazione che ne ha fatto richiesta.
- **Dispositivi di Archiviazione di File**, come il **Network-Attached Storage** (**NAS**): possono archiviare un grande volume di file per la condivisione di file in una rete locale. Sono spesso utilizzati per memorizzare immagini e video. Questi sistemi sono veloci, sicuri e affidabili. Inoltre, i dispositivi NAS sono scalabili per soddisfare le crescenti esigenze di archiviazione. Forniscono servizi di archiviazione veloci, sicuri e affidabili a reti private (Figura 6).



Fig. 6 Un dispositivo NAS.

La Tabella 2 illustra le differenze tra i sistemi di storage di rete SAN e NAS.





Caratteristica	SAN	NAS
Rete	Rete dedicata di dischi fissi che appare come un disco unico.	Rete LAN.
Mezzo utilizzato	Utilizza la connettività Fibre Channel, una tecnologia di rete che utilizza la fibra ottica per trasferire dati ad alta velocità e in modo affidabile.	Si collega alla rete tramite una connessione Ethernet standard.
Modalità di trasferimento dati	Archivia i dati a livello di blocco, ideale per applicazioni che richiedono un accesso diretto ai dati, come i database.	Accede ai dati come file, più adatto per l'accesso a file condivisi.
Velocità per il backup	È necessario eseguire il backup di tutti i singoli blocchi, indipendentemente dal fatto che contengano dati o siano vuoti.	Il backup può essere notevolmente più veloce poiché vengono copiati interi file anziché singoli blocchi di dati.

Tab. 2 Confronto tra i sistemi di storage SAN e NAS.

Pit Stop

7 In che cosa consiste l'infrastruttura di archiviazione di un data center?

8 Che cosa sono NAS e SAN?

9 In che cosa consiste l'infrastruttura di rete di un data center?

Le prestazioni delle SAN variano in base al tipo di dischi utilizzati. Con collegamenti Fibre Channel, è possibile raggiungere velocità superiori a 16 Gbit/s. Attualmente, si sta diffondendo una nuova tecnologia chiamata FCoE (*Fibre Channel over Ethernet*), che permette di ottenere velocità fino a 100 Gbit/s.

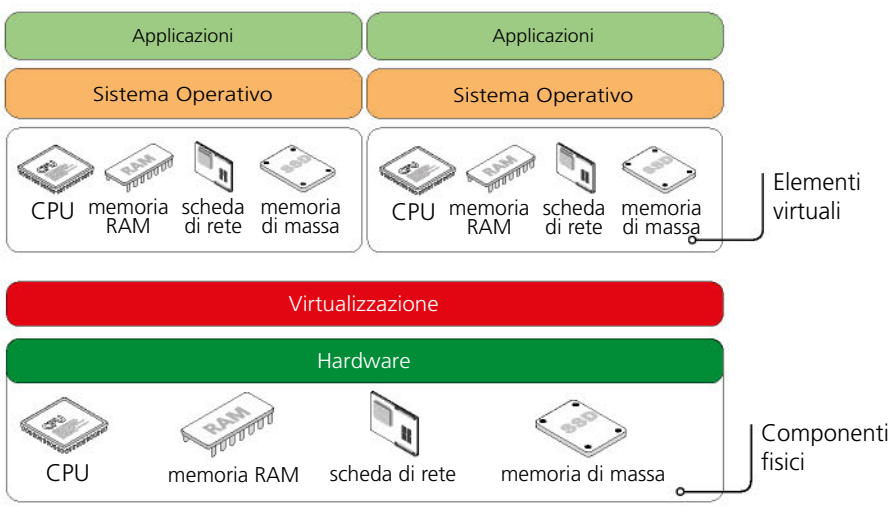
Infrastruttura di rete: il network

L'infrastruttura di rete SAN (*Storage Area Network*) è costituita dal cablaggio e dai dispositivi di rete che collegano tra loro le risorse di calcolo e di storage. Questa infrastruttura consente di interfacciare i data center agli utenti finali, condividere informazioni e connettersi a Internet. Gli elementi fondamentali includono:

- **cavi,** o altri mezzi fisici: collegano i dispositivi per consentire la comunicazione e lo scambio di informazioni;
- **switch**: necessari per collegare i diversi dispositivi all'interno di una LAN;
- **router**: necessari per instradare i dati tra diverse reti;
- **firewall**: fondamentale per la sicurezza;
- **access point**: necessari per consentire ai dispositivi wireless di connettersi a una rete cablata;
- **load balancer** (**bilanciatore del carico**): utili per distribuire le richieste che arrivano da diversi client su più server per garantire una distribuzione uniforme del carico e migliorare la disponibilità e le prestazioni complessive del sistema.

3 La Virtualizzazione

La virtualizzazione è un processo che consente la creazione di più ambienti di elaborazione simulati su un unico sistema fisico (**Figura 7**).



➜ **Fig. 7** Una macchina virtuale è dotata dei propri componenti virtuali (CPU, RAM, disco, schede di rete) realizzati tramite software e si comporta allo stesso modo di un computer fisico.

notabene

Virtualizzazione ed emulazione sono cose diverse: in un ambiente virtualizzato le risorse virtuali sono gestite come partizioni delle risorse fisiche lasciando inalterata la loro natura; ciò garantisce il mantenimento di integrità dei processi e performance elevate. I processori virtuali, pertanto, avranno la stessa capacità di calcolo e lo stesso set di istruzioni del processore fisico originario.

La virtualizzazione è spesso utilizzata per eseguire più sistemi operativi sullo stesso hardware contemporaneamente, sfruttando al massimo la capacità di calcolo dei computer moderni. Un ambiente di calcolo virtualizzato presenta due caratteristiche fondamentali:

- l'hardware è separato dal software;
- non ci sono limitazioni né dipendenze legate all'hardware.

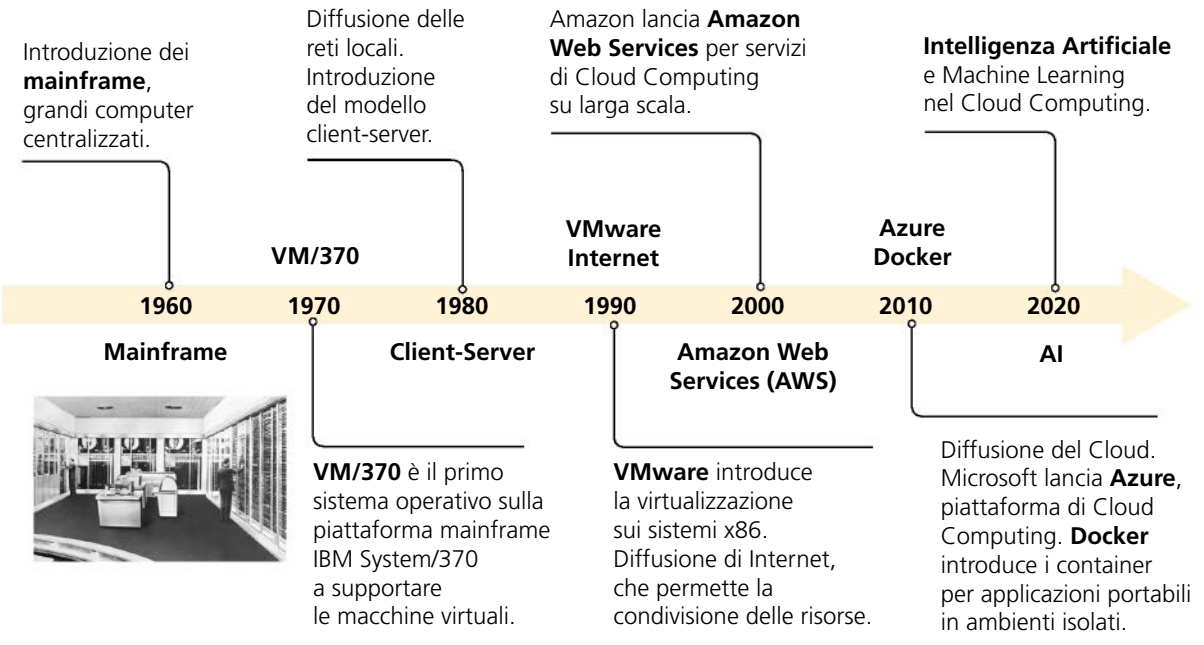
Pit Stop

10 Che cosa si intende per virtualizzazione?

Dagli ambienti fisici a quelli virtuali

Negli anni Sessanta del secolo scorso, IBM dominava il mercato dei mainframe (**Figura 8**) utilizzati da grandi aziende e istituzioni per l'elaborazione e la gestione di elevate quantità di dati. I costi erano molto alti e le aziende avevano la necessità di eseguire più applicazioni contemporaneamente, cosa che la struttura monolitica di allora non era in grado di soddisfare.
Fu negli anni Settanta che IBM introdusse il concetto di macchine virtuali (VM). Su un singolo mainframe erano ospitate più macchine virtuali indipendenti, ciascuna con un proprio sistema operativo e le proprie applicazioni.
Il sistema operativo VM/370 gestiva le risorse hardware e garantiva l'isolamento tra le diverse macchine virtuali tramite un componente chiamato Virtual Machine Monitor.
Questo concetto di virtualizzazione si è evoluto con la diffusione di VMware, che ha introdotto la virtualizzazione su sistemi x86. Questo ha portato alla moderna virtualizzazione, che ottimizza l'uso delle risorse hardware. L'avvento di Internet ha dato un ulteriore impulso alla virtualizzazione, che è alla base del cloud computing odierno.
La virtualizzazione è una componente fondamentale dei data center, poiché permette di eseguire in modo efficiente più applicazioni su un singolo server fisico, migliorando l'utilizzo delle risorse e riducendo i costi. Inoltre, grazie alla facilità di gestione e alla scalabilità, la virtualizzazione consente alle aziende di adattarsi rapidamente alle nuove esigenze di mercato.

Fig. 8 Cronologia del passaggio dagli ambienti fisici a quelli virtuali.



Funzionamento della virtualizzazione

Nella virtualizzazione non ci sono limitazioni o dipendenze imposte dall'hardware. Le applicazioni eseguite su una **macchina virtuale** (VM - Virtual Machine) hanno accesso alle stesse risorse hardware e software che avrebbero se fossero in esecuzione su una macchina fisica dedicata. Tuttavia, anche se possono essere eseguite sullo stesso sistema host, **ogni VM è isolata**.
La virtualizzazione è realizzata tramite un livello software che astrae (nascondi) le risorse del sistema fisico su cui è in esecuzione: CPU, GPU, memoria, storage o larghezza di banda di rete. Queste risorse vengono assegnate dinamicamente alle macchine virtuali, che le utilizzano per ottenere le risorse di cui hanno bisogno. Ogni VM viene eseguita come un singolo file sul sistema host e può essere facilmente spostata da un sistema all'altro, o anche nel cloud.
Il software che realizza la virtualizzazione si chiama **Virtual Machine Monitor** (**VMM**) o **hypervisor**. È il programma di basso livello che consente ai sistemi operativi ospitati (guest) di essere eseguiti in contemporanea su un singolo computer (host). Il codice dell'hypervisor è ben strutturato ed efficiente perché deve allocare le risorse in tempo reale. Può essere pensato come un vigile urbano che controlla il traffico e ottimizza l'avanzamento delle auto a un incrocio, in modo che tutti possano passare nel più breve tempo possibile.
Ci sono due tipi di implementazione dell'hypervisor (Figura 9):

- **Tipo 1**: l'hypervisor si integra con il kernel del sistema operativo e si interfaccia direttamente con l'hardware, consentendo una gestione più efficiente, veloce e stabile delle risorse assegnate alle macchine virtuali. Questa architettura non prevede l'utilizzo di sistemi operativi preesistenti sulle macchine, garantendo alte prestazioni. È usata per:
  - eseguire servizi server diversi (file server, database, web server, FTP server, DNS server, server di posta). Questi servizi sono in esecuzione su diverse macchine virtuali sulla stessa macchina fisica;

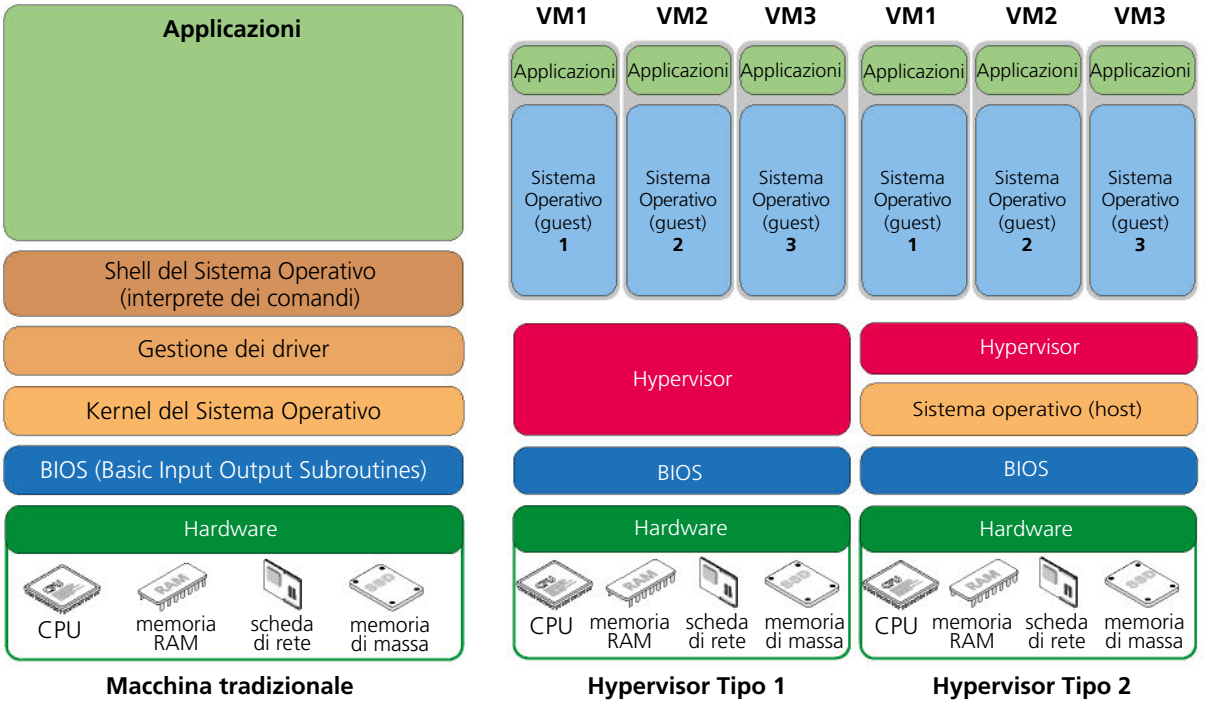


Fig. 9 Una macchina tradizionale e i due tipi di hypervisor.

– realizzare una *Virtual Desktop Infrastructure* (VDI) che consente di creare sistemi desktop personalizzati per ciascun utente, gestiti in modo centralizzato. La tecnica VDI può essere usata, per esempio, in grandi organizzazioni, ma anche in ambienti scolastici che utilizzano numerosi PC collegati in rete, che utilizzano sistemi operativi e applicazioni diverse. Esempi di Hypervisor di tipo 1 sono: Microsoft Hyper-V, Oracle VM Server, VMware ESXi.

- **Tipo 2**: l'hypervisor si appoggia su un sistema operativo esistente in grado di ospitarlo (hosted) e crea macchine virtuali a un livello superiore. Fa da cuscinetto tra il sistema operativo già presente e le macchine virtuali che vengono generate e installate sopra di esso. Svolge anche azione di controllo e monitoraggio delle virtual machine e ne permette il debug. Questa soluzione è meno efficiente e meno veloce della soluzione di tipo 1, perché si presenta come applicazione utente e non gestisce direttamente le risorse fisiche dell'hardware.
  Gli hypervisor di tipo 2 possono essere installati senza difficoltà e spesso sono disponibili come prodotti con licenza d'uso gratuita, sia open source sia commerciali. Ciò consente di usarli per provare applicazioni in esecuzione su sistemi operativi differenti ed essere al riparo dai rischi legati a errori di funzionamento e malware. Esempi comuni di hypervisor di tipo 2 sono QEMU, VirtualBox, VMware Player e VMware Workstation.

Virtualizzazione delle risorse

La virtualizzazione è applicata a una o più componenti di un sistema di calcolo gestito da un data center. Il coordinamento della gestione e la supervisione delle risorse virtuali sono affidati ad un **virtual data center manager** che provvede alla distribuzione delle risorse su più host fisici, bilanciando i carichi e diminuendo il rischio di blocchi operativi.

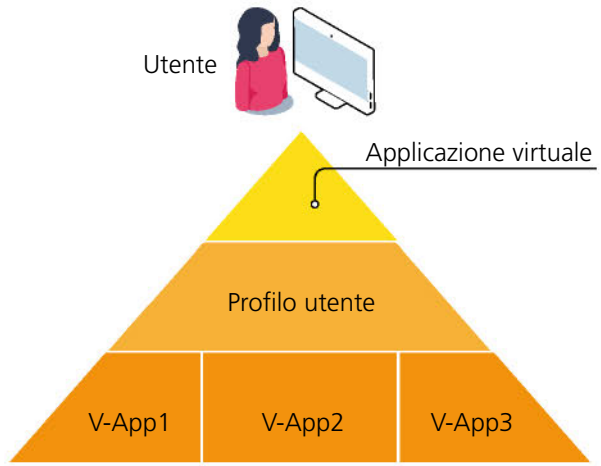
- **Virtualizzazione dei server** È l'applicazione più comune della tecnologia di virtualizzazione. Poiché i server sono progettati per eseguire molte attività, partizionare le risorse di calcolo perché possano essere usate in modo più efficiente costituisce un grande vantaggio per molte organizzazioni.
- **Virtualizzazione dello storage** Consente di gestire lo storage che può essere fisicamente su reti o luoghi fisici diversi, come se fosse logicamente un unico dispositivo condiviso. Ciò semplifica le attività di backup, archiviazione e ripristino. Le tecnologie usate sono SAN (Storage Area Network) e NAS (Network-Attached Storage), che forniscono le risorse di storage per gli ambienti virtualizzati.
- **Virtualizzazione della rete** Grande importanza assume oggi la connettività di rete. È infatti impensabile pensare a un computer come a una macchina isolata, senza interconnessioni con altri sistemi. In un ambiente di virtualizzazione questo aspetto riveste notevole importanza in quanto la connettività deve essere garantita sia a livello di prestazioni sia a livello di sicurezza. Come la rete fisica è un insieme di macchine collegate tra loro per potersi scambiare i dati, così la rete virtuale (virtual network) è un insieme di macchine virtuali, in esecuzione su una singola macchina fisica, che sono collegate logicamente tra loro in modo che possano scambiarsi dati. Una rete fisica è costruita sui dispositivi di rete: schede di rete, router, switch, che permettono l'interfacciamento alla rete e il collegamento tra terminali. In modo analogo, gli ambienti virtuali forniscono, sotto forma di software, le funzionalità di schede di rete virtuale, switch virtuale, router virtuali ecc.

Pit Stop

11 Che cos'è hypervisor?

12 Come può essere implementato hypervisor?

- **Desktop virtuale** È un desktop che esiste virtualmente, accessibile ovunque tramite Internet. È una variante del modello client/server, indicato come server-based computing. I personal computer degli utenti di un'azienda sono sostituiti da desktop virtuali intesi come "terminali" di un server centralizzato (VDI, *Virtual Desktop Interface*). L'utente si collega remotamente al server, utilizzando un PC, un terminale, un tablet o un altro dispositivo su cui è installato il programma client che instaura una connessione di rete. La centralizzazione dell'infrastruttura permette di accedere da remoto con la sicurezza di avere dati protetti e disponibili. Un desktop virtuale permette a un utente di accedere al proprio sistema operativo e ai propri dati da un PC remoto utilizzando le proprie credenziali.
- **Virtualizzazione delle applicazioni** La virtualizzazione delle applicazioni separa l'applicazione dal sistema operativo e dall'hardware su cui viene eseguita. L'utente finale accede comunemente alle applicazioni virtualizzate da un thin client, un computer economico che si collega a un server centrale che ospita le applicazioni e i dati necessari all'utente.
  L'installazione di un'applicazione virtuale avviene creando un contenitore (shell) che, alla stregua di una cartella protetta, contiene le impostazioni dell'ambiente di esecuzione. In pratica, possiamo costruire una postazione di lavoro utente modulare dove colleghiamo all'ambiente VDI le applicazioni virtualizzate e, in uno storage condiviso, un profilo per ogni utente (**Figura 10**).



➜ **Fig. 10** Un'applicazione virtuale è un'applicazione ottimizzata per funzionare su infrastrutture virtuali in modo indipendente. Più applicazioni utente (V-App) fanno capo a un singolo utente.

Questo metodo offre diversi vantaggi:
- Gestione centralizzata. La manutenzione e gli aggiornamenti possono essere gestiti centralmente, riducendo i costi operativi e semplificando il lavoro.
- Sicurezza. Il rischio di infezioni da malware o attacchi informatici è ridotto e limitato al solo server centrale.
- Riduzione dei costi. I thin client richiedono meno risorse hardware rispetto ai tradizionali PC desktop. Ad esempio, non hanno bisogno di una grande quantità di memoria, poiché la maggior parte delle operazioni di calcolo e l'archiviazione dei dati avvengono su server centrale.
- Collegamento da remoto. Permette agli utenti di avere il proprio ambiente di lavoro sul proprio dispositivo, accedendo da remoto.

Approfondimento
Il Virtual Networking

Vantaggi e problematiche della virtualizzazione

A fronte dei numerosi benefici della virtualizzazione delle risorse, emergono anche alcune problematiche e limitazioni che sintetizziamo qui di seguito.

Benefici:

- **Risparmi sui costi ed efficienza**: riduzione dei costi per l'hardware e per lo spazio necessario ad ospitarlo. Uso efficiente delle risorse e risparmio energetico.
- **Scalabilità e flessibilità**: capacità di adattare l'uso delle risorse in base ai carichi di lavoro. Rapidità nella configurazione iniziale delle risorse (*provisioning*).
- **Disaster recovery e continuità operativa**: la virtualizzazione aiuta a proteggere i dati e a mantenere i servizi sempre disponibili. Offre funzioni come la copia dei dati e lo spostamento delle applicazioni da un server all'altro senza interruzioni, garantendo così che tutto continui a funzionare senza problemi. Inoltre, supporta strategie di disaster recovery per riprendersi rapidamente da problemi gravi, riducendo i tempi di inattività (*downtime*).
- **Ambienti di test e sviluppo**: la virtualizzazione rende più facile creare ambienti di test isolati, permettendo di eseguire prove indipendenti e accelerare lo sviluppo senza influenzare le altre applicazioni.

Limitazioni:

- **Prestazioni e allocazione delle risorse**: anche se la virtualizzazione permette di eseguire più sistemi operativi su un singolo server fisico, potrebbe esserci un impatto negativo sulle prestazioni se non vengono allocate correttamente le risorse. Alcuni software possono richiedere licenze separate per essere eseguiti in ambienti virtualizzati, aumentando i costi operativi. Inoltre non dimentichiamo che se il server fisico che ospita le macchine virtuali subisce un guasto, tutte le macchine virtuali potrebbero essere compromesse (*Single Point of Failure Dependency*).
- **Sicurezza**: per preservare la sicurezza, è necessario garantire l'isolamento tra le macchine virtuali e la riservatezza dei dati, impedendo accessi non autorizzati.
- **Compatibilità e integrazione**: potrebbero verificarsi problemi di compatibilità tra i vecchi sistemi (*legacy*) e quelli virtualizzati, con conseguenti difficoltà nella migrazione dei dati.

Pit Stop

13 Quali sono i vantaggi della virtualizzazione?

notabene

Portare tutti i servizi su un'unica struttura determina un punto di criticità (**SPoF, Single Point of Failure**) perché, in caso di guasto, si avrebbe la paralisi completa dei sistemi informatici.

I data center virtuali

Non tutte le organizzazioni hanno la necessità o la volontà di dotarsi di un data center interno personalizzato, perché anche se questo consentirebbe una gestione diretta delle proprie strutture fisiche, richiederebbe comunque investimenti significativi per l'acquisto di hardware, e per provvedere alla configurazione, alla manutenzione e alla sicurezza. Spesso è più conveniente rivolgersi a un fornitore di servizi che offre risorse per l'infrastruttura di rete, lo storage e la capacità di calcolo, fornendo misure di sicurezza adeguate.
In questo caso, si parla di **data center virtuale**. La differenza principale tra le due configurazioni è la seguente:

- **data center fisico**: è implementato localmente (*on-premise*).
- **data center virtuale**: è ospitato presso un fornitore di servizi (*off-premise*) che gestisce l'infrastruttura e garantisce l'accesso alle risorse tramite connessione Internet.

notabene

Il fatto che si paghino solo le risorse utilizzate implica che l'utilizzo di ogni risorsa deve poter essere misurato.

Nei data center virtuali, sia l'hardware (router, switch, server, CPU, memoria RAM, controller,...) sia il software (server web, gestore del database, firewall,...) sono disponibili in remoto. La complessità dell'infrastruttura è gestita dal fornitore di servizi, consentendo all'utente di concentrarsi sul proprio progetto, la produttività e i processi aziendali.
Quando un'azienda configura un data center virtuale, tramite il proprio pannello di controllo, può definire diverse impostazioni, tra cui:

- **localizzazione**, che stabilisce dove il data center fisico (del fornitore) è situato geograficamente;
- **sistema operativo**, che sceglie il sistema operativo per le applicazioni (ad esempio, Windows o Linux);
- **hypervisor**, che specifica l'hypervisor utilizzato per la virtualizzazione (come Hyper-V o VMware);
- **template dell'ambiente di lavoro**, che costituisce una "immagine" del sistema operativo e del software preconfigurato dell'ambiente di lavoro informatico;
- **risorse**, che definisce le risorse di calcolo, storage e connettività che desidera utilizzare.

La possibilità di definire e gestire le risorse necessarie è fondamentale per la scalabilità: un ambiente on-premise è generalmente meno scalabile rispetto ai data center virtuali che consentono di incrementare o ridimensionare le risorse in modalità on-demand. Inoltre, il pagamento avviene solo per le risorse effettivamente utilizzate (modello Pay-per-use). Gli aggiornamenti sono gestiti direttamente dal provider e le impostazioni possono essere modificate in qualsiasi momento in base alle esigenze.

Tipi di data center

Di seguito riassumiamo i diversi tipi di data center evidenziandone i vantaggi e gli svantaggi relativamente alla collocazione e alla gestione delle risorse.

Data center on-premise

Questi data center sono realizzati, gestiti e di proprietà delle aziende stesse.

- **Vantaggi**:
  - Maggiore sicurezza: consente di gestire i rischi internamente all'organizzazione.
  - Possibilità di personalizzare il data center per rispondere alle necessità specifiche.
- **Svantaggi**:
  - Richiedono costi significativi per l'acquisto dell'hardware, la configurazione del sistema e la manutenzione continua.
  - Potrebbero essere necessari **più data center** per implementare una strategia di ridondanza, distribuendo i carichi di lavoro. Avere un solo data center, infatti, rappresenta un punto critico ad alto rischio (*Single Point of Failure*).

Data center in colocation

Le strutture di co-locazione consentono di affittare spazio per archiviare server, storage e altri hardware. Offrono sistemi di raffreddamento, larghezza di banda e sicurezza. L'azienda gestisce i propri componenti all'interno di questa infrastruttura.

- **Vantaggi**:
  - **Riduzione** dei costi di mantenimento.
  - Distribuzione geografica dell'hardware per **minimizzare la latenza**.
- **Svantaggi**:
  - Può essere difficile trovare la struttura di co-locazione giusta nelle diverse aree geografiche in cui si opera.
  - I **costi** di affitto dell'infrastruttura possono aumentare molto rapidamente con l'aggiunta di nuovi servizi.

Data center in cloud off-premise

È possibile affittare sia lo spazio sia l'infrastruttura da fornitori di servizi in cloud. Si accede a questa infrastruttura utilizzando servizi flessibili e a pagamento.
Esempi di fornitori di servizi in Cloud sono: Amazon Web Services (AWS), Microsoft (Azure), IBM Cloud o altri provider di cloud pubblico.

- **Vantaggi**:
  - Riduzione dell'investimento nell'hardware e dei costi di mantenimento delle infrastrutture.
  - Offre diverse opzioni di utilizzo, condivisione delle risorse, disponibilità e ridondanza.
- **Svantaggi**:
  - È necessaria una connessione a Internet per poter raggiungere la struttura esterna alla sede locale.
  - I dati vengono archiviati e gestiti da un fornitore esterno (esternalizzati).

Comprendi con l'analogia

Una cena tra amici e… i data center



Alla fine della scuola, in una limpida sera d'inizio estate, quando il caldo è ancora sopportabile e la brezza serale ti invade il cuore facendoti sognare viaggi esotici, ti ritrovi a pianificare una cena con amici e colleghi. Ho tre opzioni da valutare per venire incontro alle esigenze di tutti. Ogni scelta ha i suoi pro e contro, proprio come i diversi tipi di data center:

A Casa Mia (*Data Center On-Premise*): ho deciso di cucinare tutto a casa mia. Il vantaggio è che ho il controllo completo sulla cucina e sugli ingredienti: so bene dove sono i piatti, i coltelli e cosa ho nel frigo. Il problema è che devo possedere una buona cucina e sperare che il forno non si guasti! Questa soluzione è analoga a un data center on-premise, dove tutto è gestito internamente con il pieno controllo sull'hardware, la rete e il software.

Affitto Uno Spazio con Cucina (*Data Center in Colocation*): con i miei amici, abbiamo deciso di affittare uno spazio con una cucina completamente attrezzata, fornelli e forno inclusi. Portiamo le nostre pentole e ingredienti, ma la cosa bella è che possiamo utilizzare le forniture efficienti e professionali presenti nello spazio-cucina. Questo è simile a un data center in colocation, dove si affitta uno spazio fisico in cui inserire le proprie apparecchiature, condividendo alcune risorse comuni, come l'elettricità e la connettività.

Cena da Asporto con Consegna a Domicilio (*Data Center in Cloud*): gli altri amici preferiscono ordinare una cena da asporto. La cosa bella è che non dobbiamo preoccuparci della cucina o degli ingredienti. Semplicemente facciamo un ordine e il cibo ci viene consegnato dove preferiamo. Questa soluzione è analoga a un data center in cloud, dove non possediamo nulla di fisico, ma utilizziamo i servizi remoti forniti da un fornitore di cloud, senza dover gestire nulla internamente.

Pit Stop

14 Quali sono i diversi tipi di data center?

4 Sicurezza e continuità operativa nei data center

Livelli di sicurezza nei data center

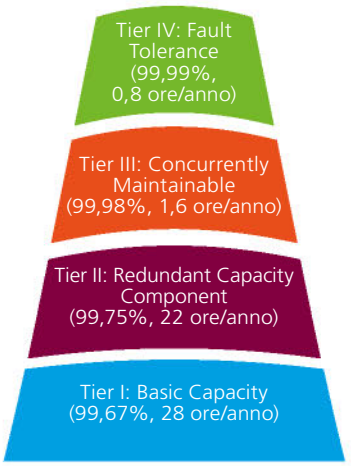
Nei data center è fondamentale implementare sistemi di sicurezza che siano relativi a riservatezza, integrità e disponibilità dei dati. Una prima panoramica sulla sicurezza dei data center prevede una divisione nei seguenti livelli:

- **Livello Perimetrale**, che include il controllo degli accessi e dei dispositivi fisici (recinzioni, personale di sicurezza , sistemi di rilevamento anti intrusione ecc);
- **Livello dell'Infrastruttura**, che protegge le apparecchiature da danni e surriscaldamento (sistemi di raffreddamento, apparecchiature di alimentazione e di backup ecc);
- **Livello dei Dati**, che protegge la perdita dei dati e l'accesso non autorizzato (sistemi di rilevamento delle minacce, controlli periodici per garantire la conformità);
- **Livello Ambientale**, che si concentra sul controllo ambientale e, in particolare, sull'utilizzo dell'energia rinnovabile e del risparmio energetico. Include anche sensori e dispositivi per il rilevamento automatico di catastrofi naturali.

La continuità del servizio

Per garantire la **continuità del servizio**, è necessario prendere misure per ridurre al minimo le interruzioni causate da guasti o manutenzione. La **disponibilità dei dati** vuol dire che i dati sono sempre accessibili e utilizzabili. In alcuni casi, il tempo di inattività delle macchine è così critico per l'attività aziendale che questo problema è noto come **business continuity**. Con l'aumento delle dimensioni e della complessità dei data center e l'archiviazione di informazioni sensibili, i governi e altre organizzazioni hanno stabilito numerose norme. Lo standard più diffuso per la progettazione e l'infrastruttura dei data center è **ANSI/TIA-942**, che definisce quattro categorie basate su livelli di ridondanza e tolleranza ai guasti. La classificazione in quattro strati ("tier") segue una progressione verso una maggiore affidabilità e disponibilità (Figura 11):

1. **Tier I** (**Infrastruttura di base – basic capacity**): ha componenti con capacità singola e una distribuzione non ridondante, cioè senza backup o duplicazioni che garantiscano la continuità del servizio in caso di guasto. Protegge dalle interruzioni dovute a errori umani, ma non da guasti imprevisti. Il tempo di inattività annuale previsto è di 29 ore.
2. **Tier II** (**infrastruttura con componenti ridondanti – redundant capacity component**): utilizza componenti con capacità ridondante, ma un percorso di distribuzione (infrastrutture che trasportano i dati) senza percorsi alternativi o backup in caso di guasto. Il tempo di inattività annuale previsto è di 22 ore.
3. **Tier III** (**infrastruttura gestibile senza interruzioni dei servizi – concurrently maintenable**): offre protezione da quasi tutti gli eventi fisici, consentendo la manutenzione senza interrompere i servizi. Il tempo di inattività annuale previsto è di 1,6 ore.
4. **Tier IV** (**infrastruttura tollerante ai guasti – fault tolerance**): offre la massima ridondanza e tolleranza ai guasti. I sistemi sono completamente duplicati, il che garantisce che, in caso di guasto, ci sia sempre un sistema di backup pronto a intervenire limitando il tempo di inattività a soli 26 minuti all'anno.



↑ **Fig. 11** I quattro livelli (TIER) per la classificazione dei data center in base alla continuità del servizio.

Soluzioni base per la continuità del servizio

Il malfunzionamento di un qualsiasi elemento può causare una **indisponibilità di servizio** (**downtime**) con ripercussioni economiche anche gravi. Se, per esempio, pensiamo a un sistema di server utilizzato da una società di e-commerce, capiamo bene che ogni minuto di fermo-macchina comporta una notevole perdita economica. È molto importante quindi garantire un'alta **disponibilità di servizio** (in termini tecnici, ciò prende il nome di **high availability**). Per questo, un ambiente di virtualizzazione ben progettato prevede tecniche di:

- ridondanza e duplicazione;
- cluster di server;
- sistemi di archiviazione.

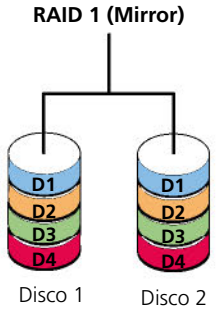
Questi sistemi sono progettati per minimizzare gli effetti di guasti e blocchi imprevisti e possono arrivare a replicare l'intero data center per garantire la continuità del servizio. Lo **standard ISO 22301** fornisce le linee guida da seguire in caso di incidenti che potrebbero causare l'interruzione delle attività. Queste raccomandazioni non si riferiscono solo ad apparati e risorse fisiche e logiche, ma anche a persone e fornitori esterni. Il "**Business Continuity Plan**" contiene le procedure di risposta, recupero e ripristino delle attività a seguito di un'interruzione.
Alcune definizioni ci possono aiutare a capire meglio il significato dei termini più ricorrenti:

- **Fault Tolerance – «Prevenire le perdite di dati»**: mira a evitare interruzioni nei servizi a fronte di guasti tecnici. Si tratta di predisporre dei sistemi duplicati per rilevare guasti hardware a processori, memorie, dispositivi di rete, alimentatori e, in caso di guasto, spostare il servizio su sistemi paralleli. Tra le tecniche utilizzate ricordiamo RAID (*Redundant Array of Independent Disks*) per accertare che i dati letti e scritti sui dischi siano accurati e integri.
- **Disaster recovery – «Primo: non perdere dati!»**: È il processo che permette di recuperare e ripristinare i dati e le applicazioni in caso di disastro. Una politica di disaster recovery prevede di organizzare un secondo luogo fisico in cui tenere il duplicato dei dati, recuperandoli in caso di incidenti, guasti o catastrofi naturali. L'elemento determinante è il tempo di ripristino: la velocità di recupero dei dati dipende molto dalle politiche di pianificazione e dai processi che vengono messi in atto per rispondere a situazioni critiche.
- **Business Continuity – «Zero downtime»**: la continuità del servizio garantisce una continuità operativa, evitando i disservizi, in caso di malfunzionamenti, rotture o gravi danni al sistema. Di fatto si tratta di impegnare le risorse hardware e software per fare in modo che i sistemi continuino a funzionare, senza interruzioni, anche durante il verificarsi di un evento avverso. Durante la fase di progettazione di un data center è fondamentale prevedere ridondanze su tutto quanto può costituire **Single Point of Failure**, al fine di evitare che il malfunzionamento di un componente possa compromettere l'intero sistema. È quindi consigliabile che alimentazioni, collegamenti e dispositivi di rete siano ridondanti, e che l'intero data center sia duplicato in luoghi geograficamente distinti. Per non compromettere le prestazioni, questi siti dovrebbero trovarsi entro una distanza di 50 km, riducendo il rischio che entrambi i siti siano colpiti dalla stessa catastrofe, mantenendo però una bassa latenza per le operazioni che vengono effettuate con regolarità, come il backup dei dati.

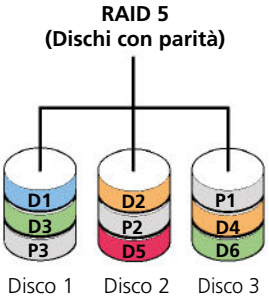
Pit Stop

15 Che cosa si intende per "continuità del servizio"?

16 Quali sono le principali differenze tra i quattro livelli di data center?



↑ **Fig. 12** RAID 1: due dischi fissi, di cui uno è la copia dell'altro.



↑ **Fig. 13** RAID 5: i controlli di parità sono ripartiti tra più dischi: D1, D2 con parità P1; D3, D4 con parità P2 e D5, D6 con parità P3.

RAID: strategie di ridondanza dei dati

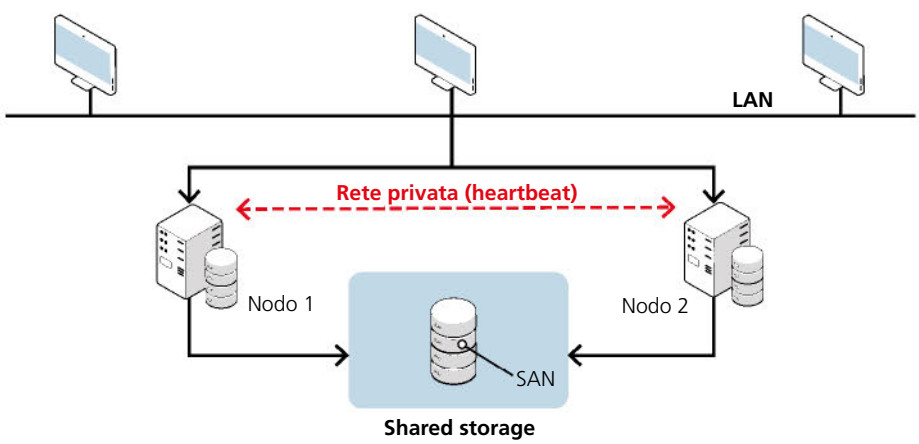
Un aspetto fondamentale nella gestione della memoria è la gestione delle ridondanze: occorre considerare la possibilità di guasti hardware che mettano in pericolo l'integrità dei dati. La tecnica **RAID** (**R***edundant* **A***rray of* **I***ndipendent* **D***isks*) viene utilizzata per migliorare la tolleranza ai guasti, aumentare le prestazioni (suddivide i dati tra più dischi, permettendo l'accesso parallelo) e ampliare la capacità di archiviazione, combinando più dischi fisici in un unico disco logico (volume). Esistono diverse versioni di RAID. Tra le più comuni troviamo:

- **RAID 1** (detto anche *mirroring*) (**Figura 12**): si configurano due dischi, di cui uno è la copia dell'altro. Se uno si guasta, il sistema lo esclude e continua a operare normalmente: verrà inviato un allarme al fine di poter procedere alla sostituzione dell'unità guasta e, dopo la sua sostituzione, il sistema provvederà automaticamente alla ricostruzione dei dati sulla nuova unità. La configurazione mirroring offre ottime prestazioni e sicurezza, ma riduce lo spazio disponibile: solo il 50% dello spazio totale dei dischi è utilizzabile.
- **RAID 5**: risolve i problemi di inefficienza di RAID 1. Prevede l'utilizzo di tre o più unità disco (**Figura 13**). Ad esempio, se si utilizzano tre unità disco, i dati vengono scritti in modo distribuito su due di esse (immaginiamo di scrivere i byte come parole in colonna: D1 e D2, dove ogni riga rappresenta un'unità disco diversa). Sulla terza unità viene scritta la parità (P1): 1 se la somma dei bit della colonna è pari, 0 se la somma è dispari. In caso di rottura di un disco, sarà possibile procedere alla sua ricostruzione riscrivendo la tabella di parità, una volta sostituita l'unità guasta. I valori della tabella di parità saranno calcolati sulla base dei dati presenti sui dischi funzionanti. Il RAID 5 permette un minore spreco di risorse, in quanto lo spazio di una sola unità viene dedicato alla gestione dell'errore, ma è penalizzato nelle prestazioni, perché ogni operazione di scrittura richiede la lettura delle informazioni per poi procedere alla scrittura del bit di parità.

Gestione di un cluster di server

Uno degli aspetti fondamentali che permettono di sopperire ai fermi macchina e garantire la continuità del servizio è l'utilizzo di un **cluster di failover**. Un cluster è costituito da un gruppo di nodi (server) che lavorano insieme per garantire la disponibilità dei dati e dei servizi (**Figura 14**), riducendo al minimo i tempi di inattività. In caso di malfunzionamento di un server fisico, il gestore del virtual data center può individuare il guasto e spostare le virtual machine dall'host danneggiato agli altri host fisici, consentendo loro di ripartire. I nodi del cluster sono collega-

Approfondimento
RAID



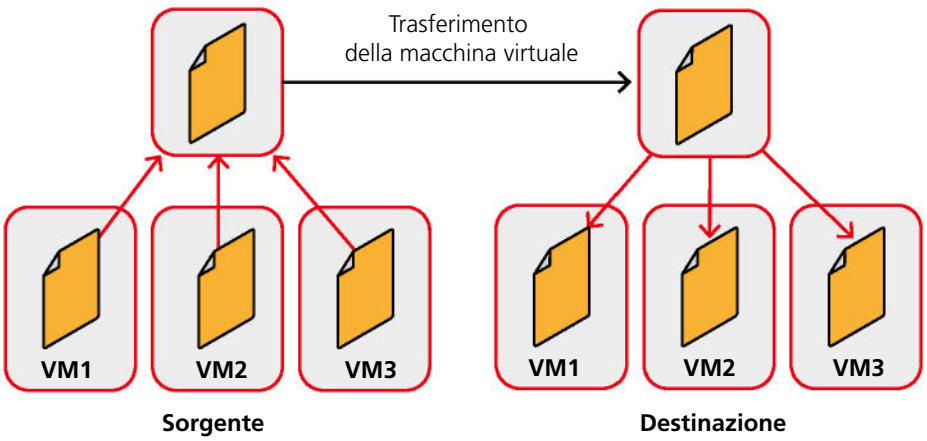
→ **Fig. 14** Un cluster di failover composto da due nodi. Ciascun cluster è collegato allo storage (SAN) condiviso.

ti tramite una rete privata di importanza vitale ("**heartbeat network**", "rete battito cardiaco"), che serve a monitorare costantemente lo stato del sistema: in caso di guasto, il cluster interviene reindirizzando le richieste da un server all'altro.

Le funzioni di migrazione

Oltre a dover intervenire sui guasti, può essere necessario migrare (spostare) le macchine virtuali da un host fisico all'altro, o trasferire i file da uno storage fisico a un altro, per migliorare le prestazioni dei sistemi, aggiornarli e manutenerli.

- **Migrazione di macchine virtuali** (**live migration**): permette di spostare una macchina virtuale completa in esecuzione da un server fisico a un altro **senza alcuna interruzione nel funzionamento**. In realtà, la procedura non avviene istantaneamente, ma occorre un certo tempo, seppur breve, per trasferire lo stato di esecuzione della macchina virtuale e della sua memoria. Per assicurare l'integrità delle transazioni, la macchina virtuale originaria viene sospesa solo dopo aver copiato l'intera memoria e lo stato del sistema sull'host di destinazione. Il tempo di fermo macchina (downtime) è dell'ordine di pochi secondi. Questo dà all'utente la sensazione che non vi siano interruzioni. (Figura 15)



← Fig. 15 Migrazione di una macchina virtuale da un sistema fisico a un altro.

- **Migrazione dello storage** Lo spostamento dei file associati alle macchine virtuali, cioè la migrazione dello storage, permette di spostare i file da uno storage all'altro (o all'interno dello stesso storage) senza interruzioni di servizio (live). Questa operazione è utile, ad esempio, nel caso di manutenzione, che viene effettuata in seguito al guasto di un'unità disco appartenente a un configurazione RAID, oppure in caso di aggiornamento dell'hardware. L'operazione è effettuata anche per ottimizzare i carichi: ad esempio, se un disco sta esaurendo lo spazio, si può usare la memoria di altri "volumi" (dischi) anche a macchina accesa.

Snapshot

Uno snapshot è una funzione che consente di catturare lo stato di una virtual machine così com'è nel momento in cui la funzione di snapshot è eseguita. È utile per definire dei **punti di ripristino** da utilizzare quando abbiamo la necessità che la macchina torni nello stato precedente un determinato evento.
Si possono creare più snapshot, ognuno dei quali viene identificato tramite da un nome ed è associato allo stato della macchina nell'istante in cui è stato creato.

Pit Stop

17 Che cos'è il RAID?

18 A che cosa serve il RAID?

19 Che cos'è un cluster di server?

20 A che cosa serve un cluster di server?

Pit Stop

21 Cosa si intende per "migrazione" di una macchina virtuale?

Pit Stop

22 Che cos'è uno snapshot?

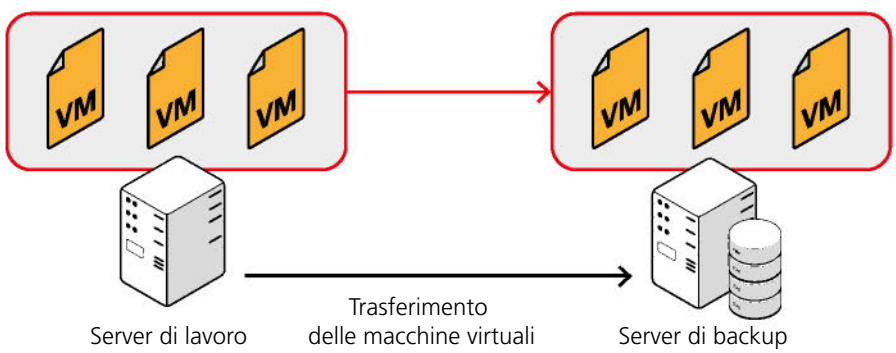
È utile quando si devono fare modifiche o aggiornamenti critici alla virtual machine e, temendo di sbagliare, ci si tutela creando uno snapshot che consenta di tornare allo stato precedente la modifica. Occorre porre attenzione alla gestione degli snapshot, perché il ripristino comporta la perdita dei dati memorizzati successivamente all'attivazione e potrebbe causare situazioni di inconsistenza. Inoltre non va trascurato il fatto che l'uso di snapshot crea un aumento dello spazio richiesto su disco; pertanto si consiglia di renderlo attivo unicamente quando necessario e per un tempo limitato.

Clonazione e template

La **clonazione** delle macchine virtuali è un processo che ci permette di **duplicare una VM** ottenendone un'altra con la stessa configurazione. Ad esempio, possiamo creare un ambiente di prova identico a quello di produzione.
Un'altra tecnica utile per accelerare la creazione di nuove macchine virtuali è la duplicazione da una VM esistente su un **template**. In questo caso, non otteniamo una nuova VM, ma un **modello** (template) che può essere utilizzato per generare altre macchine simili. Durante la creazione delle nuove VM, possiamo parametrizzare il nome della macchina, la configurazione di rete e altri dati per evitare conflitti con gli ambienti esistenti.

Backup e repliche del data center virtuale

Un aspetto molto importante di un qualsiasi sistema informatico è la gestione dei backup, cioè la realizzazione di copie di salvataggio che permettano il ripristino dei dati in caso di perdite accidentali di informazioni. Nei sistemi tradizionali, basati su hardware fisico, si è soliti effettuare una copia dei dati e il ripristino in un ambiente operativo già funzionante. Nel caso si debba ripristinare il server, è necessario riconfigurare il sistema operativo di base e successivamente procedere alla copia dei dati e delle applicazioni. Tutto ciò prevede disagi e tempi lunghi. Negli ambienti virtuali invece è possibile attivare una procedura di **disaster recovery** che consente di **ripristinare l'intero server su un sistema remoto**, partendo da una copia di backup che contiene lo stato del sistema, dati compresi (Figura 16). Il ripristino dei dati può avvenire integralmente, oppure può essere parziale e selettivo, individuando semplicemente i file o le cartelle di cui viene richiesto il ripristino. Anche la creazione di ambienti di disaster recovery online, in grado di entrare in funzione immediatamente nel caso di crash del data center, risulta essere molto utile. In questi casi viene ricreata remotamente una struttura di host fisici e storage simile a quella utilizzata nel data center principale. Il software di backup permette di replicare in remoto l'intero ambiente virtuale, in modo che tutte le attività possano essere reindirizzate, tempestivamente, sui server remoti.



→ **Fig. 16** Una procedura di disaster recovery permette di replicare, in tempi rapidi, le virtual machine su un server di backup.

Approfondimento - Tecnologia

La storia delle virtualizzazioni: da VM/SP a VMware

IBM introdusse il concetto di virtualizzazione già negli anni Sessanta del secolo scorso. Il sistema VM/SP (una famiglia di "IBM virtual machine operating systems") è considerato il primo sistema operativo commercializzato per la creazione di ambienti virtuali e fu implementato su numerosi mainframe della casa americana. Il cuore dell'architettura VM è un programma di controllo, o hypervisor, che crea l'ambiente della macchina virtuale fornendo la virtualizzazione completa della macchina con la condivisione delle risorse fisiche del sistema.
Verso la fine degli anni Novanta, VMware lanciò sul mercato VMware Virtual Platform, il primo prodotto di virtualizzazione x86, basato su studi precedenti effettuati all'Università di Stanford. Da allora, molti ne hanno seguito l'esempio, ma tutte le macchine si basano sui principi teorici proposti nel 1974 dagli informatici americani Gerald Popek e Robert Goldberg, che ancora oggi costituiscono le fondamenta della virtualizzazione. In pratica, per realizzare la virtualizzazione delle risorse a livello software (Virtual Machine Monitor, VMM), bisogna considerare tre aspetti fondamentali:

1. **Equivalenza** (**Equivalence/Fidelity**): un programma in esecuzione su una macchina virtuale deve presentare un comportamento sostanzialmente identico a quello ottenuto durante l'esecuzione su una macchina fisica.
2. **Controllo delle risorse**: VMM deve avere il controllo completo delle risorse virtualizzate.
3. **Efficienza**: una parte significativa delle istruzioni deve avvenire senza l'intervento del VMM.



Oggi VMware continua a essere un leader nel settore della virtualizzazione e del cloud computing, puntando molto sulla sovranità digitale, cioè sulla possibilità che le aziende e le istituzioni possano gestire e proteggere i propri dati senza dipendere da fornitori esterni. Le cose, però, potrebbero cambiare nel prossimo futuro. A seguito di un'acquisizione, VMware ha cambiato le politiche commerciali, ad esempio non rendendo più disponibile la versione gratuita. Di conseguenza, il mercato sta già cercando un successore.

Approfondimento
La gestione della rete virtuale

Laboratorio

ATTIVITÀ 1
Introduzione alle Macchine Virtuali con Oracle VirtualBox

Scenario

Utilizzando un hypervisor come **VirtualBox**, è possibile creare e gestire più VM su un singolo computer fisico (host). VirtualBox è un **hypervisor di tipo 2**, che richiede un sistema operativo host (come Windows, macOS o Linux) per funzionare. Il software hypervisor viene installato come un'applicazione normale. Una volta installato, permette di creare e gestire macchine virtuali che possono eseguire altri sistemi operativi "guest" all'interno del sistema operativo host. Questo lo rende facile da installare e utilizzare, ma può avere prestazioni inferiori rispetto agli hypervisor di tipo 1, che funzionano direttamente sull'hardware fisico. Ogni VM funziona come un computer indipendente, con il proprio sistema operativo, applicazioni e risorse.

Obiettivo

In questa esercitazione utilizzeremo VirtualBox per creare e configurare due macchine virtuali: una con una distribuzione Linux e l'altra con Kali Linux. Questo ci permetterà di comprendere meglio come funzionano le macchine virtuali e operare in un ambiente sicuro e isolato per creare e testare software ed eseguire analisi di sicurezza.

Svolgimento

Passo 1: installazione di VirtualBox

- Scaricare VirtualBox dal sito ufficiale e installarlo sul sistema operativo host della propria macchina seguendo le istruzioni. In rete si trovano facilmente numerosi e validi tutorial su come installare e configurare una macchina virtuale su VirtualBox, a cui si rimanda per i dettagli tecnici.

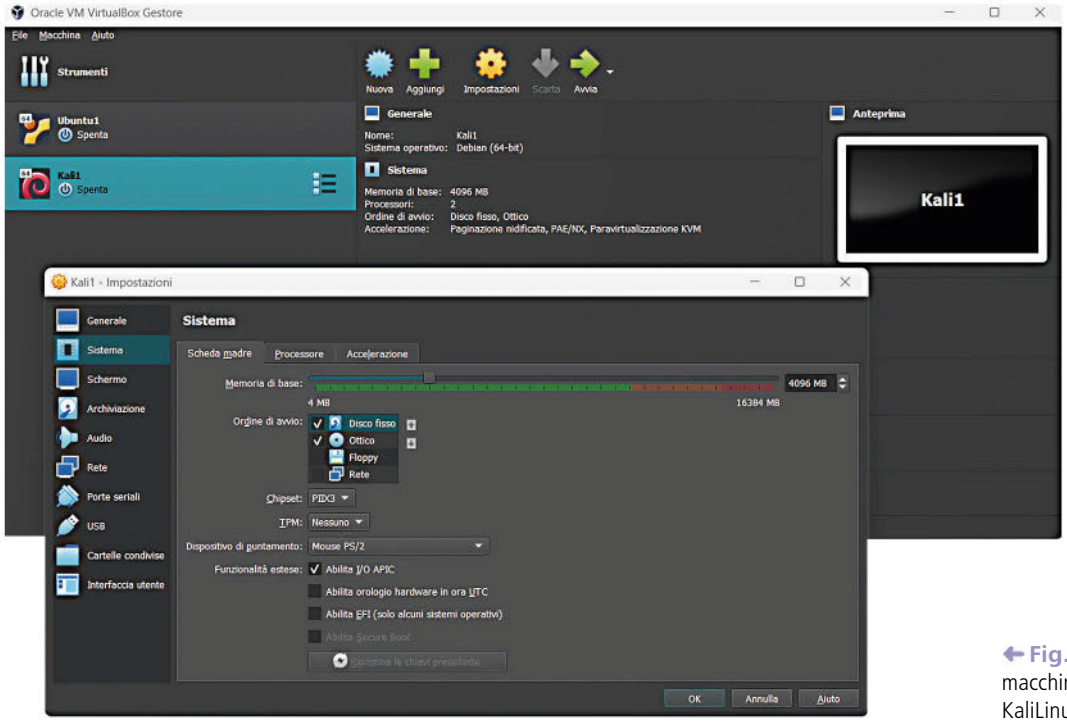
Passo 2: creazione e installazione di una Macchina Virtuale Linux

- Aprire VirtualBox e cliccare su Nuova per creare una nuova VM.
- Assegnare un nome alla VM (ad esempio, "Ubuntu1") e selezionare, dal menu a discesa, il tipo di sistema operativo, ad esempio Linux Ubuntu, e la versione.
- Configurare la memoria RAM desiderata e lo spazio di archiviazione (disco) per la VM.
- Completare la configurazione e avviare la VM.

Passo 3: creazione e installazione di una Macchina Virtuale Kali Linux

- Ripetere i passaggi precedenti per creare una nuova VM, con la differenza che questa volta occorre scaricare dal sito ufficiale di Kali Linux l'immagine ISO o la VM preconfigurata.
- Quando si configura la macchina virtuale, nella sezione Archiviazione, selezionare Scegli un file di disco ottico virtuale e navigare fino all'immagine ISO di Kali Linux scaricata.

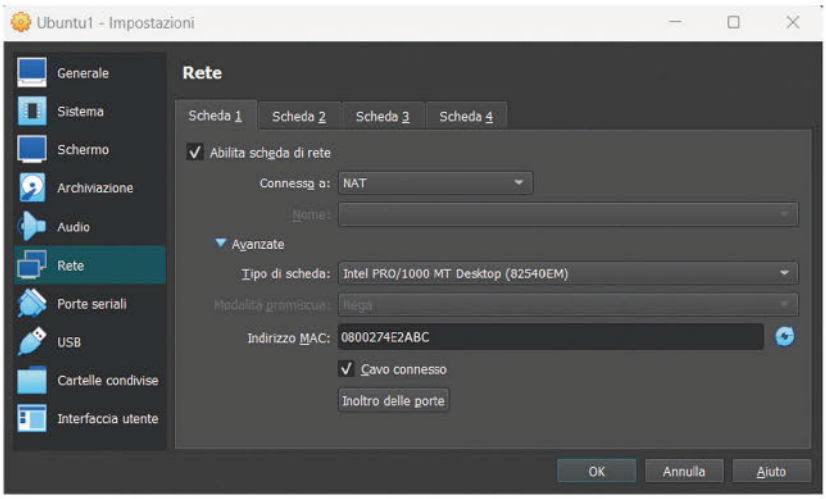
Alla fine di questo processo, si ottiene il sistema mostrato in Figura 1. È sempre possibile verificare e modificare la configurazione della scheda madre, della memoria, del disco e del processore.



← Fig. 1 Il sistema della macchina virtuale con KaliLinux.

Passo 4: configurazione delle schede di rete virtuali

Una scheda di rete virtuale permette alla macchina virtuale di comunicare con altre macchine virtuali e con la rete esterna (si veda l'approfondimento sulla gestione delle reti virtuali). È possibile configurare fino a quattro adattatori di rete per ogni macchina selezionando la casella "Abilita scheda di rete" (Figura 2) e scegliendo dal menu a tendina le diverse opzioni, tra cui NAT per accedere a Internet e "Bridged Adapter", per ottenere un indirizzo IP dalla rete locale, come se fosse un dispositivo fisico collegato ad essa. L'opzione "Avanzate" fornisce ulteriori opzioni, come il tipo di scheda di rete virtuale, ad esempio Intel PRO/1000 MT Desktop, e l'indirizzo MAC virtuale, che è generato dal software e non corrisponde all'indirizzo fisico di una scheda di rete reale. Anche l'indirizzo IP virtuale (VIP) non corrisponde a un'interfaccia di rete fisica. Per vedere l'indirizzo IP assegnato alla macchina virtuale, si può utilizzare, all'interno del sistema operativo ospitato, il classico comando di rete ipconfig per Windows o ifconfig per Linux.



← Fig. 2 le impostazioni della prima scheda di rete virtuale.

Passo 5: utilizzo delle Macchine Virtuali
Una volta installati i sistemi operativi, le VM possono essere avviate separatamente e utilizzate come se fossero computer fisici autonomi. È possibile installare applicazioni, configurare reti virtuali e sperimentare con diversi scenari di utilizzo. Ad esempio, una macchina virtuale con Kali Linux è stata utilizzata nell'attività 5 dell'Unità 3 relativa alla sicurezza informatica per lo scanner delle vulnerabilità.

ATTIVITÀ 2
Creazione di un server per la virtualizzazione con Microsoft Hyper-V

Scenario

Un hypervisor molto diffuso è Microsoft **Hyper-V**. È disponibile una versione autonoma gratuita, chiamata Hyper-V Server 2019, che però dal 2024 non riceverà più aggiornamenti regolari e nuove funzionalità. Hyper-V è un **hypervisor di tipo 1**, cioè un software che si esegue direttamente sull'hardware fisico senza bisogno di un sistema operativo sottostante. Le applicazioni utente vengono eseguite all'interno delle macchine virtuali. Il sistema operativo host, come Windows Server, non esegue direttamente le applicazioni, ma fornisce un'interfaccia per gestire e controllare le macchine virtuali. Hyper-V può ospitare diverse tipologie di macchine virtuali, non solo quelle Microsoft, ma anche varie distribuzioni Linux come Red Hat, CentOS e Ubuntu.

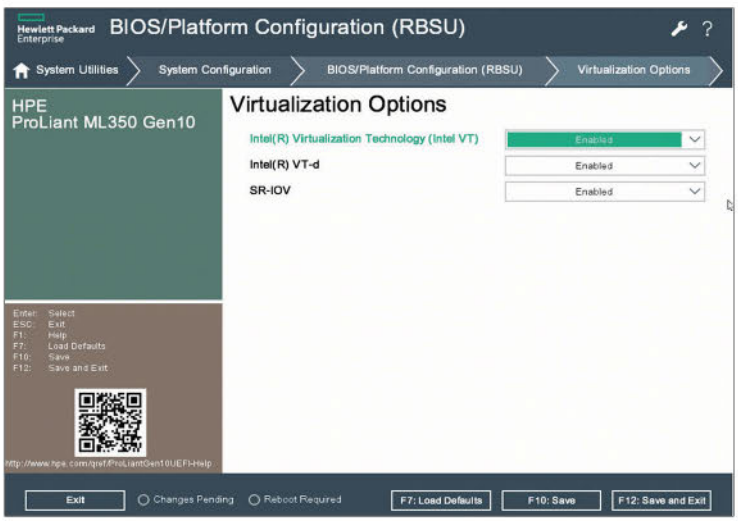
Obiettivo

Attivazione del "ruolo" Hyper-V, per la creazione del server host per la virtualizzazione.

Svolgimento

I passi che seguono spiegano in modo sintetico come attivare il ruolo Hyper-V e creare il server host per la virtualizzazione.

Passo 1
Verifica della disponibilità delle funzioni di virtualizzazione nel BIOS della macchina (Figura 3):

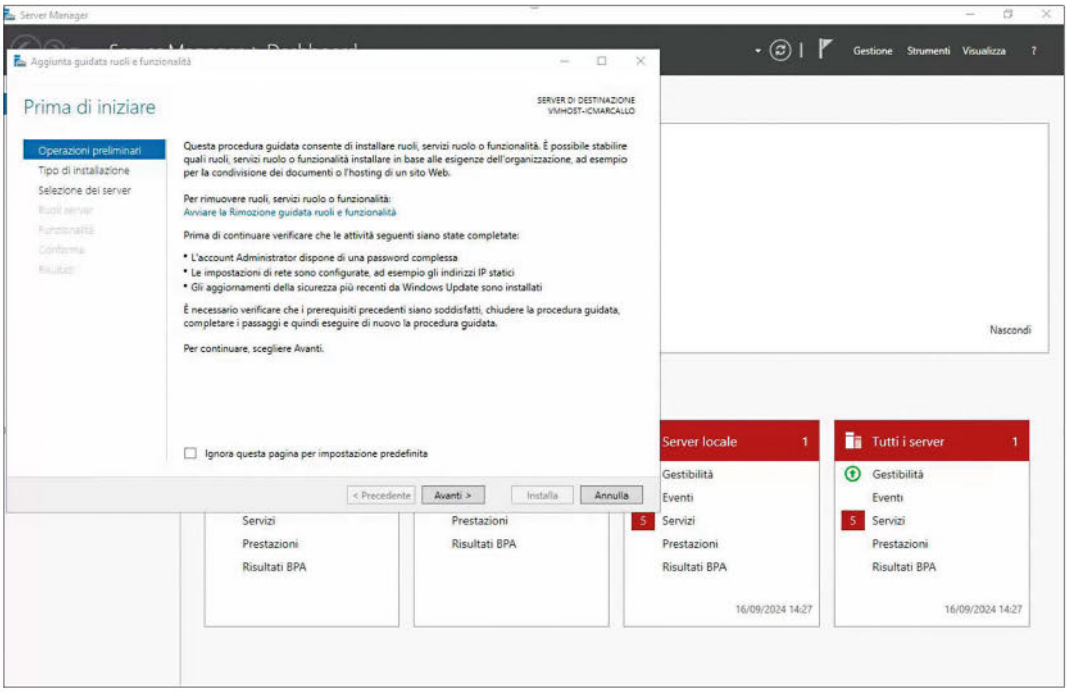


➜ Fig. 3 Opzioni di virtualizzazione nel BIOS della macchina.

Passo 2: inizio della procedura guidata (Figura 4):

- Dopo aver installato il sistema operativo, aprire il Server Manager.
- Cliccare su Aggiungi ruoli e funzionalità per avviare la procedura guidata.

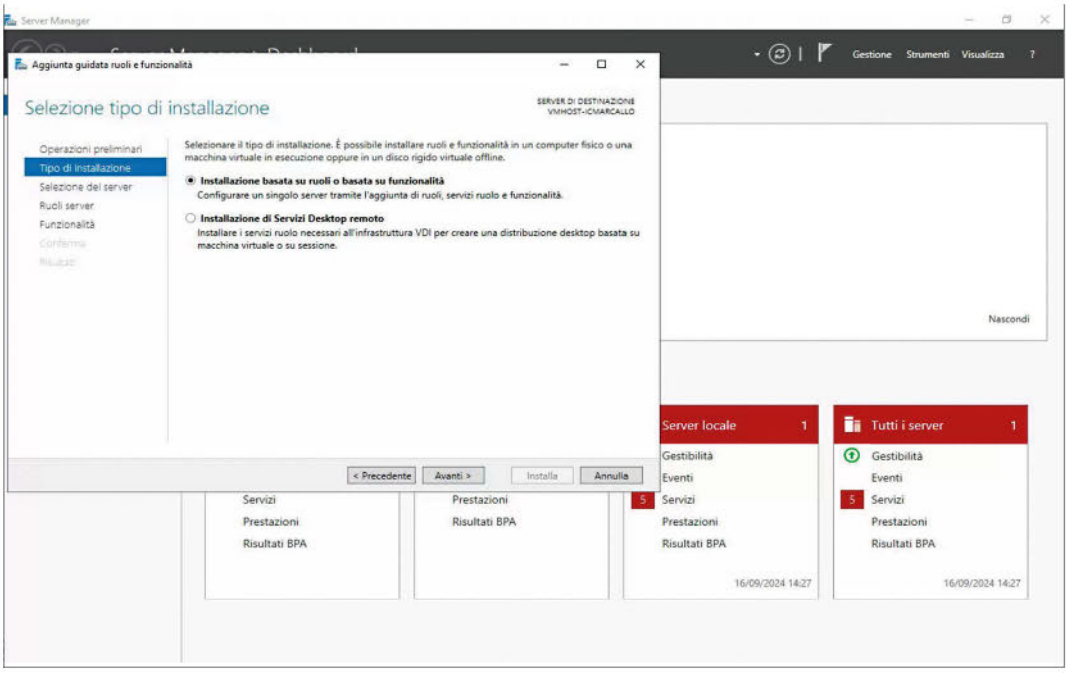
Fig. 4 Inizio della procedura guidata per le operazioni di virtualizzazione.



Passo 3: selezione del tipo di installazione (Figura 5):

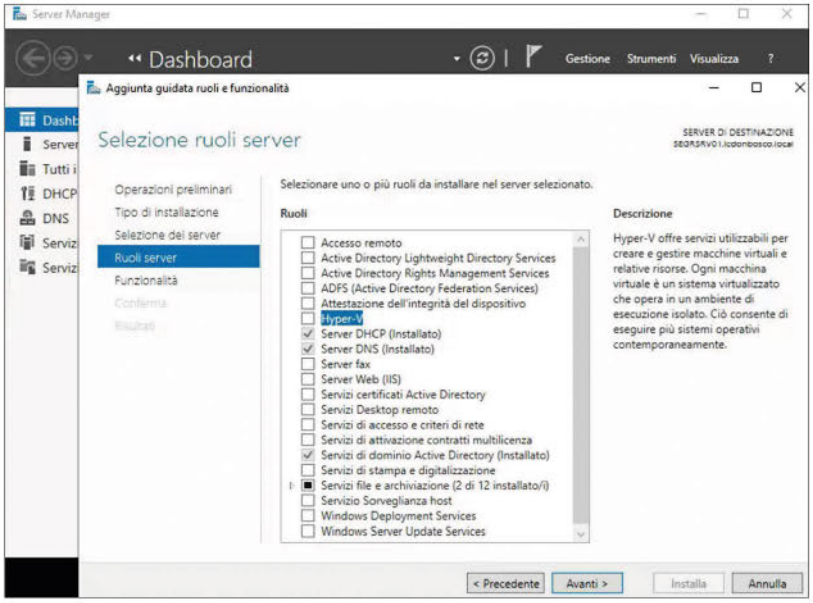
- Selezionare "Installazione basata su ruoli o basata su funzionalità".

Fig. 5 Tipo di installazione.



Passo 4: selezione di Hyper-V (Figura 6)
Nella schermata "Selezione ruoli server", spuntare la casella "Hyper-V"

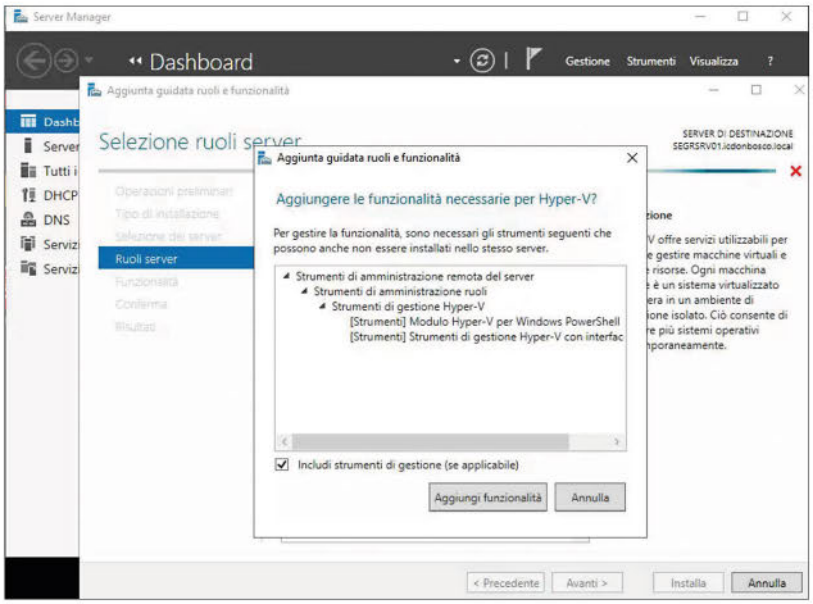
→ Fig. 6 Selezione di Hyper-V.



Passo 5: aggiunta delle funzionalità di gestione del modulo Hyper-V (Figura 7)

- aggiungere le funzionalità necessarie per Hyper-V, cliccando su "Aggiungi funzionalità".
- Procedere con la procedura guidata fino al termine dell'installazione

→ Fig. 7 Aggiungere le funzionalità di gestione del modulo Hyper-V.



notabene

Se al termine delle operazioni compare un errore come quello mostrato accanto, l'hardware utilizzato non è compatibile o non sono state attivate correttamente le opzioni di virtualizzazione all'interno del BIOS.



DATA CENTER
Spazio fisico che ospita le infrastrutture informatiche e tecnologiche di un'azienda

SICUREZZA
Sistemi per garantire riservatezza, integrità e disponibilità dei dati, per il supporto di applicazioni business-critical.

TIPI DI DATA CENTER
- On-premise
- Co-location
- Cloud off-premise

VIRTUALIZZAZIONE
Processo che consente la creazione di più ambienti di elaborazione simulati su un unico sistema fisico. L'hardware è separato dal software.

COMPONENTI/ RISORSE
- Calcolo (Compute)
- Memorie (Storage)
- Rete (Network)

CONTINUITÀ DEL SERVIZIO
È necessaria per garantire la disponibilità dei dati riducendo al minimo le interruzioni dovute a guasti o interventi di manutenzione.

DATA CENTER VIRTUALI
È ospitato presso un fornitore di servizi (off-premise) che gestisce l'infrastruttura e garantisce l'accesso alle risorse tramite connessione Internet.

VIRTUALIZZAZIONE DELLE RISORSE
- Virtual data center manager
- Server virtuali
- Storage virtuale
- Rete virtuale
- Desktop virtuale
- Applicazioni virtuali

VANTAGGI E SVANTAGGI DELLA VIRTUALIZZAZIONE

RAID
Tecnologia usata per garantire l'affidabilità dei dati anche in caso di un guasto a una singola unità disco.
- RAID 1 (mirroring): due dischi fissi, di cui uno è la copia dell'altro.
- RAID 5: utilizzo di tre (o più) unità disco. Il dato è scritto in maniera vettoriale su due unità; si scrive la parità per la rilevazione e correzione degli errori.

CLUSTER DI SERVER
Gruppo di server che lavorano insieme per garantire la disponibilità dei dati e dei servizi.

BACKUP
Copie di salvataggio che permettano il ripristino dei dati in caso di perdite accidentali di informazioni.

CLONAZIONE E TEMPLATE
- Clonazione: tecnica che permette di duplicare una Virtual Machine ottenendone un'altra con la stessa configurazione.
- Template: modello che può essere utilizzato per generare altre macchine simili.

Verifica delle CONOSCENZE

Vero o Falso?

1 La virtualizzazione consente la condivisione delle risorse hardware di un computer. V F

2 La virtualizzazione crea più hardware fisici indipendenti. V F

3 I componenti logici di una macchina virtuale sono indipendenti dall'hardware. V F

4 Un server virtuale è un insieme di file. V F

5 Ogni macchina virtuale ha almeno una CPU fisica propria. V F

6 Hypervisor è il processo che gestisce la virtualizzazione delle risorse. V F

7 Un data center deve assicurare la continuità del servizio. V F

8 Un data center è un database centralizzato. V F

9 Il personale operativo non fa parte di un data center. V F

10 Un virtual data center è pericoloso perché mischia le applicazioni degli utenti. V F

11 Un virtual data center favorisce la scalabilità. V F

12 Un cluster di host aumenta l'affidabilità di un sistema. V F

13 RAID è usato per prevenire guasti sullo storage. V F

14 Un data center di livello 4 garantisce un massimo di 25 ore di fermo macchina all'anno. V F

15 SAN è una rete di storage. V F

16 Un thin client consente di accedere a applicazioni locali. V F

17 Un cluster di server previene fermi macchina. V F

18 Un server flat è adatto a grandi data center. V F

19 Un data center in cloud è più costoso di un data center on-premise. V F

20 Con un data center in cloud si ha un costo fisso per le risorse utilizzate. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

21 Negli ambienti di virtualizzazione il file system, gestito a livello di host fisico:

a deve garantire segretezza, autenticazione e integrità dei dati
b deve essere orientato alla condivisione, permettere l'interfacciamento con l'hypervisor, garantire la sicurezza dei dati e la piena indipendenza fra gli ambienti ospitati
c è più semplice del file system di un ambiente tradizionale perché è essenziale e deve solo garantire l'integrità dei dati
d è inglobato nell'hypervisor

22 Lo storage:

a si basa su sistemi che permettono di configurare volumi di dischi rendendoli disponibili a uno o più host fisici tramite connessioni di rete dedicate
b è connesso direttamente alla macchina, rendendo impossibile la condivisione della memoria di massa tra più sistemi
c utilizza per il collegamento agli host virtuali una rete dedicata
d non necessita di un sistema RAID

23 Una differenza tra SAN e NAS è:

a SAN è una rete dedicata di dischi, NAS è collegato alla LAN
b SAN è una memoria interna, NAS è una memoria esterna
c SAN si usa in cloud, NAS si usa in locale
d SAN può essere virtualizzato, NAS non può essere virtualizzato

24 Un single point of failure è:

a un punto di ripristino
b un nodo della rete
c un elemento di un cluster di host
d un punto critico del sistema

25 Per downtime si intende:

a l'interruzione dell'alimentazione
b la funzione di ripristino del sistema
c l'indisponibilità del servizio
d la funzione di backup di una virtual machine

Domande per la prova orale

26 Che cosa si intende per virtualizzazione?
27 Quali sono i vantaggi della virtualizzazione?
28 Quali sono i requisiti che devono essere rispettati per realizzare la virtualizzazione?
29 Che cosa si intende per RAID?
30 Che cosa si intende per "virtual network"?
31 Che cos'è un data center?
32 Che cosa si intende per business continuity?
33 Che cos'è un Virtual Data Center?
34 Che cosa si intende per single point of failure?
35 Che cosa sono le funzioni di Snapshot e Backup, e come si realizzano?
36 Quali sono le componenti di un data center?
37 Quali sono i tipi di data center?
38 Cosa si intende per business continuity?
39 Quali sono le strategie utilizzate per garantire la continuità del servizio?

Verifica delle ABILITÀ

40 Riporta in una tabella vantaggi e svantaggi relativi all'utilizzo di un data center on-premise rispetto a un data center off-premise.

41 Un'impresa di piccole dimensioni commercializza i propri prodotti artigianali a livello locale. Recentemente l'azienda ha deciso di investire per espandersi a livello internazionale. Elenca quali sono, a tuo avviso, gli elementi base relativi all'infrastruttura tecnologica, utili per supportare il progetto dell'azienda.

42 Elenca i tipici server che sono utilizzati in una rete aziendale, specificando:

a. servizio offerto;
b. collocazione fisica.

43 Fai una ricerca sul Web e rispondi alle seguenti domande:

a. cosa si intende per "data center design"?
b. quali sono i criteri fondamentali da utilizzare per la progettazione di un data center?

- Elabora e sintetizza i risultati ottenuti.
- Interroga l'AI su questo argomento e confronta e valuta i risultati ottenuti con quelli da te precedentemente elaborati.
- Successivamente prepara una presentazione sintetica (massimo 5 slide) corredata di immagini e un breve testo esplicativo per presentare i risultati del tuo studio comprensivi di contenuti e confronti con AI.

44 Fai una ricerca sul Web per cercare i principali fornitori di servizi di data center in cloud e completa una tabella riportando le seguenti informazioni:

Nome	Stato/locazione	Servizi offerti
.....	.....	.....
.....	.....	.....
.....	.....	.....

Esercizi in più

Data center

Abstract

A data center is the part of the company where the IT infrastructure is concentrated. The main resources are the servers for processing, storage for data retention, and the network to connect and enable communication between components and users. A data center can be on-premise (where the company owns and is responsible for everything, including the facilities that host it), co-located (where the company rents space and infrastructure but manages its own resources), or off-premise (virtual data center, where everything is managed by a service provider and resources are accessed via the Internet). Virtualization is a process that enables the creation of multiple simulated computing environments on a single physical system. It optimizes the use of physical resources and is achieved through software called a Virtual Machine Monitor (VMM) or hypervisor. The management of a data center must ensure security in terms of confidentiality, integrity, and availability of data. Service continuity must be guaranteed, preventing downtime and managing possible Single Points of Failure. Solutions include: RAID, VM and storage migration, server clustering, cloning and templates, snapshots, backup, and disaster recovery plans.

Questions

Answer all questions

1 What is a data center?

2 What do we mean by "virtualisation"?

3 What is a hypervisor?

4 What do we mean by "storage virtualisation"?

Choose the correct answer

5 Among the benefits of virtualisation, we have:
- a staff reduction
- b an increase in physical space
- c software sharing
- d hardware sharing

6 The NAS
- a is a virtualised protocol
- b is a hypervisor
- c is a security system
- d enables storage sharing

7 A virtual network
- a is a backup system
- b is a virtual router
- c allows VLAN design
- d is a VPN

8 In a virtual environment
- a each virtual machine can have an operating system that might be different from the one of the host machine
- b the operating system is wired in the hardware
- c the virtual machines' operating system must be the same, but it can differ from the host's one
- d there is no need for an operating system

Crosswords

Across

5 Component of the system for data backup

6 Technique used to ensure storage security

7 Technique used to remotely access virtual applications

8 Critical point of a system

10 Infrastructure for storage with block data transfer

Down

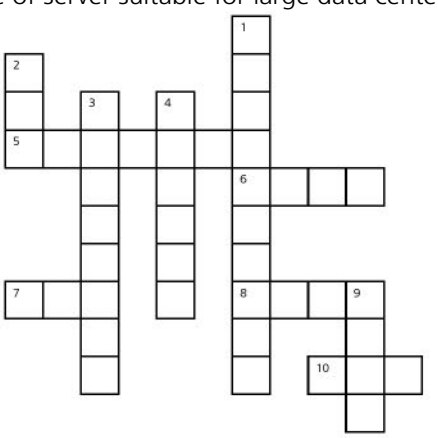
1 Software for managing virtual machines

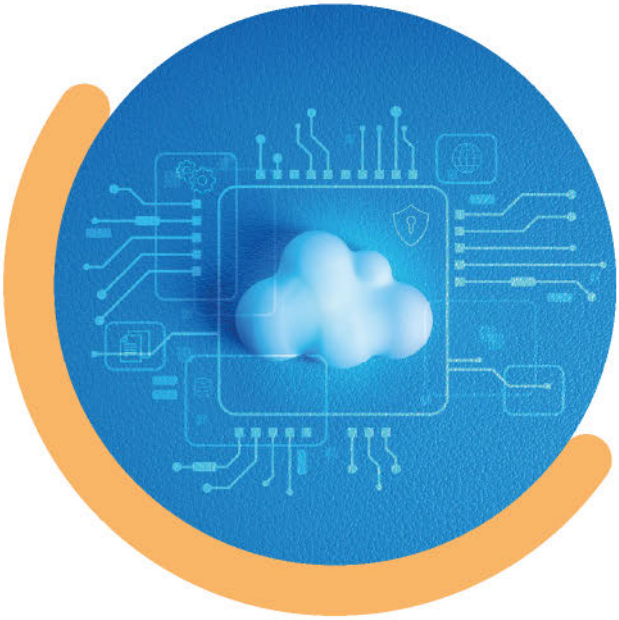
2 Storage devices connected to the LAN

3 Machine inactivity period

4 Data recovery copies

9 Type of server suitable for large data centers

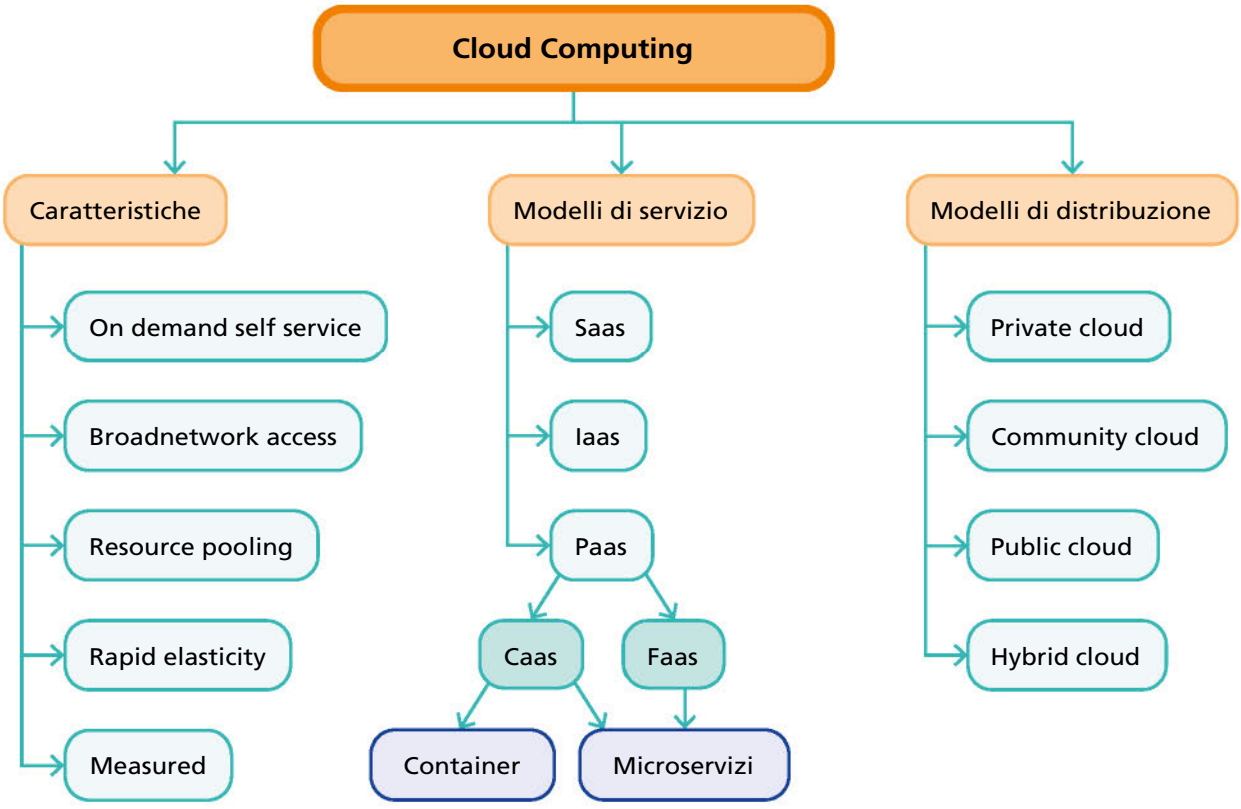




Unità

9

Il Cloud Computing



Visione d'insieme

- Il Cloud Computing e le sue caratteristiche essenziali.
- Modelli di servizio del Cloud Computing.
- Modelli di distribuzione dei servizi in Cloud Computing.

1 Introduzione: un viaggio nel tempo

Nel passato, le organizzazioni e le persone dovevano acquistare e gestire i propri server fisici. Questi server erano collocati in locali dedicati, richiedevano manutenzione costante e spesso rimanevano sottoutilizzati.
Con l'avvento del Cloud Computing tutto è cambiato: le risorse informatiche non sono più legate a un hardware fisico. Immagina un cielo azzurro e terso: il Cloud Computing libera le informazioni dagli spazi limitati e dalle applicazioni che richiedono memoria e aggiornamenti continui, permettendo agli utenti di accedere e utilizzare le risorse tramite Internet.
Il Cloud Computing offre una maggiore potenza di calcolo, le risorse possono essere facilmente scalate in base alle esigenze, gli utenti pagano solo per le risorse effettivamente utilizzate e le applicazioni possono essere eseguite in modo più efficiente.

2 Il Cloud Computing: dal "possesso" al "servizio"

Il Cloud Computing è un modo di utilizzare risorse informatiche, sia hardware sia software (calcolo, storage, rete, servizi, applicazioni), tramite Internet. Utilizzare una risorsa in cloud significa accedere a essa tramite Internet, senza possederla.
È il compimento, nell'ambito della tecnologia, dell'evoluzione che ha condotto alla filosofia "dal possesso al servizio", realizzando modelli di distribuzione di risorse con le seguenti caratteristiche.

- **AS A SERVICE (aaS)**: offre servizi e risorse tramite Internet, consentendo agli utenti di accedere a funzionalità specifiche senza dover gestire l'infrastruttura sottostante.
- **ON DEMAND**: prevede l'accesso immediato alle risorse quando necessario.
- **PAY PER USE**: consente agli utenti di pagare solo per le risorse effettivamente utilizzate.

Pit Stop

1 Che cosa si intende per "Cloud Computing"?

In questo modo non è più necessario installare applicazioni sul proprio computer, non serve avere un ambiente di sviluppo locale e non è più necessario possedere infrastrutture o un data center locale. La gestione delle risorse in cloud è affidata ai fornitori di servizi (provider), che rendono disponibili le risorse necessarie tramite un'interfaccia web e la rete Internet, liberando gli utenti da installazioni, manutenzioni e aggiornamenti.
Il NIST (*National Institute of Standards and Technology*), in un documento ufficiale, ha definito il Cloud Computing come un modello con cinque caratteristiche essenziali, tre modelli di servizio e quattro modelli di distribuzione (Tabella 1).

Pit Stop

2 Come sono organizzati i contenuti del documento del NIST sul Cloud Computing?

Caratteristiche essenziali	Modelli di Servizio	Modelli di Distribuzione
On-demand self-service	SaaS (Software as a Service)	Private cloud (cloud privato)
Broad network access	PaaS (Platform as a Service)	Community cloud (cloud di comunità)
Resource pooling	IaaS (Infrastructure as a Service)	Public cloud (cloud pubblico)
Rapid elasticity		Hybrid cloud (cloud ibrido)
Measured service		

→ Tab. 1 Caratteristiche, modelli di servizio e modelli di distribuzione del Cloud Computing.

3 Caratteristiche essenziali

Le caratteristiche essenziali sono fondamentali per i servizi in cloud. Esse mirano a favorire flessibilità e scalabilità, riducendo i costi e gli spazi. Vedremo come queste caratteristiche siano alla base dei modelli di servizi AS A SERVICE, ON DEMAND e PAY PER USE, che abbiamo anticipato nella precedente unità come ultima fase dell'evoluzione dei data center che si completa con i servizi di Cloud Computing.

- **On-demand self-service**. Un utente può accedere autonomamente ai servizi offerti da un fornitore (capacità di elaborazione e storage) senza la necessità di un intervento umano dei gestori (AS A SERVICE).
- **Broad network access**. Le funzionalità devono essere disponibili in rete e accessibili tramite dispositivi standard, come telefoni cellulari, tablet, computer portatili e workstation.
- **Resource pooling**. Le risorse fornite, sia fisiche sia virtuali (larghezza di banda, potenza di calcolo, applicazioni), sono raggruppate e organizzate in "multi tenancy" per essere disponibili per più consumatori. Le risorse vengono assegnate e riassegnate dinamicamente in base alla domanda dei consumatori, indipendentemente dal luogo fisico in cui si trovano.
- **Rapid elasticity**. Le risorse possono essere assegnate e rilasciate elasticamente e rapidamente in base alle necessità (ON DEMAND). L'utente ha la sensazione di disporre di capacità illimitate che possono essere assegnate in qualsiasi momento.
- **Measured service**. Ogni servizio utilizzato deve poter essere misurato e controllato in modo trasparente; ciò permette di ottimizzarne l'uso e calcolare i consumi per poter pagare solo quello che si usa (PAY PER USE).

notabene

La multi tenancy consente a più clienti di un fornitore cloud di utilizzare le stesse risorse di elaborazione, pur mantenendo i loro dati completamente separati. Ogni cliente opera come se avesse risorse dedicate, anche se in realtà sono condivise. È una componente determinante del Cloud.

Pit Stop

3 Quali sono le 5 caratteristiche essenziali del Cloud Computing?

4 Modelli di Servizio

Il documento del NIST definisce tre modelli base di servizio, che rappresentano i modi in cui il Cloud può essere utilizzato, corrispondenti al tipo di servizi forniti dal provider. Essi si differenziano per il tipo di risorse rese disponibili. Analizziamo i tre modelli.

1. **Software as a Service** (**SaaS**). Consiste nella distribuzione di applicazioni software tramite Internet. Il software delle applicazioni, i dati e tutta l'infrastruttura sottostante sono nel data center del provider, che gestisce l'hardware e il software, garantendo la disponibilità e la sicurezza delle applicazioni. Il consumatore non gestisce né controlla l'infrastruttura. Le applicazioni sono accessibili da vari dispositivi client tramite un'interfaccia thin client, come un browser web. I prodotti SaaS sono sempre pronti all'uso, con aggiornamenti, correzioni e manutenzione.
2. **Platform as a Service** (**PaaS**). Consiste nella distribuzione di applicazioni create dal consumatore utilizzando un ambiente di sviluppo (linguaggi di programmazione, librerie, servizi e strumenti) del fornitore. Il consumatore non gestisce né controlla l'infrastruttura cloud sottostante, inclusa la rete, i server, i sistemi operativi o lo storage, ma ha il controllo sulle applicazioni distribuite e sulle impostazioni di configurazione per l'ambiente di hosting delle applicazioni. I servizi offerti spaziano dagli strumenti di gestione ai database, fino a dare accesso, tramite API, a librerie di Intelligenza Artificiale. Una soluzione PaaS supporta il ciclo di vita completo delle applicazioni web: creazione, test, distribuzione, gestione e aggiornamento. PaaS consente di sviluppare applicazioni personalizzate senza dover avviare e mantenere

notabene

Il middleware è un software posto tra il sistema operativo e le applicazioni e ha un ruolo di intermediario per le applicazioni distribuite in rete.

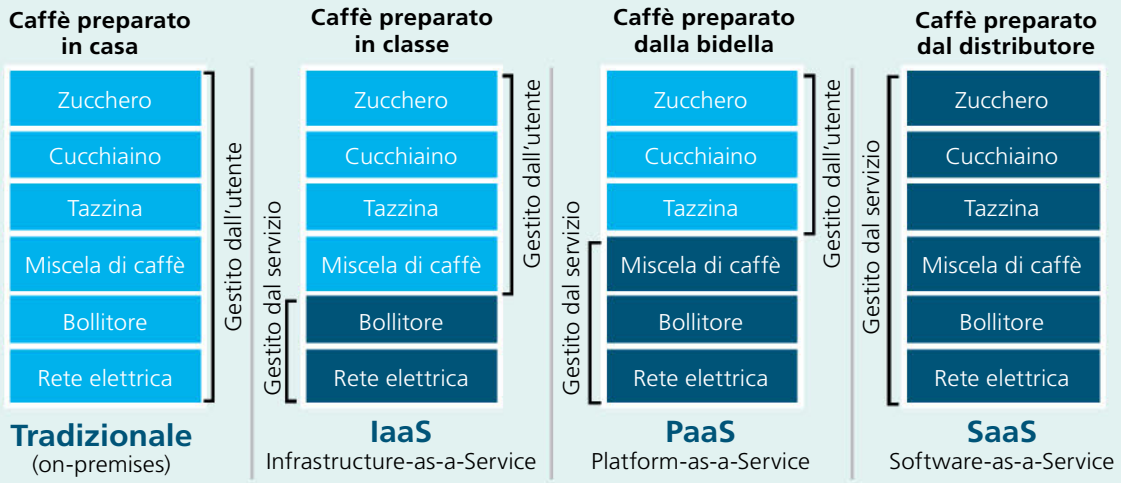
tutti i sistemi necessari per supportare l'ambiente di sviluppo. Gli sviluppatori possono utilizzare componenti software preesistenti per creare le loro applicazioni, come mattoncini per costruire un edificio, in modo rapido ed efficiente. Il modello PaaS consente di evitare le spese e la complessità legate all'acquisto e alla gestione di licenze software, middleware o strumenti di sviluppo e altre risorse. Il cliente gestisce le applicazioni e i servizi che sviluppa, mentre il provider è responsabile di tutto il resto.

3. **Infrastructure as a Service** (**IaaS**). Consiste nella distribuzione di capacità computazionale (risorse di calcolo), archiviazione, reti e altre risorse informatiche. Il consumatore non gestisce né controlla l'infrastruttura fisica cloud sottostante, ma ha il controllo sui sistemi operativi, sullo storage e sulle applicazioni distribuite. Il cliente può ottenere intere macchine virtuali comprensive di sistemi di storage e componenti di rete, per poter autonomamente erogare le proprie applicazioni e i propri servizi.

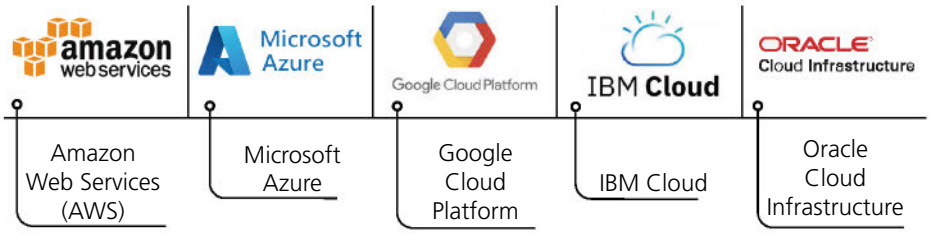
Comprendi con l'analogia

I Servizi di Cloud Computing (*Tradizionale*, *IaaS*, *PaaS*, *SaaS*) sono come le modalità di preparazione del caffè

Lo schema mostra differenti modalità di preparazione del caffè, che possono essere paragonate ai modelli di servizio del Cloud Computing.



- **Caffè preparato in casa** (**Tradizionale**). Ogni passaggio del processo di lavorazione è eseguito autonomamente. L'utente gestisce tutto, dalla scelta dei chicchi di caffè alla preparazione e pulizia della macchina. Questo è paragonabile alla gestione on-premises, dove l'utente è responsabile di tutta l'infrastruttura.
- **Caffè preparato in classe** (**IaaS**). Si sfrutta la rete elettrica e il bollitore della scuola. L'utente porta solo la miscela di caffè e l'acqua. Questo è analogo a Infrastructure-as-a-Service, dove il provider fornisce l'infrastruttura di base (rete, server, storage) e l'utente gestisce il sistema operativo e le applicazioni.
- **Caffè preparato da un volontario** (**PaaS**). Un volontario si offre per aggiungere la miscela di caffè e l'acqua, utilizzando il bollitore della scuola. L'utente deve solo scegliere il tipo di caffè. Questo è paragonabile a Platform-as-a-Service, dove il provider gestisce l'infrastruttura e l'ambiente di sviluppo, mentre l'utente sviluppa e gestisce le applicazioni.
- **Caffè preparato dal distributore automatico** (**SaaS**). Il distributore automatico provvede a tutto il necessario per la preparazione e il servizio del caffè. L'utente deve solo premere un pulsante per ottenere il caffè. Questo è simile a Software-as-a-Service, dove il provider gestisce tutto, dall'infrastruttura alle applicazioni, e l'utente accede al servizio tramite un'interfaccia.



← Fig. 1

In Figura 1 sono indicati alcuni fornitori di servizi in Cloud Computing disponibili sul mercato.

I tre modelli di servizio appena descritti sono quelli presenti nel documento ufficiale del NIST scritto nel 2011. Da allora, il Cloud Computing ha fatto un passo avanti consentendo agli sviluppatori di disporre di strumenti sempre più potenti e flessibili. Per questo motivo, come ulteriore evoluzione del PaaS, che ha posto le basi per lo sviluppo di applicazioni cloud, si sono affermati altri due modelli di servizio.

- **Container as a Service** (**CaaS**): si concentra sulla gestione di container, pacchetti software autonomi che contengono tutto il necessario per eseguire un'applicazione. CaaS offre maggiore flessibilità e scalabilità.
- **Functions as a Service** (**FaaS**): è un alto livello che consente di eseguire solo piccole porzioni di codice (funzioni) senza preoccuparsi dell'infrastruttura sottostante e della gestione dei server.

CaaS e FaaS offrono un livello di granularità più fine rispetto al PaaS e sono particolarmente utili per sviluppare applicazioni basate su microservizi cioè su piccole unità di codice indipendenti che comunicano tra loro.
Ogni modello di servizio implica un diverso livello di gestione da parte del cliente e del fornitore, come è mostrato nella Figura 2.

Pit Stop

4 Quali sono i tre modelli di servizio del Cloud Computing?

5 Che cosa si intende per SaaS?

6 Che cosa si intende per PaaS?

7 Che cosa si intende per IaaS?

On-Premise *Tradizionale*	IaaS *Infrastructure-as-a-Service*	CaaS *Container-as-a-Service*	PaaS *Platform-as-a-Service*	FaaS *Functions-as-a-Service*	SaaS *Software-as-a-Service*
Applications	Applications	Applications	Applications	Applications	Applications
Data	Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking	Networking
Gestito dall'Utente			Gestito dal servizio Cloud		

← Fig. 2 I modelli di servizio cloud a confronto con il modello tradizionale.

5 Container e microservizi

I container raggruppano un'applicazione con tutti i file necessari per la sua esecuzione (dipendenze) in un unico ambiente di esecuzione. Un container può essere facilmente spostato ed eseguito ovunque su qualsiasi sistema: da un data center privato al cloud pubblico o anche sul computer di uno sviluppatore.
I container occupano poco spazio di memoria, possono essere eseguiti in qualunque momento e velocemente in qualsiasi ambiente e rendono le applicazioni autosufficienti.
I container favoriscono lo sviluppo di applicazioni basate su microservizi e **rappresentano un nuovo modo di progettare il software, diverso da quello tradizionale**. Occorre distinguere tra container e microservizi.

- **Microservizi**. Come abbiamo introdotto nell'unità 1, i microservizi sono funzioni autonome e indipendenti, utilizzate in rete, che possono essere combinate per comporre un'applicazione più complessa. Per utilizzare i microservizi si utilizzano le API (Application Programming Interface).
- **Container**. I container sono ambienti di sviluppo virtuali che consentono di eseguire i microservizi stessi, fornendo le risorse necessarie per la loro esecuzione.

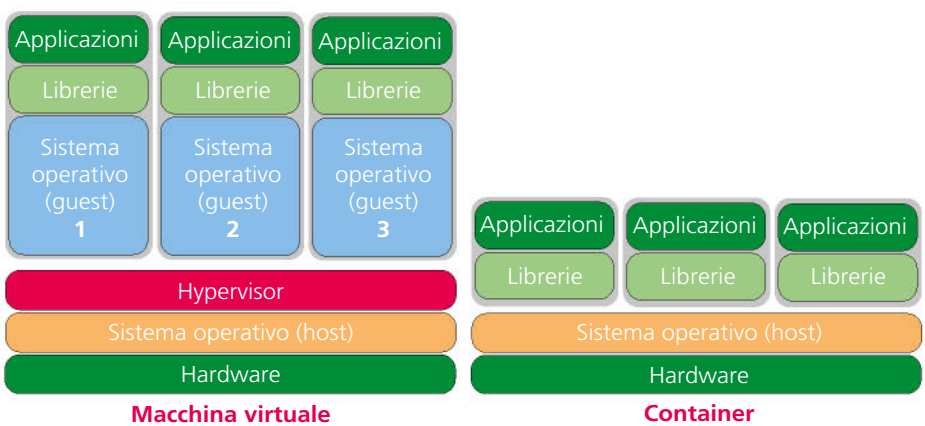
Pit Stop

8 Che cosa sono i container?

9 Che cosa si intende per "microservizio"?

Consideriamo la prenotazione online di una camera di un hotel, come esempio di architettura di un'applicazione scomposta in più microservizi. Un primo servizio è quello fornito dagli algoritmi di ricerca che vengono effettuati per individuare l'hotel, la città e l'eventuale data di arrivo e partenza. Un altro servizio è quello che, in tempo reale, ci segnala i feedback dei clienti e ci propone offerte che sono simili alle nostre richieste, oppure ci suggerisce prodotti correlati con le nostre ricerche. Questi servizi sono basati su un database di preferenze dei clienti e, spesso, sfruttano algoritmi di Intelligenza Artificiale per dare suggerimenti mirati. Infine, il pagamento è un servizio a parte in cui la sicurezza gioca un ruolo fondamentale.

La tecnologia dei container consente di eseguire applicazioni utilizzando un metodo di virtualizzazione alternativo rispetto alle macchine virtuali tradizionali. Invece di virtualizzare l'hardware, i container garantiscono l'isolamento delle applicazioni anche se molte di esse sono in esecuzione sulla stessa macchina fisica o virtuale. Questo approccio rende efficiente l'utilizzo delle risorse di elaborazione, storage e rete.



→ **Fig. 3** Macchina virtuale e Container. La macchina virtuale virtualizza l'intero hardware e i container sfruttano il sistema operativo della macchina su cui sono ospitati per isolare ed eseguire le singole applicazioni.

Diversamente dai modelli IaaS e PaaS, **i container non si basano su hypervisor**, ma sfruttano il sistema operativo delle macchine ospitanti per isolare l'esecuzione dei singoli processi. Un container può essere visto come un "pacchetto software" che contiene l'applicazione, il codice sorgente, le librerie e le dipendenze necessarie per l'esecuzione in un ambiente isolato (Figura 3).
La separazione tra applicazione e ambiente di esecuzione runtime facilita lo sviluppo e il rilascio delle applicazioni basate su container, indipendentemente dall'ambiente di destinazione (locale, data center privato o pubblico). Questa tecnica aiuta anche a separare i compiti tra sistemisti e sviluppatori e permette di inglobare i microservizi.
L'applicazione "pacchettizzata" è accompagnata da un file "manifest" che contiene le metainformazioni descrittive e informa il sistema operativo su come gestire l'avvio dell'applicazione.

La gestione dei container è supportata da ambienti come Docker e Kubernetes.

- **Docker** è una piattaforma usata dagli sviluppatori per progettare, testare e distribuire applicazioni utilizzando container, offrendo un modo semplice per separare le applicazioni dall'infrastruttura.
- **Kubernetes** è un software di gestione di applicazioni containerizzate.

A titolo di esempio mostriamo la creazione di un programma in Python che stampa "ciao" e il suo inserimento in un container Docker.

notabene

Assicurarsi di avere Docker installato o scaricarlo e installarlo dal sito ufficiale di Docker.

Comprendi con l'analogia

I container virtuali sono come i container fisici

Era un giorno del 1956. Malcolm McLean, un imprenditore americano che, da inizi modesti, aveva accumulato una certa fortuna nel campo dei trasporti, sedeva annoiato aspettando che la merce nei suoi camion fosse stivata sulla nave. Guardando lavorare gli scaricatori, fu colpito da un'idea tanto semplice quanto geniale: invece di scaricare i camion e collocarne il contenuto nella stiva, sarebbe stato meglio spostare sulla nave il cassone stesso con tutto il suo carico. Erano nati i container e la containerizzazione che permette non solo di ridurre gli ingombri e velocizzare le operazioni di imbarco e sbarco, ma di caricare le merci e non doverle più movimentare sino a destinazione, passando anche attraverso vettori di trasporto diversi.
L'idea del container software, ripresa cinquant'anni dopo, mantiene alcune caratteristiche dei container tradizionali: la granularità, l'isolamento e la possibilità di essere trasferiti su piattaforme diverse conservandone la natura originale.



I docker (scaricatori), sotto la supervisione di ingegneri, effettuano la movimentazione efficiente dei container.

Esempio 1

- Creazione del file Python 'hello.py', nella cartella di lavoro C:\app

```
# Python
print("ciao")
```

- Creazione del file di testo "dockerfile", editato senza estensione, nella stessa cartella, che contiene i comandi necessari a Docker per eseguire il file Python:

```
# immagine di base di Python
FROM python:3.8-slim-buster
# Imposta la directory di lavoro
WORKDIR /app
# Copia il file Python nella directory di lavoro
COPY hello.py .
# comando di avvio
CMD ["python","hello.py"]
```

- Costruzione dell'immagine Docker "hello-python"

```
C:\app>docker build -t hello-python .
[+] Building 17.6s (8/8) FINISHED
                                    docker:desktop-linux
```

- Visualizzazione del contenuto della cartella di lavoro

```
C:\app>dir
```

Il volume nell'unità C è Windows

```
30/08/2024  16:31        262 dockerfile
30/08/2024  16:03         14 hello.py
```

- Esecuzione:

```
C:\app>docker run hello-python
ciao
```

- Salvataggio dell'immagine in un file compresso

```
C:\app>docker save -o hello-python.tar hello-python
```

Ciò serve, eventualmente, per trasferire l'immagine Docker su un'altra macchina.

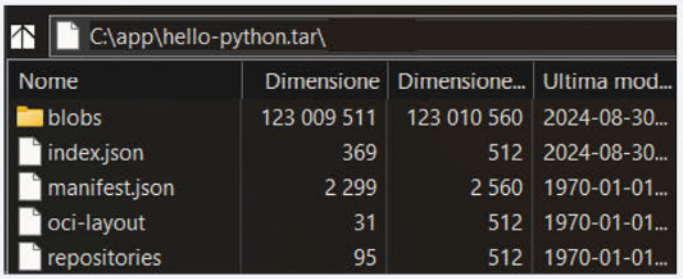
- Visualizzazione del contenuto della cartella di lavoro e del file compresso, come mostrato in figura

```
C:\app>dir
Directory di C:\app
```

notabene

Un'immagine Docker è un file che contiene tutto il necessario per la creazione di un container, tra cui il sistema operativo da utilizzare, le librerie, i file di configurazione, le interfacce utente e i comandi necessari per eseguire il container.

```
30/08/2024  16:31         262 dockerfile
30/08/2024  17:17     123.026.944 hello-python.tar
30/08/2024  16:03          14 hello.py
```



6 Modelli di distribuzione

NIST propone i quattro modelli di distribuzione del Cloud, descritti in Tabella 2. ↓Tab. 2

Modello di distribuzione del Cloud	Vantaggi
1. Private Cloud L'infrastruttura cloud è fornita a uso esclusivo di una singola organizzazione. L'infrastruttura può essere di proprietà dell'organizzazione, di un provider o di entrambi e può trovarsi dentro o fuori la sede aziendale.	• Controllo dell'infrastruttura e dei dati. • Maggiore sicurezza, perché le risorse non sono condivise con utenti esterni. • Personalizzazione dell'ambiente per soddisfare precise esigenze aziendali. • Scalabilità paragonabile a quella di un cloud pubblico.
2. Community Cloud L'infrastruttura cloud è fornita a uso esclusivo di una specifica comunità di consumatori che condividono degli interessi, per esempio la stessa politica aziendale o specifici requisiti di sicurezza. L'infrastruttura può essere di proprietà dell'organizzazione, di un provider o di entrambi e può trovarsi dentro o fuori la sede aziendale.	• Vantaggi del cloud privato con l'aggiunta della possibilità di gestire esigenze specifiche di un'utenza specializzata che ha propri vincoli e caratteristiche.
3. Public cloud L'infrastruttura cloud è predisposta per l'uso pubblico. L'infrastruttura è nella sede del provider che gestisce e rende disponibili, tramite Internet, le risorse di elaborazione e archiviazione. L'utente non ha il controllo dei dati.	• Facile accessibilità a tutti gli utenti con costi ridotti: non si devono acquistare spazi fisici, hardware o licenze software e si paga solo per i servizi usati. • Mancanza di spese di manutenzione o di formazione del personale, che sono a carico del provider. • Scalabilità, con la possibilità di ottenere risorse on-demand per tutte le esigenze aziendali. • Affidabilità elevata e garanzia della continuità del servizio.
4. Hybrid cloud Combina le risorse di cloud pubblici e privati. È una soluzione molto diffusa, perché consente di non fare affidamento interamente su un unico cloud pubblico. Molte aziende si stanno orientando verso una soluzione ibrida, soprattutto perché è possibile mantenere la parte di informazioni strategiche all'interno, lasciando all'esterno le attività ritenute meno critiche.	• Controllo delle infrastrutture e della sicurezza, come nel cloud privato. • Flessibilità nell'utilizzo delle risorse con la possibilità di ottenerne altre dal cloud pubblico in caso di necessità. • Gradualità: la migrazione da privato a pubblico può essere fatta in modo graduale e semplice. • Convenienza che discende dalla flessibilità. Si può aggiungere, e pagare, potenza di calcolo solo quando necessario.

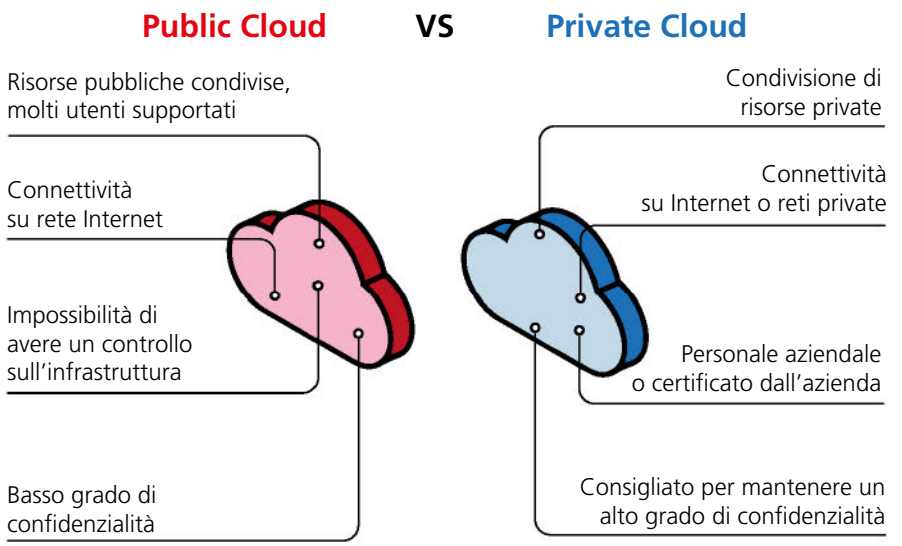
Pit Stop

10 Quali sono i modelli di distribuzione dei servizi in Cloud Computing?

Vediamo ora alcuni esempi di utilizzo dei modelli di distribuzione.

- **Cloud pubblico**. Si può usare il cloud pubblico quando si hanno esigenze che non richiedono risorse particolari o critiche e si vogliono ridurre i costi iniziali, pagando solo per le risorse effettivamente utilizzate.
- **Cloud privato**. È preferibile utilizzare il cloud privato per operazioni critiche come il trattamento di dati sensibili o operazioni finanziarie.
- **Cloud ibrido**. Un esempio interessante consiste nel mantenere un cloud privato per la normale gestione delle applicazioni e passare a un cloud pubblico in momenti critici particolari, come durante picchi di accesso alle applicazioni (ad esempio, nel corso delle vendite in particolari momenti dell'anno).
- **Multi-cloud**. Un'azienda, per motivi economici o per evitare la dipendenza da un singolo ente, potrebbe scegliere una soluzione multi-cloud, utilizzando più cloud pubblici di fornitori diversi. Anche in questo caso è possibile combinare il cloud privato con il cloud pubblico per raggiungere la massima flessibilità. Tuttavia, la migrazione da un cloud a un altro deve essere affrontata con prudenza, poiché le tecnologie utilizzate dai service provider possono differire.

La Figura 4 confronta il cloud pubblico e il cloud privato, evidenziando le principali caratteristiche.



➜ **Fig. 4** Confronto tra le caratteristiche salienti del cloud pubblico e privato.

Approfondimento - Tecnologia 1

I container e la loro gestione automatizzata

I container sono utili per eseguire in modo più efficiente le nostre applicazioni, possibilmente organizzate e strutturate in microservizi. Quale meccanismo rende fattibile tutto ciò? Chi fa partire un container, chi lo duplica per esigenze di scalabilità, chi lo riavvia se si ferma?
Nasce da queste domande il concetto di **Containers Orchestrator**, un sistema software che organizza e rende robusto e funzionante questo processo, garantendo sicurezza, prestazioni e ottimizzazione. Riassumiamone i concetti principali.

- Un **container** è la copia in esecuzione di una "container image" conservata in un repository di immagini.
- Un **container** è eseguito all'interno di un **POD** (eventualmente da solo o insieme ad altri container).
- Il **POD** è la più piccola unità di orchestrazione (quindi soggetta a monitoraggio, riavvio, scalabilità...).
- I **POD** sono allocati in **Worker Nodes**.
- I **Worker Nodes** rappresentano le risorse di elaborazione che vogliamo dare alla nostra architettura. Potremmo avere cluster con un numero piccolo o grande di Worker Nodes.
- Un **cluster** è la nostra architettura, contenente il nostro sistema nei Worker Nodes e che usa altri tipi di Nodi (Boot, Management, Master, Vulnerability Advisor ecc.).

Esempi di orchestratori di container sono **Kubernetes**, open source ideato da Google, e **OpenShift** di RedHat, basato anch'esso su Kubernetes.
Cluster piccoli con pochi Worker Nodes (almeno uno) serviranno per sistemi semplici, mentre cluster con molti Worker Nodes potranno gestire milioni di utenti contemporaneamente. Possono essere creati cluster di qualsiasi dimensione per adattarli a esigenze specifiche.

Docker

Per pacchettizzare e distribuire un'applicazione tramite container, si possono sfruttare strumenti che, come Docker, permettono la creazione, la distribuzione, la condivisione e l'esecuzione di container. Docker è un progetto open source che include tutto il necessario per creare ed eseguire i container (codice, runtime, l'ambiente di esecuzione necessario per far funzionare i container, strumenti di sistema, librerie di sistema e impostazioni), a partire da un formato standard interoperabile, in modo da pacchettizzare le applicazioni ed eseguirle all'interno di qualsiasi ambiente operativo (Figura 1). Docker è diventato di fatto uno standard per la containerizzazione, supportato da una vasta comunità e da numerosi strumenti complementari che ne facilitano e rendono efficiente l'uso.

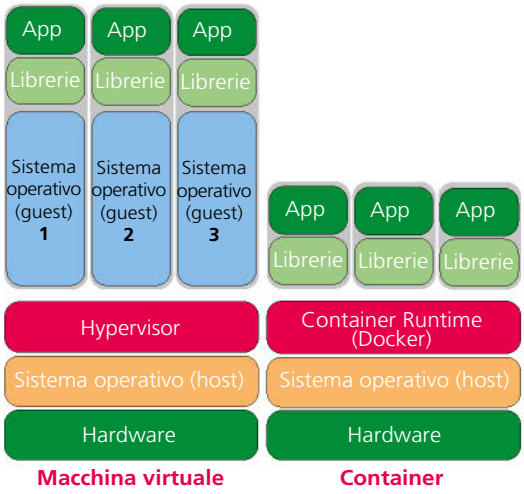


Fig. 1 **Docker** si basa su **LXC** (Linux Containers), un ambiente di virtualizzazione che opera a livello del sistema operativo e permette di eseguire diversi ambienti container isolati tra loro su una singola macchina reale avente il kernel Linux. Docker si serve di un motore software (Docker Engine) per mandare in esecuzione il codice del container a prescindere dall'infrastruttura isolando il software dall'ambiente di esecuzione e rendendolo indipendente dal sistema operativo.

Kubernetes

Con l'aumentare del numero dei container, è necessario dotarsi di strumenti di controllo per rendere efficiente la loro gestione.
Nasce così l'idea di **container orchestration**, di cui Kubernetes, un sistema open source sviluppato originariamente dal team di Google, è un esempio di spicco.
Il suo scopo è quello di automatizzare i processi manuali, come controllare le risorse del server, monitorare l'avvio e l'esecuzione dei processi e controllarne le dipendenze.
Kubernetes permette di distribuire e bilanciare i carichi di lavoro e interagire con più container contemporaneamente, raggruppando i container in pod, condividerne le immagini e fornire funzionalità di storage e di rete ridondanti in modo da ridurre il rischio di fermo macchina.

Approfondimento - Storia



La pietra miliare è un cippo, posto sul ciglio delle strade, utilizzato per stabilire le distanze stradali. Nell'antica Roma le distanze, in miglia, venivano calcolate a partire dal miliarium aureum, una colonna in marmo rivestita di bronzo dorato fatta innalzare nel Foro romano da Augusto nel 20 a.C.

Le pietre miliari del Cloud Computing

Le radici del Cloud Computing affondano nella ragione stessa dell'esistenza di Internet e del Web: la condivisione e l'utilizzo remoto delle risorse e delle informazioni. Ci sono tuttavia delle date precise, pietre miliari sulla strada del cloud, che ne hanno segnato lo sviluppo.

Anno	Evento
1995	L'Unione europea emana la direttiva sulla protezione dei dati che disciplina il trattamento dei dati personali al suo interno. Si tratta di un primo contributo importante per la tutela della vita privata e dei diritti umani.
1998	Il "Data Protection Act", in Inghilterra, pone le basi legali della manipolazione e memorizzazione dei dati.
1999	Nasce la prima piattaforma per l'accesso a servizi online.
2002	Amazon lancia la prima infrastruttura web con i servizi in cloud.
2006	Amazon sviluppa "Elastic Compute Cloud, EC2" per permettere agli utenti di usare (e pagare) esclusivamente i servizi ritagliati su misura.
2008	Google propone Google Apps per l'incremento della produttività.
2009	Microsoft, con Windows Azure, permette agli utenti di costruire e offrire le proprie applicazioni nel cloud.
2012	La Commissione europea prevede di unificare la protezione dei dati all'interno dell'Unione europea con una sola legge: il "regolamento generale sulla protezione dei dati (GDPR)".
2013	Docker introduce il software open source per container.

Laboratorio

Le esercitazioni che seguono si basano sull'utilizzo di **IBM Cloud Platform**, la piattaforma cloud messa a disposizione da IBM.
La piattaforma fornisce agli utenti l'opportunità di creare un proprio datacenter in cloud, con macchine fisiche e virtuali e altri componenti infrastrutturali e installare il proprio software sfruttando i molteplici servizi presenti sulla piattaforma (intelligenza artificiale, networking, sicurezza, IoT ecc.). È basata, in gran parte, su soluzioni open source, e consente la portabilità delle applicazioni in container.
L'esecuzione pratica di queste esercitazioni presuppone la registrazione a IBM Cloud Platform (cloud.ibm.com) per l'ottenimento di un account gratuito di tipo "lite" a tempo indeterminato. Questo permette l'utilizzo immediato di tutti i servizi contrassegnati con la label "lite" presenti nel catalogo.
Obiettivo delle esercitazioni è quello di mostrare e sperimentare servizi in cloud (PaaS e IaaS) per capire meglio quanto detto in questa unità, in un reale ambiente professionale.
I casi di studio presi in esame sono i seguenti (alcuni sono reperibili tra le risorse on line).

- Attività 1: Introduzione all'utilizzo della IBM Cloud Platform.
- Attività 2: Creazione di un programma in Java e sua esecuzione in cloud.
- Attività 3: Creazione di un cluster Kubernetes e deploy di un'applicazione containerizzata.
- Attività 4: Introduzione e utilizzo delle Function Serverless.
- Attività 5: Creazione di un'applicazione mobile (Android o iOS) per l'accesso a un Data Base in cloud.

ATTIVITÀ 1

Introduzione all'utilizzo della IBM Cloud Platform

Approfondimento
Modelli di sviluppo del codice in Cloud

Scenario

Dopo essersi registrati, collegarsi alla piattaforma https://cloud.ibm.com/.

Consegna

Esplorare il menu della piattaforma IBM Cloud Platform.

Svolgimento

Di seguito esploriamo sinteticamente il menu principale (Figura 1).
Il *Catalogo* (*Catalog*) presenta i servizi offerti in piattaforma. (Figura 2).
La voce *Gestisci* (*Manage*) offre informazioni per poter procedere alla fruizione della piattaforma in modo efficace. In particolare si ponga attenzione su *Account* → *CloudFoundry Organization* (Organizzazioni) (Figura 3).



Fig. 1 Il menu con i servizi di IBM Cloud Platform.

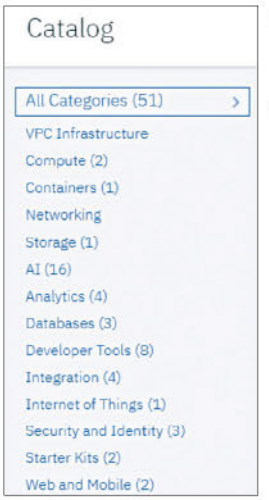


Fig. 2 Parte del menu Catalogo.

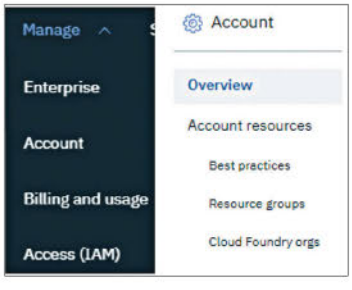


Fig. 3 Menu Manage → Account.

Le *Organizzazioni* sono il criterio di base con cui organizzare i propri progetti. È necessario crearne almeno una prima di iniziare a lavorare.
All'interno delle Organizzazioni possono essere creati uno o più **Spazi** (Space). Normalmente si usano i nomi convenzionali *DEV* e *PROD* per riferirsi, rispettivamente, agli spazi software di sviluppo e a quelli di produzione. Per la nostra esercitazione sarà sufficiente un solo spazio, tipicamente chiamato DEV o con un altro nome a scelta (Figura 4).
La *Dashboard* (da menu a sandwich, tre lineette) (Figura 5a e 5b) permette di visualizzare le proprie risorse e controllare le proprie applicazioni e servizi.

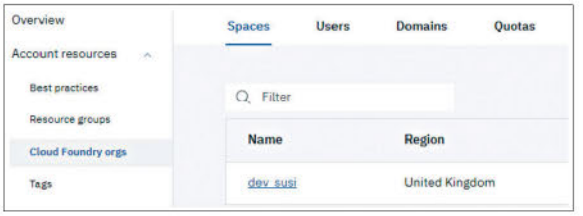
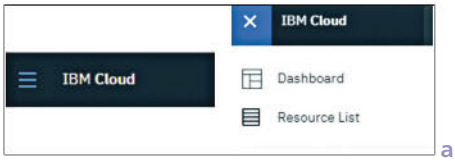


Fig. 4 Space all'interno di una organizzazione.
Per visualizzarlo cliccare sul nome dell'organizzazione.



a.

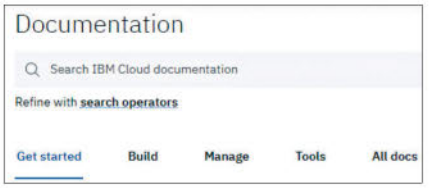


b.

Fig 5 a. Da menu sandwich si accede alla dashboard; b. la dashboard per vedere le proprie risorse.

La voce *Documenti* (*Docs*) permette di approfondire ogni genere di argomento correlato alla piattaforma (Figura 6). È possibile esplorare tutte le altre voci per scoprire le possibilità offerte.

→ Fig. 6



ATTIVITÀ 2

IBM Cloud Platform: creazione di un programma in Java e sua esecuzione in Cloud

Approfondimento
Ingegnerizzazione dell'app

Scenario

Avete in mente da un po' di tempo di realizzare una vostra applicazione da condividere con i vostri amici e non vedete l'ora di metterla online.

Consegna

Scopo di questa esercitazione è realizzare una semplice applicazione Java ed eseguirla in Cloud.

Svolgimento

Passo 1: selezione del servizio dal catalogo

- Andiamo nel catalogo di IBM Cloud Platform e selezioniamo la categoria Calcola (*Compute*). Selezioniamo poi il box *Cloud Foundry* (Figura 7).

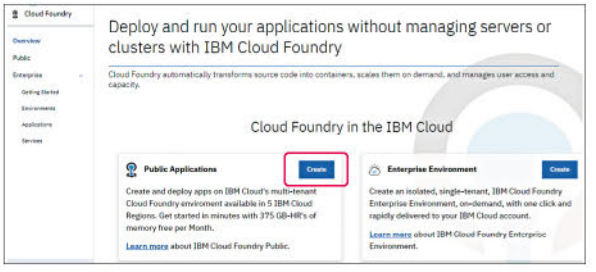
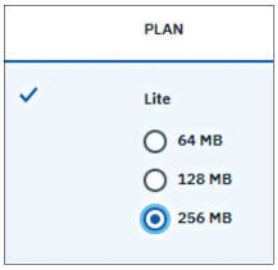


Fig. 7 Menu Catalog → Compute → Cloud Foudry.

Passo 2: creazione applicazione

- Creiamo la nostra applicazione con *Create* nel box Public Application.
- A questo punto dobbiamo scegliere la memoria necessaria: selezionare 256 MB (Figura 8). *Attenzione: nella versione lite la quantità di memoria disponibile è limitata. Per questo motivo non è possibile creare numerose applicazioni; tuttavia una o due applicazioni sono sufficienti per capire come funziona questo servizio.*

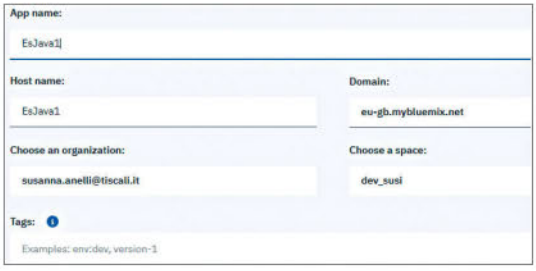


↑ Fig. 8 La scelta della quantità di memoria.

- Ora selezioniamo lo starter kit *Liberty for Java* (è possibile anche scegliere NodeJS... o qualsiasi altro linguaggio presente). Clicchiamo sul rettangolo del linguaggio scelto (Figura 9) e procediamo a creare un'istanza, dando il nome dell'applicazione. Questa applicazione sarà un semplice "hello world" per iniziare.
- Successivamente fornire i parametri richiesti.
  - Il **nome** deve essere univoco in rete, quindi è consigliabile mettere nel nome qualche carattere numerico (comunque differente da quello mostrato in questo esempio, a meno di non avere un dominio proprietario).
  - Inoltre devono essere **valorizzati i campi** relativi alle indicazioni geografiche (cioè in quale continente desideriamo che giri la nostra applicazione) tra quelle disponibili, il nome dell'organizzazione e dello spazio entro cui vogliamo crearla. Scrivere anche un tag servirà a gestire con più snellezza le varie applicazioni (Figura 10).

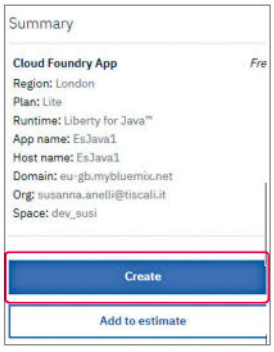


↑ Fig. 9 Selezione del servizio: scelta del linguaggio per la costruzione dell'applicazione.

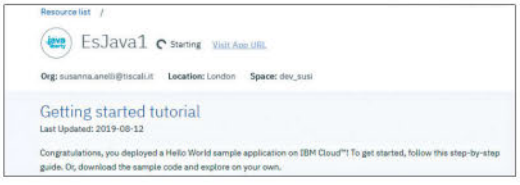


↑ Fig. 10 Creazione dell'applicazione: nome e valorizzazione dei campi.

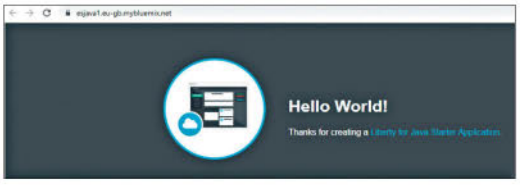
Ora siamo pronti: cliccare su *Create* a destra (Figura 11). Verrà visualizzata una schermata contenente delle ulteriori informazioni (Figura 12) e dopo circa un minuto avremo la nostra applicazione di prova attiva e funzionante (Figura 13).

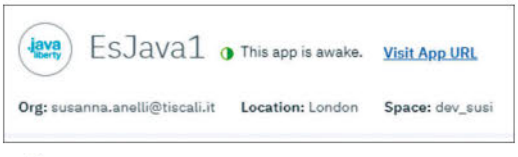


→ Fig. 11



← Fig. 12 L'applicazione è in fase di creazione.





← ↑ Fig. 13 L'applicazione è stata creata.

Passo 3: esecuzione e test dell'applicazione
Clicchiamo sulla voce *Visit app URL* in alto; si apre una pagina del browser con l'output della nostra app Hello World.
Nel nostro esempio si potrà accedere a questa app da qualsiasi postazione in Internet digitando l'url: https://<nometuaapplicazione>.mybluemix.net/.
Ovviamente la vostra applicazione avrà un URL differente o anche un dominio differente nel caso ne aveste inserito uno vostro.
In questo caso l'URL è https://esjava1.eu-gb.mybluemix.net/.
L'applicazione è disponibile per essere eseguita in rete!
Noi andremo a modificare e personalizzare il codice sorgente.

Passo 4: gestione dell'applicazione
Andiamo sulla Dashbord (o su Resource list, Figura 14), per vedere lo stato della nostra applicazione da Cloud Foundry App. In questo momento la App è in stato di Running. È possibile fermarla/riattivarla cliccando sui tre puntini. Si tenga presente che un'applicazione ferma non consuma nulla. Sempre dai tre puntini l'applicazione può essere rinominata o cancellata del tutto. **Potete fare qualche test di stop e start della vostra applicazione di prova.**
Clicchiamo ora sul nome della App e entriamo in una sorta di pannello di controllo (Figura 15).

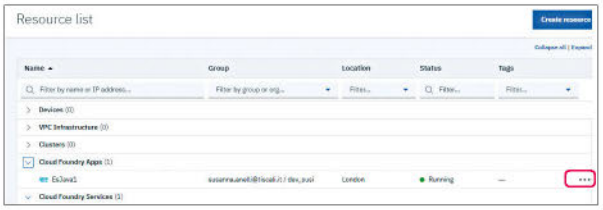


Fig. 14 Resource list.

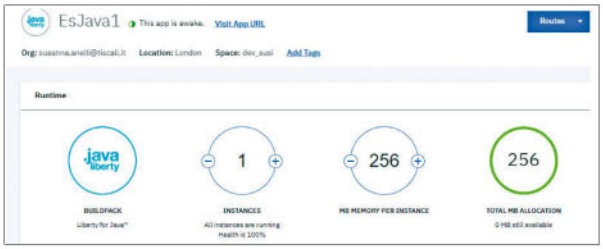


Fig. 15 Il pannello di controllo dell'app.

I cerchietti che compaiono nella pagina servono ad aumentare o diminuire il numero di istanze che si vogliono utilizzare (*scalabilità orizzontale*) e la memoria che dedichiamo alla nostra App (*scalabilità verticale*). Tarando opportunamente questi parametri, si può fare in modo che l'applicazione possa rispondere efficacemente a un numero arbitrariamente alto di utenti. Al crescere del numero di istanze e della loro taglia ovviamente i costi crescono. Si può abilitare un servizio di *Autoscaling* (che però non è disponibile negli account lite) affinché sia la stessa piattaforma a incrementare o diminuire il numero di istanze in ottemperanza ad alcune regole che avrete dato voi stessi. In questo modo si è sicuri che non ci saranno istanze inutilmente attive.

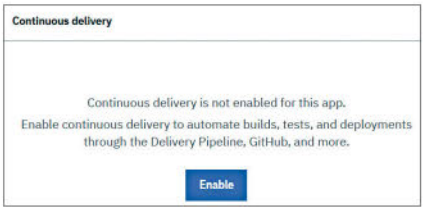


Fig. 16 Fornitura continua.

La toolchain e il continuous delivery. Andando in basso nella stessa pagina troverete un pulsante *Abilita* (*Enable*) sotto la voce *Fornitura continua* (*continuous delivery*, Figura 16). Con questo pulsante viene abilitata una toolchain (Figura 17) che vi consente alcune importanti attività, come il controllo del codice sorgente, la gestione dei task (in un'ottica collaborativa tra più persone) e il controllo dei meccanismi di compilazione e deploy. Il nostro scopo è accedere al codice sorgente.
Procediamo e premiamo il pulsante *Enable* e successivamente il pulsante *Create* (in alto a destra).
Verrà chiesta una IBM Cloud api Key, che potete creare premendo il pulsante a destra (*Create*). Il consiglio è quello di copiare la Key generata e metterla in un file di testo.

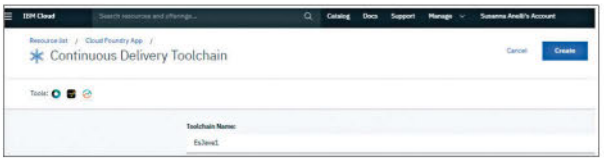
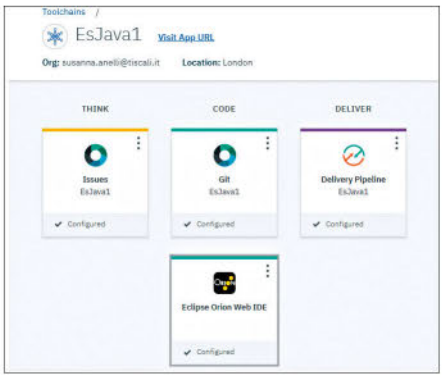


Fig. 17 Creazione della toolchain.

Premere ancora il pulsante *Create* in alto a destra. Se tutto andrà bene, dopo pochi secondi avrete la vostra toolchain fatta in questo modo (Figura 18):

Fig. 18 La toolchain.



Accesso al codice. Cliccando sul *repository GIT* al centro della toolchain, accediamo al codice dell'App tramite la sua cartella (Figura 19).
Andare nella directory src/main (Figura 20).
Clicchiamo poi sulla directory: *java/.../servlet e poi sul file SimpleServlet.java*.
Si apre una pagina col codice della servlet che possiamo modificare cliccando in alto a destra il comando EDIT.

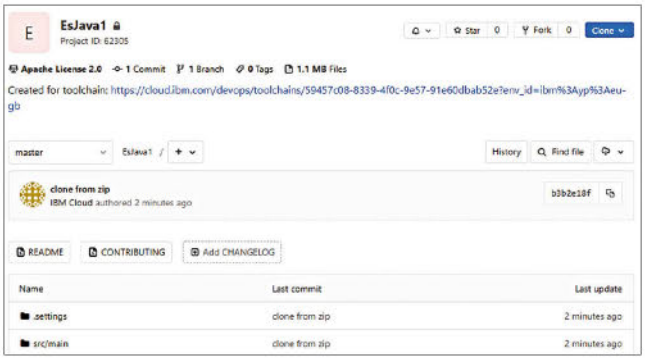


Fig. 19 L'accesso al codice da cartella.

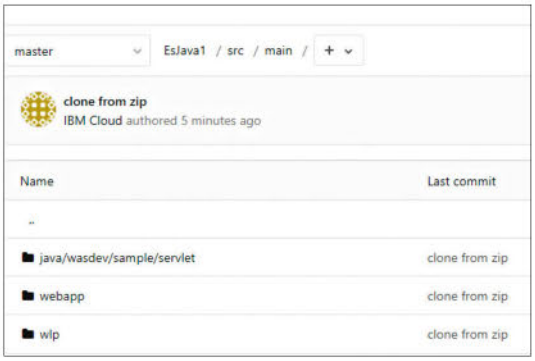


Fig. 20 La cartella dei sorgenti.

Cambiamo il messaggio "Hello World" con la stringa "Ciao a tutti" (o un'altra a piacere) come in Figura 21.

```
 8  import javax.servlet.http.HttpServletRequest;
 9  import javax.servlet.http.HttpServletResponse;
10
11  /**
12   * Servlet implementation class SimpleServlet
13   */
14  @WebServlet("/SimpleServlet")
15  public class SimpleServlet extends HttpServlet {
16      private static final long serialVersionUID = 1L;
17
18      /**
19       * @see HttpServlet#doGet(HttpServletRequest request, HttpServletResponse response)
20       */
21      @Override
22      protected void doGet(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {
23          response.setContentType("text/html");
24          response.getWriter().print("CIAO A TUTTI!!! ");
25      }
26
27  }
28
```

Fig. 21 Modifica del codice sorgente.

Nel campo *Commit message* in basso inseriamo il testo: "Personalizzazione del messaggio" (Figura 22) e premiamo il pulsante verde *Commit changes* per confermare le modifiche apportate. Il codice modificato viene salvato e si innesca, automaticamente, di nuovo la procedura di compilazione e deploy.

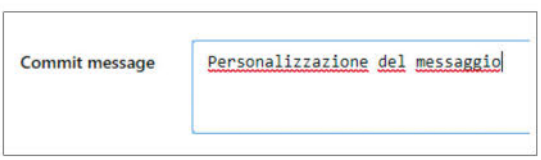


Fig. 22 Il Commit message.

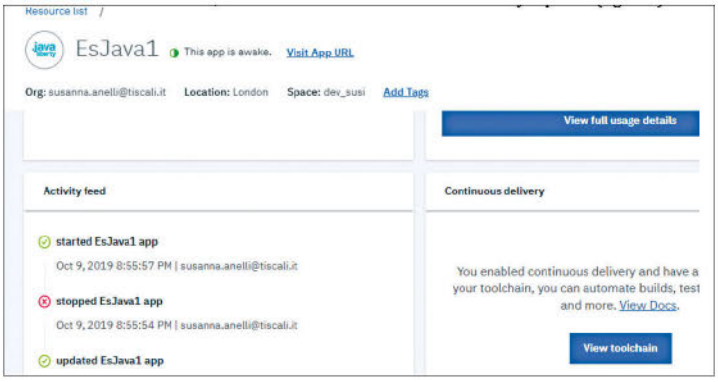


Fig. 23 La Delivery Pipeline.

Per vedere l'esecuzione occorre tornare nella pagina di overview dell'applicazione, accedere di nuovo alla toolchain, e selezionare il blocchetto della Delivery Pipeline (Figura 23). Se fate in tempo, vedrete in azione i due stage di build e deploy (Figura 24). Se il codice è compilato con successo, si avvierà la procedura di deploy che installerà la nuova versione modificata dell'App, in cloud. Quando il deploy sarà completato, potete cliccare su *View console* e tornare alla dashboard (quando sono verdi entrambi i box: Figura 25).

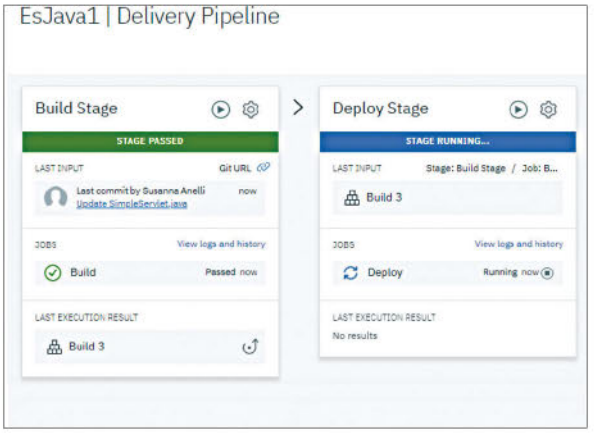


Fig. 24 Build e deploy.

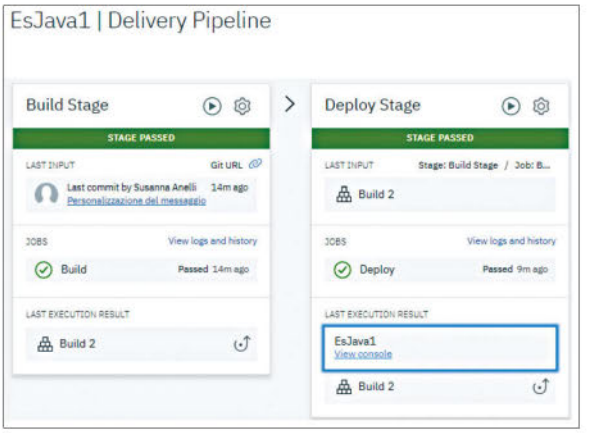


Fig. 25 Deploy completato (i due box sono verdi entrambi).

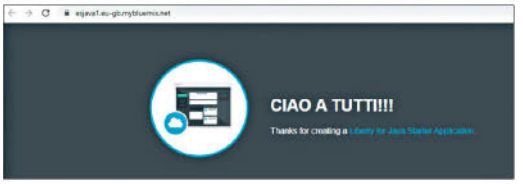


Fig. 26 Il risultato dell'app in cloud.

Tornate alla dashboard o alla lista delle risorse e, come prima, cliccando sull'URL dell'App (o aggiornando il browser se avete lasciato una finestra aperta sull'app), verrà visualizzata l'applicazione modificata (Figura 26).

ATTIVITÀ 3

IBM Cloud Platform: Creazione di un cluster Kubernetes e deploy di un'applicazione containerizzata

Scenario

L'installazione di un ambiente locale di Kubernetes e Docker è un'operazione complicata, mentre la creazione di un cluster Kubernetes tramite IBM Coud Platform è molto semplice.

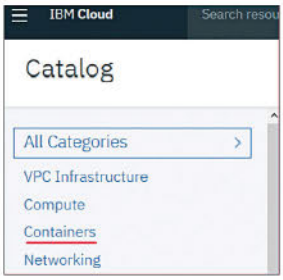
Consegna

Creazione di un cluster Kubernetes nella modalità "As-a-Service".

Svolgimento

Di seguito presentiamo una sintesi delle operazioni da fare. Dal menu di IBM Cloud Platform, selezioniamo il *Catalogo* (menù in alto) e quindi sulla sinistra clicchiamo il link *Containers* (Figura 27) e quindi su *Kubernetes* (Figura 28). Per gli esercizi scegliamo il cluster *Free* (Figura 29).

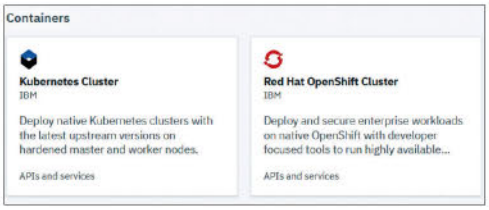
- Inseriamo nei campi i valori che vogliamo (nome cluster, resource group, geografie ecc), oppure lasciamo i valori di default.
- Clicchiamo il pulsante *Create Cluster* e aspettiamo circa 20 minuti per il completamento della creazione del nostro cluster.

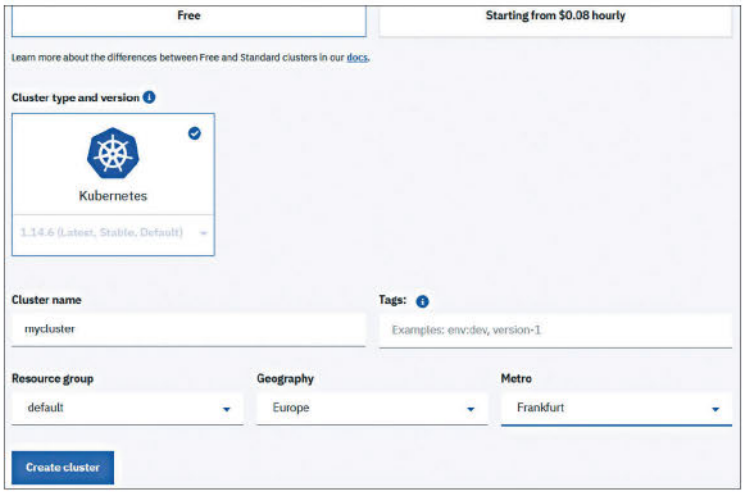


← Fig. 27

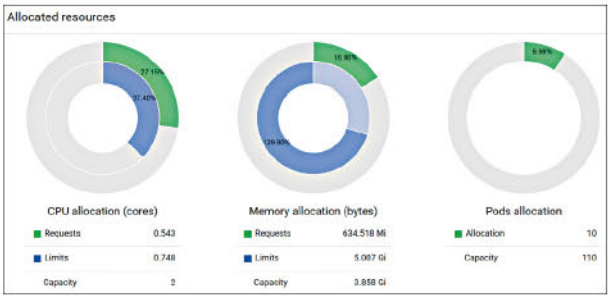
→ Fig. 29

↓ Fig. 28





Verranno fatte, **in automatico**, innumerevoli attività, completamente nascoste all'utente: creazione delle macchine virtuali con le CPU richieste, creazione di master node e worker node ecc. Alla fine vedremo il pallino verde e lo stato "normal" del cluster. Prima di concludere andiamo a vedere cosa c'è dentro questo cluster: clicchiamo su *Kubernetes Dashboard* in alto a destra.



↑ Fig. 30

Nella pagina che si apre vediamo un menù a sinistra e il servizio Kubernetes attivo. Se clicchiamo sulla voce *Nodes* (o Nodi) si apre il dettaglio dei nodi del cluster e dovrebbe apparirne soltanto uno. Clicchiamo sull'indirizzo del nodo e nella pagina successiva vediamo il suo contenuto in termini di PODS e allocazione risorse (Figura 30). In questo caso vediamo allocati 10 PODS che contengono servizi vari interni al sistema. Possiamo chiudere questa dashboard e tornare al nostro account IBM Cloud.

ATTIVITÀ 4

IBM Cloud Platform: introduzione e utilizzo delle Function Serverless

Disponibile nell'eBook.

ATTIVITÀ 5

IBM Cloud Platform: creazione di un'applicazione mobile (Android o iOS) per l'accesso a un Data Base in Cloud

Disponibile nell'eBook.

ATTIVITÀ 6

Una Panoramica per un laboratorio scolastico virtuale con OpenStack

Disponibile nell'eBook.

SINTESI

IL CLOUD COMPUTING

Il Cloud Computing è un modo di utilizzare risorse di calcolo, storage, rete, servizi, applicazioni, tramite Internet. Utilizzare una risorsa in Cloud significa accedere a essa tramite Internet, senza possederla.

CARATTERISTICHE

Tutti i servizi in Cloud Computing hanno delle proprietà che li caratterizzano che mirano a favorire flessibilità e scalabilità, riducendo i costi e gli spazi. Sono alla base dei modelli di servizi AS A SERVICE, ON DEMAND e PAY PER USE.

ON DEMAND SELF SERVICE

Un utente può accedere autonomamente ai servizi offerti da un fornitore, senza la necessità di un intervento umano dei gestori.

BROADNETWORK ACCESS

I servizi devono essere disponibili in rete e accessibili tramite dispositivi standard.

RESOURCE POOLING

Le risorse fornite sono raggruppate e organizzate per essere disponibili per più consumatori. Le risorse vengono assegnate e riassegnate dinamicamente in base alla domanda dei consumatori, indipendentemente dal luogo fisico in cui si trovano.

RAPID ELASTICITY

Le risorse possono essere assegnate e rilasciate elasticamente e rapidamente in base alle necessità.

MEASURED

Ogni servizio utilizzato deve poter essere misurato e controllato in modo trasparente, per poter calcolare i consumi e pagare solo quello che si usa.

MODELLI DI SERVIZIO

Rappresentano i modi in cui il Cloud può essere utilizzato, corrispondenti al tipo di servizi forniti dal provider. Si differenziano per il tipo di risorse rese disponibili. Ogni modello di servizio implica un diverso livello di gestione da parte del cliente e del fornitore.

SAAS

Distribuzione di applicazioni software tramite Internet. Il software delle applicazioni, i dati e tutta l'infrastruttura sottostante sono nel data center del provider, che gestisce l'hardware e il software.

IAAS

Distribuzione di capacità computazionale (risorse di calcolo), archiviazione, reti e altre risorse informatiche. Il consumatore non controlla l'infrastruttura fisica, ma ha il controllo sui sistemi operativi, sullo storage e sulle applicazioni distribuite.

PAAS

Le applicazioni sono create dal consumatore utilizzando un ambiente di sviluppo del fornitore. Il consumatore non gestisce né controlla l'infrastruttura cloud sottostante, ma ha il controllo sulle applicazioni distribuite.

MODELLI DI DISTRIBUZIONE
Modalità di accesso alle risorse. Riguarda la condivisione dei servizi tra più utenti. Simile a un controllo degli accessi.

PRIVATE CLOUD
L'infrastruttura cloud
- è fornita a uso esclusivo di una singola organizzazione;
- può essere di proprietà dell'organizzazione, di un provider o di entrambi e può trovarsi dentro o fuori la sede aziendale.

PUBLIC CLOUD
L'infrastruttura cloud
- è predisposta per l'uso pubblico;
- è nella sede del provider, che gestisce e rende disponibili tramite Internet le risorse.

COMMUNITY CLOUD
L'infrastruttura cloud
- è fornita a uso esclusivo di una specifica comunità di consumatori che condividono degli interessi;
- può essere di proprietà dell'organizzazione, di un provider o di entrambi e può trovarsi dentro o fuori la sede aziendale.

HYBRID CLOUD
Combina le risorse di cloud pubblici e privati. Consente di non fare affidamento interamente su un unico cloud pubblico.

CAAS
Si concentra sulla gestione di container, pacchetti software autonomi che contengono tutto il necessario per eseguire un'applicazione.

CONTAINER
Sono ambienti di sviluppo virtuali che consentono di eseguire i microservizi stessi, fornendo le risorse necessarie per la loro esecuzione.

FAAS
Consente di eseguire solo piccole porzioni di codice senza preoccuparsi dell'infrastruttura sottostante e della gestione dei server.

MICROSERVIZI
Funzioni autonome e indipendenti, utilizzate in rete, che possono essere combinate per comporre un'applicazione più complessa. Per utilizzare i microservizi si utilizzano le API (Application Programming Interface).

Verifica delle CONOSCENZE

Vero o Falso?

1 Cloud computing è sinonimo di virtualizzazione. V F

2 Un servizio in Cloud Computing può essere usato all'occorrenza. V F

3 Un servizio in cloud è rigido perché difficilmente controllabile. V F

4 Un servizio in cloud è poco affidabile. V F

5 Un'azienda può avere o tutti i servizi in cloud o tutti servizi proprietari. V F

6 Il Cloud Computing prescinde da Internet. V F

7 Hybrid cloud è sinonimo di multicloud. V F

8 Il Cloud Computing si basa sulla virtualizzazione delle risorse. V F

9 Un utente di un servizio in cloud deve essere un'azienda. V F

10 Il modello PaaS fornisce l'infrastruttura come servizio privato. V F

11 I microservizi aumentano la flessibilità dell'architettura delle applicazioni. V F

12 Un microservizio è un'entità atomica e indipendente. V F

13 I microservizi possono comunicare con API in modo indipendente dall'ambiente di sviluppo. V F

14 I microservizi sono legati a una determinata applicazione. V F

15 Un container è associato a un unico microservizio. V F

16 Un container è indipendente dal S.O. V F

17 Un container è indipendente dall'hardware. V F

18 Nel modello IaaS il fornitore gestisce le risorse fisiche. V F

19 Il cloud pubblico è quello usato dalla Pubblica Amministrazione. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

20 I servizi pubblici in Cloud:

a. favoriscono il controllo completo di tutta l'infrastruttura
b. sono flessibili
c. necessitano di investimenti elevati
d. richiedono competenze specifiche interne all'organizzazione che li utilizza

21 Uno degli svantaggi di un servizio in cloud è:

a. la dipendenza dal protocollo HTTP
b. l'impossibilità di utilizzare il servizio in orari definiti dalle policy aziendali
c. la dipendenza dalla connessione a Internet
d. l'elevato costo dell'infrastruttura necessaria

22 Il modello IaaS:

a. fornisce database per la raccolta dati
b. fornisce risorse hardware fisiche
c. fornisce risorse software
d. fornisce risorse hardware virtuali

23 I microservizi:

a. sono comodi ma costosi
b. non sono compatibili con l'architettura di un'applicazione client/server
c. dipendono dal sistema operativo
d. rendono flessibile l'architettura di un'applicazione

24 La forma di cloud ibrido:

a. fornisce solo servizi riservati a un'azienda
b. è sinonimo di multi cloud
c. è il modello più semplice
d. sfrutta i vantaggi del cloud pubblico e del cloud privato

Domande per la prova orale

25 Quali sono i modelli dei servizi e i modelli di distribuzione del cloud?

26 Quale caratteristica del cloud è necessaria per poter parlare di Pay per use?

27 Che cosa significa "On-demand"?

28 Quali sono i modelli di servizio del Cloud Computing?

29 Riassumi i vantaggi e gli svantaggi dell'utilizzo di una infrastruttura in Cloud.

30 Quali sono i modelli di distribuzione dei servizi in Cloud Computing?

31 Quali sono le caratteristiche dei servizi in Cloud Computing?

32 Perché un servizio in Cloud Computing deve essere misurabile?

33 Che cosa si intende per Cloud Computing?

34 Fai una ricerca sul Web e rispondi alle seguenti domande.
- **a.** Che cosa si intende per multicloud?
- **b.** Che differenza c'è tra multicloud e hybrid cloud?
- **c.** Presenta un caso reale in cui è utilizzato l'hybrid cloud.
- **d.** Presenta un caso reale in cui è utilizzato il multicluod.

- Elabora e sintetizza i risultati ottenuti.
- Interroga l'intelligenza artificiale su questo argomento; confronta e valuta i risultati ottenuti con quelli da te precedentemente elaborati.
- Riporta il prompt che hai utilizzato per cercare le informazioni.
- Confronta i prompt utilizzati dai tuoi compagni e i relativi risultati ottenuti.
- Scrivi sinteticamente le tue osservazioni.

35 Quali sono gli elementi che caratterizzano un servizio in Cloud Computing?

36 Fai degli esempi, tratti dalla tua esperienza, di utilizzo di SaaS.

37 Esponi la differenza tra cloud privato, cloud pubblico e cloud ibrido.

Cloud privato:

Cloud pubblico:

Cloud ibrido:

38 Che cosa si intende per "microservizio"?

39 Quali sono i vantaggi dell'uso dei microservizi?

40 Quale relazione c'è tra container e microservizio?

41 Quale potrebbero essere gli ostacoli che impediscono alle piccole e medie imprese di adottare soluzioni cloud?

42 Che cosa si intende per Cloud Computing quantistico?
- Per rispondere alla domanda fai una ricerca in Internet.
- Elabora e sintetizza i risultati ottenuti.
- Interroga l'Intelligenza Artificiale su questo argomento.
- Confronta e valuta i risultati ottenuti con quelli da te precedentemente elaborati.
- Riporta il prompt che hai utilizzato per cercare le informazioni.
- Confronta i prompt utilizzati dai tuoi compagni e i relativi risultati ottenuti.
- Scrivi sinteticamente le tue osservazioni.

43 Quali sono gli elementi del Cloud Computing che possono avere un impatto su una società più sostenibile?

44 Come possono i microservizi aiutare a gestire meglio la scalabilità e i pagamenti in una piattaforma di prenotazione online per hotel?

45 Quali sono i principali componenti contenuti in un'immagine Docker e come facilitano il trasferimento e la creazione di un container su un'altra macchina?

Esercizi in più

Cloud Computing

Abstract

Data centers are secure environments in which the technological infrastructure of an IT system resides. Cloud Computing services are placed in this context: services are made available in various ways to users who request them. The main purpose of cloud services is to free users from the hardware and/or software complexity necessary for the management of an IT system. The advantages are the possibility of requesting the service on the basis of needs and at any time and the possibility of making your systems scalable. There are various service models: SaaS, PaaS, IaaS, FaaS and CaaS.
The deployment models are divided into Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. The disadvantage of cloud services is that they depend on an Internet connection.

Questions

Answer all questions

1 What is Cloud Computing?

2 What are the advantages of Cloud services?

3 What is the purpose of a Hybrid Cloud?

4 What are microservices?

Choose the correct answer

5 SaaS is:
- a an hardware delivery model
- b a software delivery model
- c used to provide an entire infrastructure
- d a security system

6 Public cloud:
- a reduces costs for the company
- b allows customization of the infrastructure
- c only provides software
- d is not very flexible

7 Cloud Computing:
- a requires specialized personnel
- b is very expensive for companies
- c exploit resource virtualization
- d is an Operative System

8 A Cloud service:
- a must be quantifiable
- b can be used for a fixed period of time
- c works also off-line
- d is unsafe

Crosswords

Across

3 Platform used to design applications with containers

4 They are used for communication between microservices

6 Feature of an on-demand service

8 Cloud service platform from a well-known provider

9 Model in which the application is used

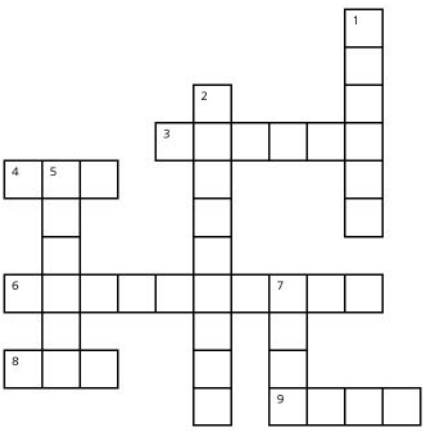
Down

1 Cloud service deployment modes

2 Development environments for microservices

5 Cloud service deployment modes where the user does not control the data

7 Model in which an entire infrastructure is used

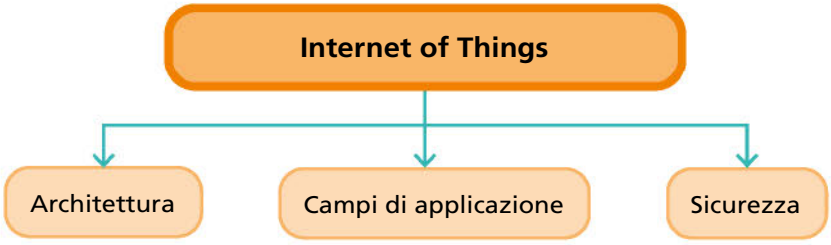




Unità

10

IoT – Internet of Things



Visione d'insieme

- I sistemi IoT e le loro caratteristiche essenziali.
- Architettura dei sistemi IoT e ambiti di utilizzo.
- Sicurezza nei sistemi IoT.

1 Introduzione

L'ultima volta che ho acquistato un'auto, ho dovuto prestare attenzione per più di un'ora al tecnico che spiegava come utilizzare i comandi e verificare il funzionamento del cruscotto Figura 1. Nascosti nei sedili, nel vano motore e nella carrozzeria, un centinaio di sensori monitorano diversi aspetti del veicolo, come le prestazioni del motore, la sicurezza, il comfort e i collegamenti con l'esterno.
Questo è solo un esempio di come l'Internet of Things (IoT) stia trasformando oggetti comuni in strumenti intelligenti che interagiscono con l'ambiente e con noi. I sensori rilevano i dati, la rete wireless li convoglia ai sistemi di controllo locale, la connettività Internet li trasferisce a un server in cloud che estrae le informazioni, e i protocolli regolano il traffico, permettendo alle applicazioni di accedere ai servizi.
Tuttavia, l'IoT porta con sé sfide significative riguardo agli aspetti tecnici, alla privacy e alla sicurezza. I protocolli sono spesso proprietari e non sempre permettono l'interoperabilità tra dispositivi di produttori diversi, rendendo necessari standard comuni.
La sicurezza informatica è un altro aspetto critico. Le misure di sicurezza devono essere integrate nei dispositivi fin dalla progettazione per poter correggere debolezze e vulnerabilità nel tempo.
Per quanto riguarda la privacy, l'IoT solleva timori significativi. La raccolta e l'analisi di grandi quantità di dati personali richiedono misure rigorose per garantire che le informazioni siano protette e utilizzate in modo etico.
L'uso dell'Intelligenza Artificiale (AI) nell'IoT suscita ulteriori timori. Gli algoritmi di AI possono essere complessi e opachi, rendendo difficile comprendere come vengono prese le decisioni. Questo può causare problemi di responsabilità e trasparenza, specialmente se gli algoritmi sono influenzati da pregiudizi.



➜ **Fig. 1** Esempio di IoT applicato ai comandi di un'auto.

2 L'ecosistema IoT

L'IoT è spesso paragonato a un **ecosistema** biologico, perché rappresenta un sistema complesso in cui vari componenti interconnessi collaborano per raggiungere obiettivi comuni e mantenere un ambiente sostenibile ed equilibrato. Questo concetto è molto utile per comprendere la composizione di un sistema IoT e l'interoperabilità tra i dispositivi intelligenti. Esaminiamo la Tabella 1.
Nelle unità precedenti abbiamo già introdotto le tecnologie principali e i protocolli utilizzati nei sistemi IoT. In questo contesto ci limiteremo a ricordare gli elementi architetturali dei sistemi IoT e a fornire esempi applicativi.

Pit Stop

1 Che cos'è un sistema IoT?

Caratteristica	Ecosistema Biologico	Ecosistema IoT
		
Definizione	Un ecosistema è una comunità di organismi che vivono in un'area circoscritta, collegati tra loro e con l'ambiente attraverso lo scambio di materiali e flussi di energia.	L'ecosistema IoT è una comunità di oggetti interconnessi attraverso lo scambio di flussi di dati.
Componenti	Organismi viventi (piante, animali, microrganismi) e componenti non viventi (acqua, aria, suolo).	Dispositivi connessi (sensori, attuatori, sistemi intelligenti), reti di comunicazione e protocolli (Wi-Fi, Bluetooth ecc.), piattaforme di gestione dei dati.
Interazioni e collaborazioni	Gli organismi interagiscono tra loro e con l'ambiente.	I dispositivi IoT comunicano tra loro e con le piattaforme di gestione per raccogliere, analizzare e condividere dati.
Equilibrio	Un ecosistema sano si mantiene in equilibrio, garantendo la sostenibilità a lungo termine.	Un ecosistema IoT efficiente fornisce l'interoperabilità tra dispositivi, opera una gestione ottimale delle risorse (banda trasmissiva, consumo energetico ecc.) e garantisce sicurezza.
Interconnessione	I componenti sono interconnessi e dipendono l'uno dall'altro.	I componenti dell'IoT sono interconnessi e dipendono l'uno dall'altro per funzionare correttamente.
Adattabilità	Gli ecosistemi si adattano ai cambiamenti ambientali.	L'ecosistema IoT si adatta ai cambiamenti tecnologici e alle necessità degli utenti.

↑ Tab. 1

3 Architettura di un sistema IoT

Gli **elementi costitutivi** di un sistema IoT comprendono: dispositivi, reti, gateway e cloud.

- **Dispositivi** (**Things**). Si tratta di sensori, attuatori, dispositivi intelligenti e altri oggetti che raccolgono e trasmettono dati attraverso la rete a cui sono collegati.
- **Reti**. Connettono i dispositivi a una rete, permettendo la trasmissione dei dati raccolti dai dispositivi al cloud o ad altre piattaforme di gestione.
- **Gateway**. Fanno da intermediari tra i dispositivi e il cloud, raccogliendo i dati dai dispositivi e pre-elaborandoli prima di inviarli al cloud.
- **Cloud**. I server remoti con le piattaforme di gestione dei dati raccolgono e immagazzinano i dati che vengono elaborati e analizzati, permettendo di prendere decisioni, anche applicando gli algoritmi di Intelligenza Artificiale.

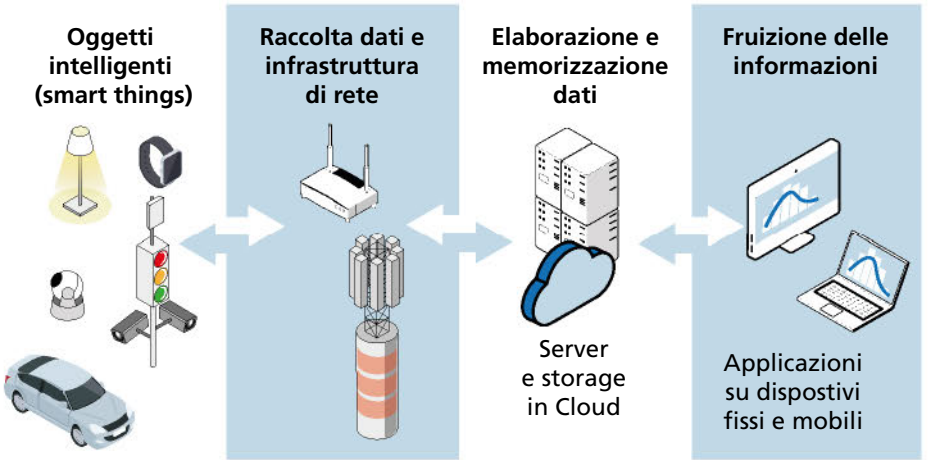


Fig. 2 La filiera dei dati nei sistemi IoT.

L'architettura dei sistemi IoT è strutturata in diversi livelli. Per introdurre il concetto, consideriamo la **Figura 2** che mostra come i dati transitano dal sensore/dispositivo intelligente all'applicazione dell'utente, passando per il gateway, la trasmissione in rete e l'elaborazione in cloud.
La **Figura 3** riprende la filiera dei dati esposta nella **Figura 2** e struttura l'architettura dei sistemi IoT in livelli logici. L'architettura multistrato dei collegamenti IoT prevede, alla base, il livello che ospita i dispositivi intelligenti. Seguono gli altri livelli relativi all'infrastruttura di rete, alla concentrazione dei dati e alla loro trasmissione, tramite rete geografica, ai server in cloud e ai server applicativi necessari a fornire all'utente le informazioni necessarie. Analizziamoli più in dettaglio.

1. **Livello dei Sensori e Dispositivi**. Questo è il livello più basso, dove risiedono i dispositivi fisici (things) come sensori e attuatori. Questi dispositivi raccolgono dati dall'ambiente circostante e possono anche eseguire azioni in risposta a tali dati.
2. **Livello di Raccolta e Trasmissione dei Dati**. Questo è il livello in cui i dispositivi inviano i dati raccolti dai sensori. I dati vengono trasmessi attra-



Fig. 3 Architettura multistrato dei collegamenti IoT. I dati sono in transito fino al raggiungimento del livello del cloud, quando i dati, finalmente a riposo, sono disponibili per l'analisi e l'uso da parte delle applicazioni.

verso un'infrastruttura di rete (come WiFi, Bluetooth ecc.) a un sistema intermedio che funge da collettore (gateway) o direttamente ai server in cloud tramite reti cellulari, router e Internet. La raccolta, l'elaborazione e la trasmissione dei dati a sistemi di elaborazione/archiviazione locale è conosciuta come *edge computing* (o *fog computing*). I gateway, o i server locali, possono pre-elaborare i dati raccolti per poi essere indirizzati ai server in cloud. Questo approccio permette di ridurre la latenza, migliorare l'efficienza e intervenire in tempo reale sui sistemi locali, se necessario, e consente di ridurre il carico sui server cloud, migliorando anche la sicurezza dei dati.

3. **Livello di Elaborazione e Analisi dei Dati**. Una volta raccolti, i dati vengono inviati al cloud per l'analisi. I server in cloud utilizzano algoritmi di **intelligenza artificiale** per analizzare i dati, per esempio in modo predittivo, e fornire risposte utili.
4. **Livello delle Applicazioni**. Questo è il livello in cui gli utenti interagiscono con i dispositivi del sistema IoT, spesso attraverso applicazioni web o mobili per capire che cosa sta succedendo e che cosa può essere fatto. Anche qui, l'Intelligenza Artificiale gioca un ruolo importante, migliorando l'interazione con i sistemi e automatizzando i processi.

La **sicurezza** è un elemento trasversale che permea tutti i livelli dell'architettura IoT, introducendo misure per proteggere i dati e i dispositivi da accessi non autorizzati e attacchi informatici.

notabene

Come spiegato nell'unità 7, il gateway è quel dispositivo che fa da ponte tra gli oggetti IoT e il cloud con lo scopo di raccogliere e filtrare i dati raccolti dai sensori e convertire i protocolli di comunicazione in un formato comprensibile per il cloud.

Pit Stop

2 Quali sono gli elementi di un sistema IoT?

4 Campi di applicazione

I dispositivi IoT combinati con gli algoritmi predittivi di Intelligenza Artificiale possono, potenzialmente, intervenire e trasformare praticamente ogni settore, migliorando l'efficienza e la sicurezza (Figura 4).



← Fig. 4 Alcune delle principali aree di applicazione IoT in città.

notabene

Attualmente le piattaforme IoT fanno largo uso dell'Intelligenza Artificiale per prendere decisioni, utilizzando strumenti di analisi avanzata per elaborare la grande quantità di dati raccolti dai dispositivi connessi (vedi Approfondimento).

Esaminiamo i vari settori di impiego.

- **Industriale**. L'IoT viene utilizzato per il monitoraggio in tempo reale delle linee di produzione e la manutenzione predittiva degli impianti.
- **Agricolo**. L'IoT è utile per controllare le condizioni del suolo, ottimizzare l'irrigazione e ridurre gli sprechi.
- **Energetico**. L'IoT migliora la gestione delle reti elettriche intelligenti (Smart Grids) e il monitoraggio in tempo reale della distribuzione dell'energia, riducendo le perdite. Analogamente, rende migliore la gestione delle reti idriche.
- **Commerciale e delle Vendite**. Nel commercio al dettaglio, l'IoT consente di migliorare l'esperienza del cliente durante l'acquisto attraverso dispositivi di rilevazione collegati a scaffali e carrelli intelligenti. Inoltre, permette una gestione più puntuale dei negozi.
- **Servizi**.
  - **Smart City**. Le città intelligenti utilizzano l'IoT e gli algoritmi di Intelligenza Artificiale per migliorare la qualità della vita dei cittadini con iniziative rivolte alla mobilità a basso impatto ambientale: veicoli connessi che comunicano tra loro e con le infrastrutture stradali, gestione intelligente dell'illuminazione pubblica e dei parcheggi, qualità dell'aria e dell'acqua, gestione e smaltimento dei rifiuti, e potenziamento della sicurezza pubblica attraverso il riconoscimento facciale.
  - **Sanità e Persona**. Attraverso i dispositivi medici per il monitoraggio remoto dei pazienti e la raccolta di dati sanitari è possibile perfezionare le diagnosi e i trattamenti. Spesso le applicazioni sanitarie ("eHealth") utilizzano dispositivi wearable, ovvero sensori "indossati" dall'essere umano, per ricavare informazioni legate allo stato di salute.
  - **Logistica**. L'IoT è utile per il monitoraggio delle flotte di veicoli, la gestione delle consegne e l'ottimizzazione delle rotte al fine di migliorare l'efficienza e ridurre i costi.
  - **Automotive**. Attraverso la connessione tra i veicoli che comunicano tra loro e con le infrastrutture stradali è possibile migliorare la sicurezza e l'efficienza del traffico.

Comprendi con l'analogia

Un giorno di ordinaria follia digitale



Giovedì 8 maggio, ore 7 del mattino. Il mio cellulare mi sveglia con una dolce melodia che va crescendo di intensità. Prima di alzarmi, l'App mi informa della durata del sonno e della sua qualità: niente male stavolta. Subito dopo mi ricorda gli impegni della giornata: scatto come un'antilope inseguita dal leone. Più di un messaggio mi ha già raggiunto e attende risposta. La posta elettronica mi segnala una serie di spam che provvedo a cancellare. Mi infilo in bagno e comincio a radermi, mentre lo specchio mi mostra le previsioni del tempo che danno pioggia abbondante. Entro in cucina dove già bolle il caffè. Estraggo dalla lavastoviglie una tazza ma, stranamente, è ancora sporca. Non perdo tempo e, mentre la mia auto esce dal garage e mi aspetta sotto casa, catturo l'ultimo yogurt dal frigorifero.
Il navigatore mi informa del traffico e mi consiglia una strada alternativa. Seguo le sue indicazioni, mentre il libro che stavo ascoltando riparte dal punto in cui l'avevo interrotto. Ora però ho voglia di musica e me ne viene suggerita una che si adatta all'orario e al traffico.

- **Domotica** (**Smart Home**). L'IoT è utile per il controllo automatico e centralizzato della casa, dalla videosorveglianza agli elettrodomestici, fino al risparmio energetico.

Un esempio reale: il collaudo degli elicotteri

Un esempio significativo è tratto dal settore elicotteristico dell'industria aerospaziale, che sta capitalizzando l'enorme quantità di dati di cui dispone per migliorare tutte le fasi del ciclo di vita del prodotto, dalla progettazione alla produzione, dall'ottimizzazione della campagna voli al supporto al cliente. In particolare, la raccolta e l'analisi di dati utili per il collaudo dei prototipi: non vengono considerati solo i parametri legati all'operatività e alle prestazioni del velivolo, acquisiti durante il volo dai sensori integrati negli aeromobili, ma anche una varietà di informazioni collaterali: dati atmosferici, commenti del pilota, configurazione del velivolo, missioni tipiche della macchina.
Questo insieme di dati arricchisce enormemente il patrimonio conoscitivo aziendale: grazie all'analisi dei dati di volo, il comportamento reale del velivolo è pienamente compreso e "trasferito" ai prototipi virtuali dell'elicottero utilizzati in simulazioni ingegneristiche multidisciplinari, a vantaggio sia del miglioramento del prodotto sia dell'ottimizzazione delle successive campagne di volo. Un secondo ambito di grande rilievo riguarda la gestione della flotta e ha come obiettivo la soddisfazione dei clienti, il contenimento dei costi operativi e il miglioramento del prodotto.

Pit Stop

3 Quali sono i campi di applicazioni dell'IoT?

5 La sicurezza dei sistemi IoT

La sicurezza dei sistemi IoT è a rischio perché spesso non consideriamo che oggetti di uso comune possano essere attaccati. In realtà, si tratta di sistemi informatici vulnerabili. Conoscendo gli interessi e le abitudini di una persona, rintracciabili dai sistemi che utilizza, è possibile accedere alle sue informazioni personali. Insinuandosi nel software dei dispositivi, è possibile prenderne il controllo per aprire porte, controllare luci o azionare motori. Introducendo codici

Stesso giorno, 9 del mattino. Arrivo in Istituto e apro Moodle, dove sono già presenti, nel forum di classe, alcune domande che gli studenti hanno fatto il giorno prima e a cui dovrò rispondere a lezione. Intanto ha smesso di piovere e uno studente mi fa notare l'arcobaleno che è apparso in cielo e che non posso ignorare e fotografare.
Stesso giorno, ore 13. A pranzo, l'App mi informa delle calorie che il menu della mensa presenta e mi consiglia il cibo da ordinare in funzione del peso che la bilancia ha rilevato stamattina.
Nel pomeriggio mi aspettano un paio di videoconferenze che, puntualmente, l'App mi ricorda un quarto d'ora prima dell'inizio.
Stesso giorno, 4 del pomeriggio.
Mentre sono in videoconferenza, mi arriva un messaggio dalla banca con il conto dell'idraulico (95 euro!) per la riparazione della lavastoviglie. Lavastoviglie?!? Realizzo che, quando sono uscito stamattina, la lavastoviglie era guasta. In mattinata, senza alcun mio intervento diretto, la lavastoviglie ha individuato il problema e ha chiamato l'idraulico.
Stesso giorno, 7 di sera. Suona il campanello. È arrivata la spesa che il frigorifero ha pensato bene di ordinare stamattina.
Stesso giorno, 9 di sera. La giornata è stata lunga. Per rilassarmi guardo brevemente la mia serie preferita partendo dal punto in cui era stata interrotta e, prima di andare a letto, rivedo le statistiche di oggi con i passi fatti e le calorie consumate, pronto a ricominciare un altro giorno di ordinaria follia digitale!

malevoli in un termostato, in un bollitore per il caffè, in una centralina di controllo di un'automobile o in un dispositivo indossabile, è possibile impedirne il funzionamento, non consentendo a un pacemaker di operare, ai freni di un'automobile di frenare o a uno sterzo di girare (**Figura 5**). Analizziamo i principali elementi di criticità.

- **Qualità dei Dispositivi**. Molti dispositivi di uso quotidiano, come tostapane, aspirapolvere e lampioni, sono in realtà computer con CPU e software. Tuttavia, a differenza dei computer tradizionali, raramente pensiamo di proteggerli con antivirus o aggiornamenti. Questi dispositivi, spesso rilasciati con funzioni minime e senza possibilità di aggiornamento, possono contenere vulnerabilità che possono essere sfruttate per attacchi informatici.
- **Quantità dei Dispositivi**. Il numero elevato di sensori interconnessi genera una grande quantità di dati, spesso inviati a fornitori di servizi. Senza protocolli di sicurezza adeguati, questi dati sono a rischio di furti o inquinamento. La scarsità di indirizzi IPv4 e l'uso del NAT aumentano la complessità di interazione con i dispositivi IoT. La centralizzazione dei servizi introduce punti di debolezza (Single Point of Failure). L'adozione massiccia di IPv6 aiuterà a mitigare questi problemi.
- **Posizionamento dei Dispositivi**. I sensori intelligenti, spesso installati in luoghi difficilmente accessibili, possono continuare a funzionare per anni senza aggiornamenti, diventando bersagli facili per attacchi DDoS.
- **Impatto sulla Privacy**. I dispositivi IoT, come sistemi indossabili, assistenti vocali, videosorveglianza e giochi per bambini, offrono benefici, ma possono anche essere usati per mappare i movimenti e spiare le abitudini, minacciando la privacy e la libertà personale.

Pit Stop

4 Quali sono le principali criticità relative alla sicurezza di sistemi IoT?



Fig. 5 e-Spartacus: ovvero della rivolta degli SmartThings. La figura mostra ironicamente cosa potrebbe succedere se qualche malintenzionato potesse modificare il firmware di oggetti di uso comune in modo da inserire un ransomware o un malware.

notabene

Per rilevare eventuali vulnerabilità dei sistemi IoT esposti, un buon riferimento è utilizzare Shodan, un motore di ricerca per sistemi IoT, che permette di trovare i dispositivi connessi a Internet, identificando potenziali punti deboli e vulnerabilità.

Approfondimento - Tecnologia 1

Edge Computing e Fog Computing: due punti di vista

I termini *edge computing* e *fog computing*, quest'ultimo introdotto da CISCO, insistono sullo stesso concetto – spostare l'elaborazione vicino all'origine dei dati, senza necessariamente servirsi dei server in cloud – ma non sono la stessa cosa.

Aspetto	Edge Computing	Fog Computing
Definizione e luogo di elaborazione dei dati	È un modello che porta l'elaborazione dei dati il più vicino possibile (estremità o "edge") ai dispositivi e ai sensori che li generano. Utilizza gli edge server per l'elaborazione, l'archiviazione e la comunicazione locale.	L'elaborazione si sposta sui processori in LAN, che possono essere fisicamente più distanti dai sensori e dagli attuatori. Consente di elaborare i dati a più livelli, filtrando i dati rilevanti da quelli irrilevanti prima di inviarli al cloud per l'archiviazione o per l'ulteriore elaborazione. È una via di mezzo tra la terra e le nuvole, da cui il nome "fog" (nebbia).
Standard e funzioni	Definisce i concetti e le pratiche per l'elaborazione locale dei dati.	Stabilisce gli standard (OpenFog - OPC Foundation) per i servizi di elaborazione, archiviazione e comunicazione tra i dispositivi finali e il cloud.
Scalabilità	Limitata alla capacità dei dispositivi locali.	Maggiore scalabilità grazie all'uso di risorse di rete.
Scenari di utilizzo	Ideale per applicazioni che richiedono risposte in tempo reale, come il monitoraggio e il controllo nei veicoli autonomi che elaborano dati dai sensori per evitare collisioni.	Utilizzato per applicazioni che necessitano di elaborazione di grandi volumi di dati, come le Smart Cities che adottano sistemi di questo tipo per monitorare il traffico e la qualità dell'aria nelle città.

Approfondimento - Tecnologia 2

Intelligenza Artificiale: i modelli probabilistici

L'Intelligenza Artificiale (AI) riguarda lo sviluppo di sistemi e algoritmi capaci di eseguire compiti che normalmente richiederebbero l'intelligenza umana, come il riconoscimento vocale e la generazione di testo. Un aspetto fondamentale nel funzionamento dell'AI è la distinzione tra possibilità e probabilità.

- **Possibilità** si riferisce al fatto che un evento possa accadere o meno. Ad esempio, è possibile che domani piova. Tuttavia, la possibilità non ci dà informazioni su quanto sia probabile che l'evento accada.
- **Probabilità**, invece, è una misura quantitativa che permette di stimare la facilità con cui un certo evento può o meno verificarsi. Ad esempio, se le previsioni del tempo indicano una probabilità dell'80% di pioggia per domani, abbiamo una misura concreta della probabilità che l'evento si verifichi.

Gli algoritmi di Intelligenza Artificiale, specialmente quelli di apprendimento automatico, utilizzano **modelli probabilistici per effettuare previsioni e**

notabene

L'acquisizione automatica si basa su algoritmi che consentono di apprendere dai dati e migliorare nel tempo. I modelli di classificazione sono un tipo di algoritmo di apprendimento automatico che assegna delle categorie ai dati di input.

prendere decisioni, con importanti conseguenze. Nei modelli di classificazione, l'obiettivo principale è determinare a quale categoria appartiene un determinato input. Ad esempio, in un modello di classificazione binaria, si cerca di stabilire se un'e-mail è spam oppure no.

La funzione sigmoide e la temperatura

La funzione matematica **sigmoide** (Figura 1) è utilizzata spesso nelle reti neurali e nei modelli di classificazione. La funzione sigmoide prende un valore di input, che può essere qualsiasi numero reale, e lo trasforma in un valore di output compreso tra 0 e 1, che può essere interpretato come una probabilità. Ad esempio, consideriamo un modello di classificazione binaria che deve determinare se un'e-mail è spam oppure no. Quando il modello analizza un'e-mail, produce un valore di output tramite la funzione sigmoide. In base a una soglia predefinita, ad esempio 0,7, possiamo decidere che: se l'output è maggiore di tale valore, l'e-mail è considerata spam, altrimenti è accettata. Se il valore di output è, ad esempio, 0,8, possiamo interpretarlo come una probabilità dell'80% che l'e-mail sia spam. Nella generazione di testi e altri contenuti, come musica e immagini, per controllare il grado di casualità nelle risposte generate si utilizza un parametro che influenza la distribuzione delle probabilità dei possibili output: la "temperatura", che determina quanto il modello sarà creativo o prevedibile. Ad esempio:

- una temperatura bassa rende il modello più deterministico e coerente;
- una temperatura alta aumenta la variabilità e la creatività delle risposte;
- quando la temperatura è impostata a 0, il modello diventa completamente deterministico, generando sempre lo stesso output per lo stesso input.

Un esempio pratico

Le modalità "Preciso", "Bilanciato" e "Creativo" di Copilot (Figura 2), uno strumento sviluppato da Microsoft che usa modelli linguistici come GPT di OpenAI, corrispondono rispettivamente a temperature bassa, media e alta, influenzando lo stile e il tono delle risposte. La formulazione del **prompt**, cioè il modo di fornire istruzioni o domande a un modello di AI, può influenzare le risposte generate dall'AI. Ad esempio, se si sottopone al modello di AI la frase "sto facendo la doccia, squilla il telefono e...", la risposta dipende dalla temperatura impostata. Con una temperatura più alta, le risposte saranno più varie e creative. Con una temperatura più bassa, le risposte saranno più prevedibili e coerenti.

- **Preciso**: "...esco rapidamente dalla doccia, mi asciugo le mani e rispondo al telefono."
- **Bilanciato**: "...esco dalla doccia, mi avvolgo in un asciugamano e rispondo al telefono, sperando che non sia una chiamata urgente."
- **Creativo**: "...esco dalla doccia, scivolo sul pavimento bagnato e, mentre cerco di stare in equilibrio, afferro il telefono e rispondo con un sorriso divertito.

Approfondimento
Algor-etica: per uno sviluppo umano della società digitale

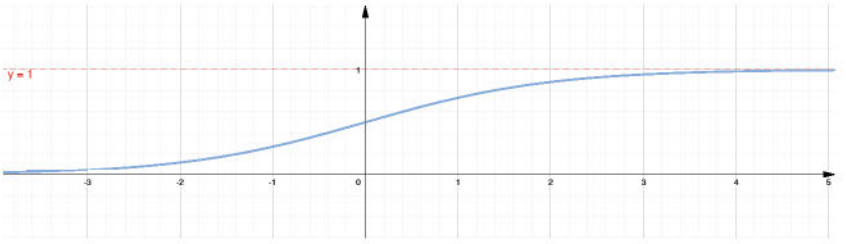


Fig. 1 Funzione sigmoide realizzata con GeoGebra.



Fig. 2 Le modalità "Preciso", "Bilanciato" e "Creativo" di Copilot sono configurazioni predefinite che influenzano lo stile e il tono delle risposte.

Approfondimento - Società

Dal transistor all'Intelligenza Artificiale

di Paolo Benanti

È accaduto qualcosa alla realtà che ci circonda. Se dovessi scrivere un titolo provocatorio, direi: «La realtà non è più quella di una volta». Questo evento si è verificato poco dopo la Seconda guerra mondiale, quando all'interno dei Bell Laboratories non è stata solo definita la realtà dell'informazione, ma è stato anche inventato e brevettato un dispositivo, il transistor, che da quel momento ha cambiato la natura degli oggetti intorno a noi. La cosa ancora più particolare è stato il modello di distribuzione di questa invenzione, che non è stata tenuta strettamente sotto il controllo della Bell Labs, ma data in licenza d'uso. Questo ha prodotto una "transistorizzazione" della realtà, cioè l'inserimento di elementi computazionali in tutto ciò che esiste. Cosa significa questo? Significa che un oggetto, come un'automobile, era definito dai pezzi meccanici di cui era composto, cioè dall'hardware. Improvvisamente è diventato una realtà definita dal software grazie al transistor. La realtà inizia quindi a essere definita dal software. Pensate a un ospedale. Se un ransomware prende possesso dei computer dell'ospedale, la natura del luogo cambia per sempre. Non è più un ospedale ma qualcos'altro. In economia si parla di commodity. La benzina è una commodity dell'auto: «tu compra da me l'auto, poi la benzina la metti dove ti pare». Ecco, l'hardware sta diventando una commodity del software: tu compri il tuo computer da chi ti pare, poi il sistema operativo lo metti tu. Ma se il software definisce la realtà, il primo grande problema è: la realtà diventa una commodity del software? Ecco che quindi stiamo cambiando le catene di potere nel mondo. Parlare di intelligenza artificiale non è più solo parlare di tecnologia, ma è diventata una questione di potere, quindi una questione che ha a che fare con quella cosa così fragile e preziosa che è la nostra democrazia. La grande domanda essenziale è come addomesticare questa tecnologia in un sistema sociale. Sembrerebbe già spaventoso così, ma questa è solo metà della risposta. L'altra metà è legata a un'altra questione. Il computer nasce in guerra, ed è uno strumento che serve a risolvere equazioni particolarmente complesse, che consentono a chi lavora a Los Alamos all'epoca di capire come devono essere posizionati l'uranio e l'esplosivo per fabbricare la prima bomba atomica. Finita la guerra, il computer si diffonde grazie all'avvento del transistor, che riesce a rendere più economica e replicabile quella potenza di calcolo. Gli anni Cinquanta e Sessanta del Novecento vedono il diffondersi del computer nelle grandi aziende, cambiandone anche la natura organizzativa; ci si riorganizza per far funzionare il computer. Nel 1970 nasce la controcultura. La parola d'ordine era: «Tutto ciò che è centralizzato è male, va ridato il potere ai singoli». Il computer che si era diffuso negli anni Cinquanta e Sessanta era una potenza di calcolo centralizzata che abitava in alcuni armadi chiamati mainframe. Ed ecco che i ragazzi della controcultura attaccano questo potere computazionale centralizzato, vogliono sgretolarlo e darlo a ciascuno di noi. Nasce il personal computer. Passa del tempo e si arriva agli anni Novanta. Di nuovo la storia bussa alla porta. Crolla il muro di Berlino. Un politologo statunitense, Francis Fukuyama, dice che la democrazia liberale ha vinto, il capitalismo è l'unico modello che rimane. Chiudiamo gli anni Duemila con un problema: l'equazione «più libero mercato uguale aumento del benessere» non è più vera, perché si può aumentare il benessere senza aumentare la democrazia.

Nel primo decennio di questo secolo, il potere computazionale assume la sua forma più personale e intima: lo smartphone. Nel 2011 arrivano le Primavere Arabe, e ciò che accade, grazie ai social network, ci fa pensare che lo smartphone e il digitale siano il miglior alleato della democrazia. Dieci anni dopo, nel 2021, le rivolte di Capitol Hill infrangono il sogno e sembra che lo smartphone, il digitale e i social network siano di fatto il peggior nemico delle nostre democrazie: fake news, post-verità e quant'altro. Ma quello che qui mi interessa è ciò che è accaduto nel 2020. Nel 2020 c'era la pandemia, e lì ci siamo resi conto che il digitale aveva surrogato le nostre vite. Potevamo firmare grazie al digitale, potevamo tenere riunioni online, potevamo andare in banca senza andare in banca...
Inizia il terzo decennio che si apre nel 2022-2023, quando la società si accorge che esiste l'Intelligenza Artificiale con l'arrivo di ChatGPT. Ecco, ChatGPT e l'Intelligenza Artificiale sono la seconda grande sfida. Perché l'arrivo dell'intelligenza artificiale non rende più visibile dove si compiono i processi computazionali. Non sappiamo più se accadono sotto il nostro potere computazionale locale o in un potere computazionale centralizzato, chiamato Cloud, che sta aspirando tutte le cose che abbiamo digitalizzato e detiene tutto il potere.
Quindi, la prima vera grande rivoluzione, la prima vera grande cyberdifesa di questo spazio digitale è l'educazione e l'impegno educativo, che è fondamentale perché noi apparteniamo a una specie unica. L'intelligenza artificiale abiterà nella nostra quotidianità e questo ci apre ad alcuni problemi. Quello che sta per accadere ci deve far interrogare su come garantire un accesso alla democrazia intergenerazionale con l'educazione, ma soprattutto su come costruire quei guardrail fondamentali per evitare che queste macchine così utili vadano fuori strada. Noi siamo la generazione che deve decidere su questo.

Biografia



Paolo Benanti (Roma, 1973) è un francescano del Terzo Ordine Regolare (T.O.R.). Teologo, si occupa di etica, bioetica ed etica delle tecnologie. In particolare, i suoi studi si focalizzano sulla gestione dell'innovazione: Internet e l'impatto del Digital Age, le biotecnologie per il miglioramento umano e la biosicurezza, le neuroscienze e le neurotecnologie.
Presso la Pontificia Università Gregoriana ha conseguito nel 2008 la licenza e nel 2012 il dottorato in teologia morale. La dissertazione di dottorato dal titolo *The Cyborg: Corpo e corporeità nell'epoca del post-umano* ha vinto il Premio Bellarmino-Vedovato.
Dal 2008 è docente presso la Pontificia Università Gregoriana, l'Istituto Teologico di Assisi e il Pontificio Collegio Leoniano ad Anagni. Oltre ai corsi istituzionali di morale sessuale e bioetica si occupa di neuroetica, etica delle tecnologie, Intelligenza Artificiale e postumano. Ha fatto parte della Task Force Intelligenza Artificiale per coadiuvare l'Agenzia per l'Italia digitale. È membro corrispondente della Pontificia accademia per la vita, con particolare mandato per il mondo delle intelligenze artificiali. A fine 2018 è stato selezionato dal Ministero dello sviluppo economico come membro del gruppo di trenta esperti che a livello nazionale ha il compito di elaborare la strategia nazionale sull'Intelligenza Artificiale e la strategia nazionale in materia di tecnologie basate su registri condivisi e blockchain. Dal 2023 fa parte del New Artificial Intelligence Advisory Board delle Nazioni Unite. Il 5 gennaio 2024 è stato nominato presidente della Commissione sull'Intelligenza Artificiale per l'Informazione del Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio dei ministri.

Laboratorio

ATTIVITÀ 1

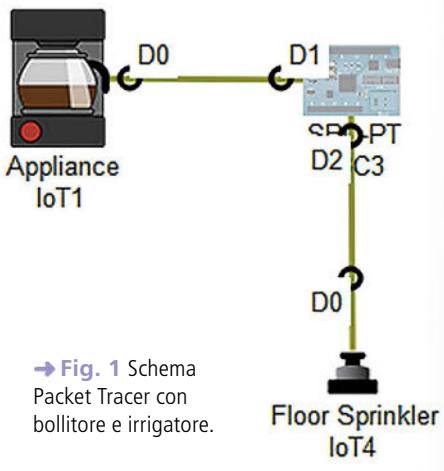
Collegare simulazione e realtà: utilizzo delle API REST in un Ambiente IoT con Cisco Packet Tracer

Scenario

L'ambiente di simulazione CISCO Packet Tracer e il mondo esterno non sono ambienti impermeabili l'uno all'altro. Esiste, infatti, la possibilità di effettuare da Packet Tracer delle chiamate HTTP API REST verso un server reale presente in Internet. In questo modo si inserisce l'anello mancante che collega il mondo simulato a quello reale.

Consegna

L'obiettivo è creare un programma in Python, presente su una scheda SBC, che faccia una richiesta API REST a un server web in Internet. Il programma, che controlla alcuni dispositivi di un ambiente IoT simulato, interpreta il codice di risposta del server (positivo, codice 200, o negativo) per intraprendere azioni semplici sugli oggetti intelligenti collegati alla scheda SBC. L'esempio contiene solo gli elementi essenziali utili al funzionamento, ma può essere ampliato per comprendere scenari più complessi come il monitoraggio ambientale, o sistemi di gestione dell'energia in collegamento con un sito web reale, o applicazioni con architettura a più livelli.



➜ Fig. 1 Schema Packet Tracer con bollitore e irrigatore.

Svolgimento

Passo 1: creazione dell'ambiente IoT in PT
L'ambiente è quello mostrato in Figura 1 e Figura 2 e contiene:

- un sistema SBC programmato in Python con due dispositivi intelligenti collegati;
- un bollitore;
- un irrigatore (sprinkler).

Passo 2: Analisi del Programma Python su SBC
Testo del programma: "Chiamare un server web in Internet: se il server risponde positivamente allora si accenda il bollitore con un buon caffè per festeggiare. Altrimenti, come alternativa, si innaffi il giardino."

Passo 3: Il programma Python su SBC

```
from real http import *
from time import *
from gpio import *

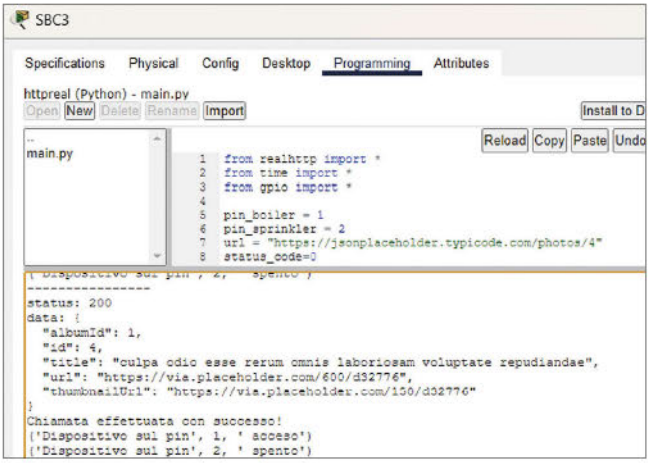
pin _ boiler = 1
pin _ sprinkler = 2
url = "https://jsonplaceholder.typicode.com/photos/4"  #server Web
status _ code=0
```

```
def control _ device(pin, state):
if state == "on":
        customWrite(pin, HIGH)
        print("Dispositivo sul pin", pin," acceso")
else:
        customWrite(pin, LOW)
        print("Dispositivo sul pin", pin," spento")

def onHTTPDone(status _ code, data):
    print("status: " + str(status _ code))
    print("data: " + data)
if status _ code == 200: #risposta positiva
    print("Chiamata effettuata con successo!")
    control _ device(pin _ boiler, "on")  # Accende il bollitore
    control _ device(pin _ sprinkler, "off")  # Spegne il sistema
    di irrigazione
else:
    print("Errore nella chiamata:", status _ code)
    #risposta negativa da parte del server
    control _ device(pin _ boiler, "off")  # bollitore Off
    control _ device(pin _ sprinkler, "on")  # Accende il sistema
    di irrigazione

def real _ call():
    print ("-----------------")
    http = RealHTTPClient() #Creazione dell'istanza di
    RealHTTPClient
    status _ code=http.onDone(onHTTPDone)  # callback
    http.get(url)   # Esecuzione del metodo GET

def main():
    # per sempre…
    while True:
        real _ call()
        sleep(10)  # Attende 10 secondi prima di effettuare
        un'altra chiamata
if _ _ name _ _ == " _ _ main _ _ ":
    main()
```



➔ **Fig. 2** Schermata di output del programma Python su SBC.

Dettagli tecnici di programmazione

- La funzione **RealHTTPClient()** in Packet Tracer permette di inviare richieste HTTP (API REST) reali verso qualsiasi sito web o servizio presente su una rete esterna. Può utilizzare i metodi REST come ad esempio get, post e put (si veda la documentazione presente in https://tutorials.ptnetacad.net/help/default/iot_python_api.htm).

notabene

Le API REST interagiscono con il controller SDN (Software-Defined Networking) presente in Packet Tracer, che gestisce la spedizione dei pacchetti in rete.

- **onHTTPDone** è la funzione di callback che viene chiamata automaticamente quando la richiesta HTTP è completata. La funzione onHTTPDone riceve il codice di stato della risposta HTTP e permette di gestire la risposta in modo asincrono. Infatti, le richieste HTTP possono richiedere del tempo per essere completate e il programma non deve bloccarsi per attendere l'esito delle operazioni.
- Il link https://jsonplaceholder.typicode.com/photos/4 chiama, tramite API, il contenuto di una cartella su un server in Internet che restituisce i dati di una foto che ha ID uguale a 4.

notabene

JSONPlaceholder è un servizio gratuito che mette a disposizione un server REST API, utilizzato per test, con dati fittizi per verificare applicazioni che fanno chiamate API.

Note di Sicurezza

Gli attacchi agli ambienti IoT, come abbiamo più volte segnalato, sono una preoccupazione reale. Dispositivi come luci, termostati e sensori intelligenti sono spesso bersaglio di intrusioni che sfruttano vulnerabilità per prendere il controllo e lanciare offensive verso altri sistemi, come nel caso degli attacchi DoS. Ad esempio, rifacendoci al caso di chiamata di un server web reale da PT, se un hacker riuscisse a inserire un codice malevolo in un dispositivo IoT, come nel codice nativo di un LED, potrebbe utilizzarlo per compiere azioni dannose. Il codice mostrato in tabella è solo un esempio indicativo, che però ci permette di riflettere su scenari reali e aumentare la nostra consapevolezza sulle minacce informatiche e sul modo in cui gli hacker possono manipolare i dispositivi.

codice nativo di LED in Packet Tracer	codice con malware inserito nel LED in Packet Tracer

…
def main():
  setup()
  while True:
  updateEnvironment()
  delay(500)
	…
	def main():
	  setup()
	  http = RealHTTPClient() # HTTP Client.
	  http.onDone(onHTTPDone) # callback
	  while True:
	  updateEnvironment()
	  delay(500)
	  # Simulazione di un attacco DoS
	  for i in range(1000): # 1000 richieste rapide
	  http.get(url) # contatta il sito target
	  sleep(1) # ritardo di 1 secondo

ATTIVITÀ 2

Domotica con registration server

Scenario

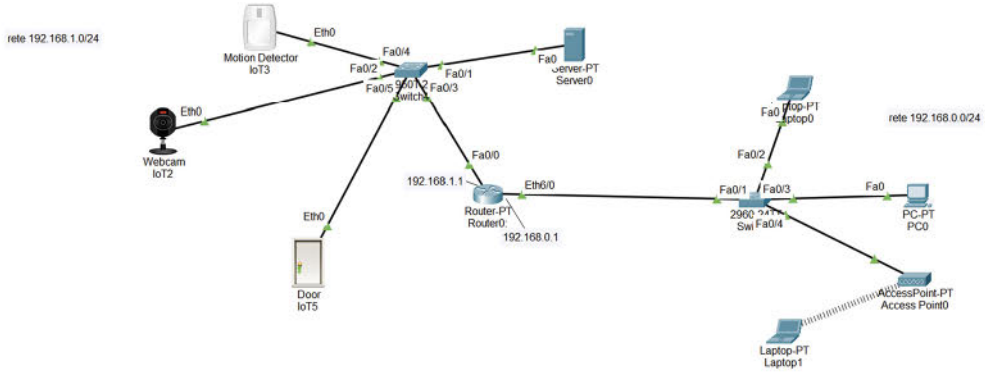
In questa attività mostreremo un esempio di progettazione di una casa intelligente che utilizza un registration server per la gestione dei dispositivi intelligenti a cui è possibile accedere da remoto.
Vediamo come gestire una porta, una webcam e un rilevatore di movimento. Utilizziamo un registration server che, oltre a collegare i vari dispositivi domestici, fornisce un'interfaccia web per monitorare e controllare i dispositivi.

Consegna

Utilizzare Cisco Packet Tracer per progettare una casa intelligente con dispositivi che possono essere gestiti tramite un laptop da remoto e un'applicazione web. I dispositivi sono collegati a un registration server.
La rete comprende:

- sensore di movimento;
- porta che può essere aperta, chiusa (non a chiave, o a chiave);
- webcam;
- server di registrazione.

La rete domestica è collegata a un'altra rete a cui appartiene il laptop usato per il monitoraggio della rete domestica intelligente.

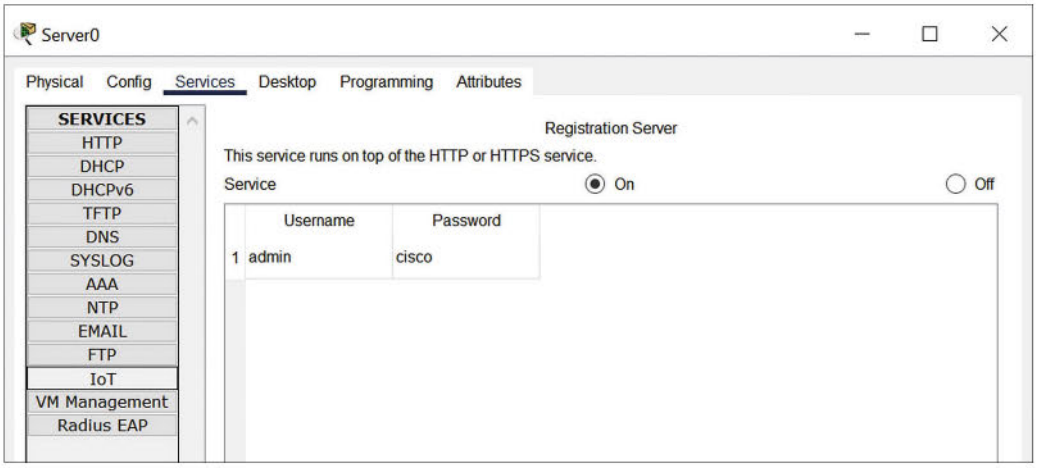


Svolgimento

Passo 1

- Disporre tutti i dispositivi sul piano di lavoro.
- Configurare la rete domestica e assegnare indirizzi IP appartenenti alla rete 192.168.1.0/24.
- Configurare la rete remota e assegnare indirizzi IP appartenente alla rete 192.168.0.0/24.
- Configurare le interfacce del router.
- Collegare opportunamente tutti i dispositivi.

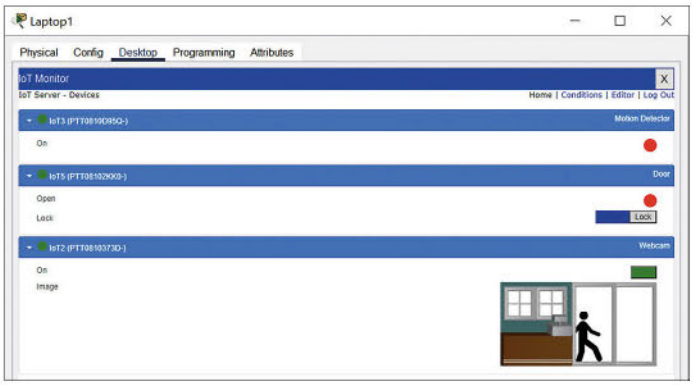
Passo 2
Configurare il server come server IoT e assegnare username e password per l'accesso da remoto.



Passo 3
Collegare i dispositivi di IoT al server.

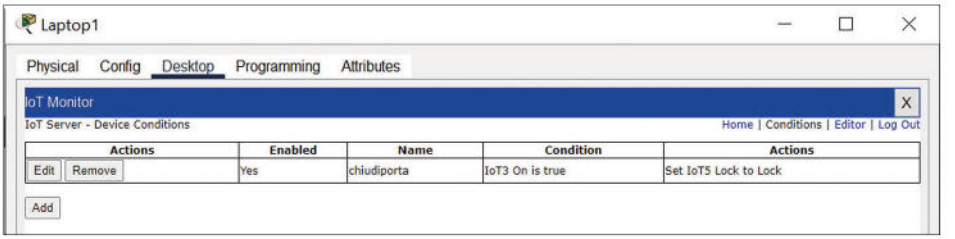


Passo 4
Dal desktop remoto, accedere alla scheda IoT Monitor, collegarsi al server con il corretto indirizzo IP e le credenziali. Saranno visualizzati i dispositivi della smart home e lo stato in cui si trovano.



Passo 5

È possibile anche impostare delle condizioni per programmare il comportamento dei dispositivi, sempre tramite l'interfaccia web. La figura seguente mostra un esempio di impostazioni della condizione: se il sensore di movimento rileva qualcosa, chiudi a chiave la porta.

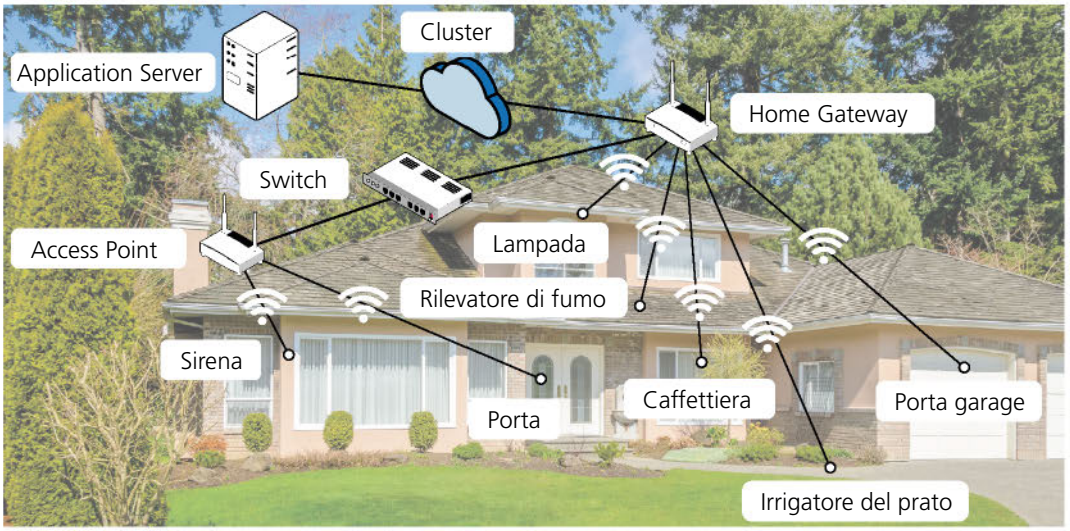


ATTIVITÀ 3

Domotica con home gateway

Scenario

In questa attività, presentiamo il progetto di una casa intelligente che utilizza un home gateway. A titolo di esempio, gestiremo alcuni dispositivi comuni che possono essere utilizzati in una casa con garage e giardino. Utilizzeremo un home gateway che, oltre a collegare i vari dispositivi domestici, fornisce un'interfaccia web per monitorare e controllare i dispositivi tramite una connessione wireless e/o cablata. Inoltre, collegheremo i dispositivi alla rete internet per inviare i dati rilevati a un server in cloud, permettendo così di effettuare elaborazioni statistiche. Ad esempio, un lampione potrebbe inviare a un'applicazione in cloud i dati relativi agli orari di accensione e spegnimento, al tempo in cui la luce resta accesa ecc.



Consegna

Utilizzare Cisco Packet Tracer per progettare una casa intelligente con dispositivi che possono essere gestiti tramite uno smartphone e un'applicazione web. La casa è suddivisa in tre aree: abitazione, garage e giardino.

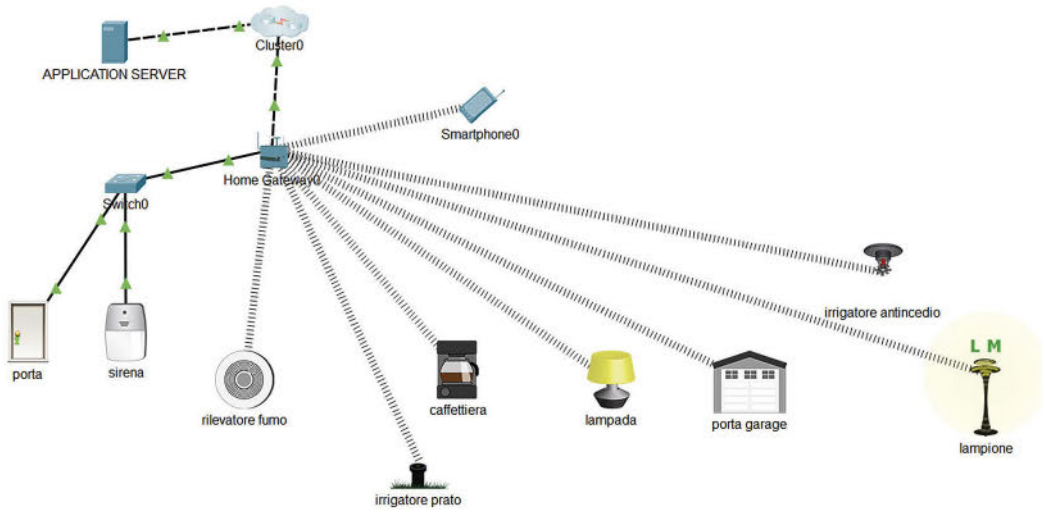
La rete comprende i seguenti dispositivi opportunamente collocati nei luoghi di interesse.

- Nell'abitazione: porta, sirena, rilevatore di fumo, lampada, caffettiera.
- In garage: porta automatica e irrigatore antincendio.
- In giardino: irrigatore per il prato, lampione.

I dispositivi sono collegati direttamente a un home gateway oppure, in base alle distanze, a uno switch intermedio. Tramite uno smartphone è possibile monitorare e governare i dispositivi. L'autenticazione per l'accesso alla rete WiFi è fatta con WPA2 con chiave condivisa.

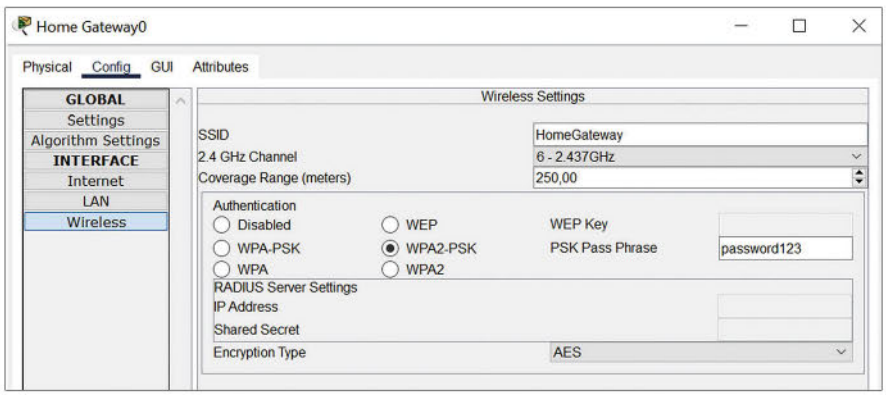
Svolgimento

Passo 1: disposizione di tutti i dispositivi sul piano di lavoro



Passo 2: configurazione dell'home gateway

- Assegnare un valore a SSID per identificare la rete. Nel nostro caso HomeGateway.
- Selezionare il metodo di autenticazione WPA2-PSK e assegnare la password. Nel nostro caso "password123".

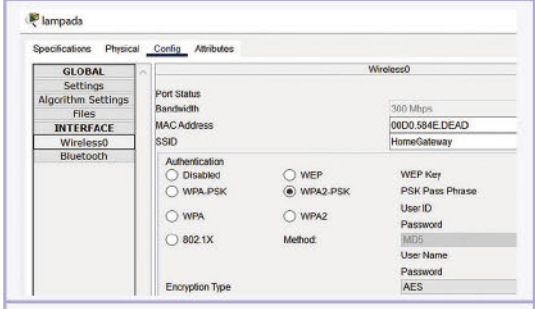


Passo 3: configurazione dei dispositivi

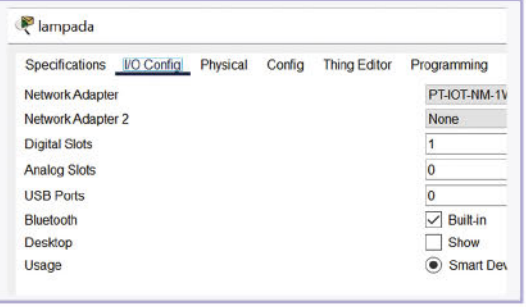
A titolo di esempio mostriamo come configurare la sirena.

Effettuare le stesse operazioni per gli altri dispositivi. Per il collegamento all'access point assegnare un SSID per ogni access point.

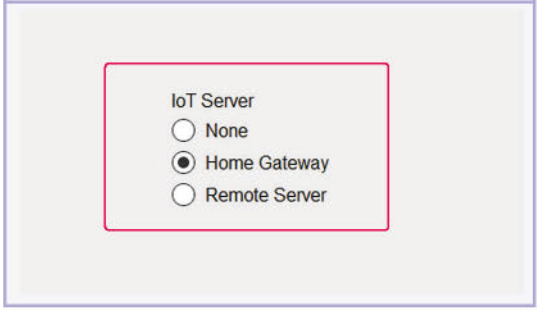
Nella scheda *config* → *wireless* configurare SSID e autenticazione come nell'home gateway



Nella scheda *config* → *I/O Config* assicurarsi che il Network Adapter sia quello per il wireless

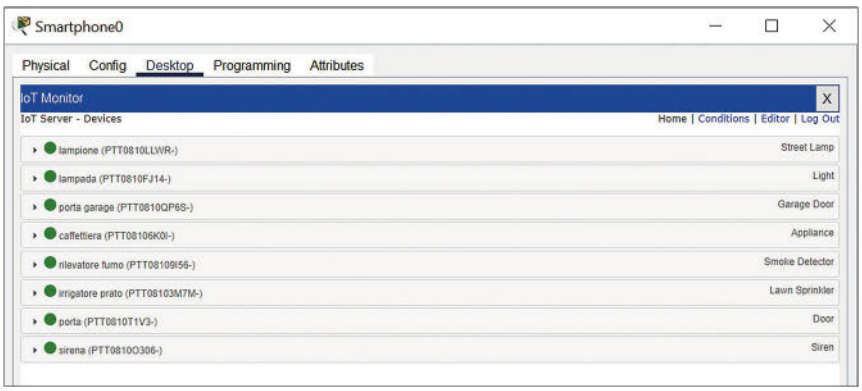


Nella scheda *config* → *setting* assegnare a IoT Server l'home gateway



Passo 4: monitoraggio da remoto

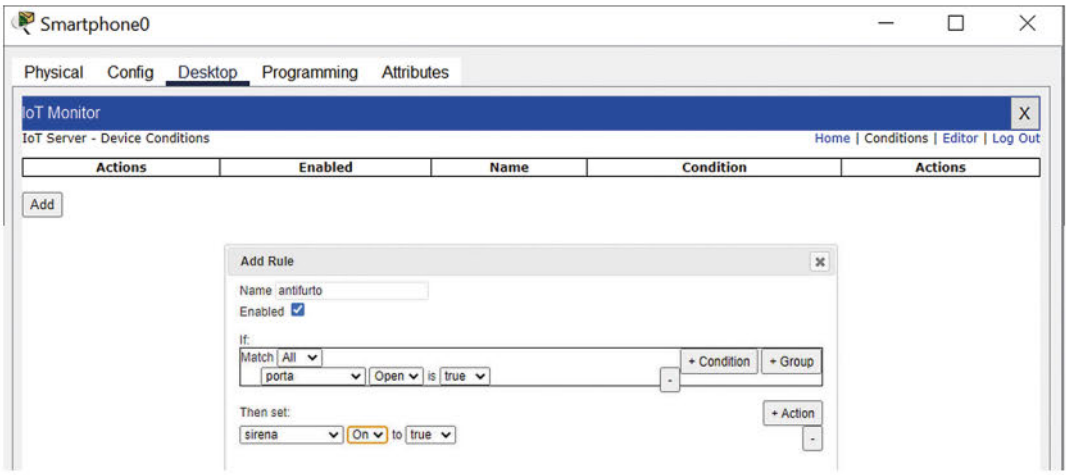
Dalla scheda *desktop* → *IoT monitor* dello smartphone accedere al pannello di controllo. Saranno visualizzati i dispositivi della smart home e lo stato in cui si trovano.



Per verificare il funzionamento del sistema provare ad aprire e chiudere la porta, attivare o spegnere l'irrigatore del prato e verificare le variazioni di stato sull'interfaccia web dell'applicazione.

Passo 5: impostazione condizioni

È possibile anche impostare delle condizioni per programmare il comportamento dei dispositivi, sempre tramite l'interfaccia web. Questo metodo è intuitivo, semplifica molto la gestione della casa intelligente e può essere utilizzato anche senza avere particolari competenze di programmazione. Per esempio, impostiamo una condizione affinché, quando si aprirà la porta, suoni la sirena. Accedere al menu *Conditions* dell'interfaccia web e impostare le condizioni come mostrato nella figura.



ATTIVITÀ 4

Utilizzo di Packet Tracer per programmare un MCU (Arduino) o un SBC (Raspberry)

Scenario

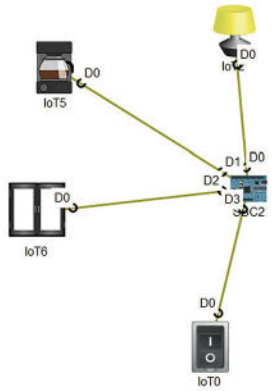
Questa attività è realizzata usando il simulatore Packet Tracer che fornisce un insieme di sensori, attuatori e microcontrollori che possono essere collegati in rete per rendere più realistica la simulazione dei dispositivi. Packet Tracer dispone di *smart thing* ("oggetti intelligenti") da programmare che si connettono ai microcontrollori (MCU-PT) o ai *Single Board Computer* (SBC-PT) attraverso ingressi e uscite analogiche o digitali. Alla famiglia dei microcontrollori (MCU-PT) appartiene Arduino, mentre Raspberry Pi fa parte della famiglia dei Single Board Computer (SBC-PT) .

Consegna

Utilizzare Cisco Packet Tracer per progettare un'area relax con dispositivi gestiti tramite un SBC. La rete comprende un interruttore, una lampada, una caffettiera e una finestra. Quando si preme l'interruttore, si accendono la lampada e la caffettiera, e si apre la finestra. Quando si apre l'interruttore, la finestra si chiude e si spegne la lampada.

notabene

In Packet Tracer, il componente SBC (*Single Board Computer*) può essere associato a un Raspberry Pi, mentre un MCU (*Micro Controller Unit*) può essere paragonato ad Arduino.



La caffettiera si spegne dopo un tempo prestabilito.

Svolgimento

Il programma associato a SBC è il seguente.

```
from gpio import *
from time import *

def main():
      pinMode(0,OUT)   #lampada
      pinMode(1, OUT) #caffettiera
      pinMode(2, OUT) #finestra
      pinMode(3,IN)    #interruttore 1

      customWrite(0,"0");
      customWrite(1,"0");
      customWrite(2,"0");
      statoint1=0;

      while True:
            statoint1=digitalRead (3)
            if statoint1 == HIGH:
                  customWrite(0,"1");  #accendo lampada
                  customWrite(1,"1");  #accendo la caffettiera
                  customWrite(2,"1");  #apro la finestra
            if statoint1 == LOW:
                  customWrite(0,"0"); #spengo lampada
                  customWrite(1,"0"); #spengo la caffettiera
                  customWrite(2,"0"); #chiudo la finestra

if _ _ name _ _ == " _ _ main _ _ ":
      main()
```

INTERNET OF THINGS

Sistema complesso costituito da dispositivi intelligenti interconnessi che scambiano dati: sensori, attuatori, sistemi intelligenti, reti di comunicazione e protocolli, piattaforme di gestione dei dati.

ARCHITETTURA

È strutturata in diversi livelli.

- Livello dei sensori e dispositivi.
- Livello di raccolta e trasmissione dei dati.
- Livello di elaborazione e analisi dei dati.
- Livello delle applicazioni.

CAMPI DI APPLICAZIONE

- Industriale, agricolo ed energetico.
- Commerciale e delle vendite.
- Servizi: Smart City, sanità e persona, logistica, automotive.
- Domotica.

SICUREZZA

Elementi di criticità:

- qualità dei dispositivi;
- quantità dei dispositivi;
- posizionamento dei dispositivi;
- impatto sulla privacy.

Verifica delle CONOSCENZE

Vero o Falso?

1 Tramite IoT è possibile raccogliere dati non strutturati. V F

2 La tecnologia IoT è comoda perché non necessita della rete Internet. V F

3 Gli oggetti di IoT si dicono intelligenti perché interpretano i dati e ottengono informazioni. V F

4 IoT e Cloud Computing sono due tecnologie ben separate. V F

5 Un sistema IoT è paragonabile a un ecosistema. V F

6 Nell'ecosistema IoT i dati raccolti vengono sempre inviati direttamente al cloud. V F

7 Compito del gateway è raccogliere i dati, consolidarli e inviarli a un server in cloud. V F

8 In IoT la raccolta dati è fatta tramite form. V F

9 Uno dei problemi di IoT è legato al consumo energetico dei sensori. V F

10 Un sensore è un elemento di un sistema IoT. V F

11 Edge computing e fog computing sono sinonimi. V F

12 Un semplice sistema IoT è difficilmente soggetto ad attacchi informatici. V F

13 I dati raccolti dai sensori sono sempre usati in ambito locale. V F

14 Smart City è un modello di applicazione dell'IoT. V F

15 Il posizionamento dei dispositivi IoT è cruciale per la sicurezza. V F

16 IoT non pone problemi di privacy perché gli oggetti sono di proprietà privata. V F

17 IoT è una tecnologia che può essere usata solo da grandi aziende perché è costosa. V F

18 Un sistema di domotica non può essere collegato a Internet. V F

19 Il fog computing permette a dispositivi smart di collegarsi a sistemi di elaborazione locali. V F

20 È molto semplice collegare dispositivi intelligenti a prescindere dai protocolli usati. V F

Rispondi ai seguenti quesiti indicando l'unica risposta esatta.

21 IoT necessita di:

a cavi di rete lunghi
b programmatori sofisticati e altamente specializzati
c connettività, cloud computing, sistemi di analisi dei dati
d grandi disponibilità economiche

22 La raccolta dati in Iot avviene:

a tramite sensori
b con un'interfaccia grafica
c manualmente
d con apposite penne

23 Il gateway:

a interconnette le LAN
b è un server i cloud
c è un dispositivo intermedio che raccoglie i dati rilevati dai sensori e li invia a un server
d serve solo per motivi di sicurezza

24 Home assistant:

a è scritto in Java
b è sviluppato in Python
c è utilizzato per applicazioni industriali
d lavora in cloud

25 Nell'architettura di un sistema IoT:

a i livelli sono costituiti da livello fisico, rete e applicazione
b i livelli sono costituiti da rilevamento dati, trasmissione, elaborazione e analisi dei dati
c i livelli sono costituiti da livello dei sensori e livello degli attuatori
d il numero dei livelli dipende dai protocolli e dalle distanze tra gli oggetti

26 Gli ambiti di applicazione dell'IoT possono essere:

a data base e applicazioni web
b sviluppo applicazioni con interfaccia grafica
c sanità, domotica, Smart City
d applicazioni locali

Domande per la prova orale

27 Cosa si intende per Internet delle cose?

28 Quali sono i possibili impatti dell'IoT sulla nostra vita quotidiana?

29 Descrivi i passaggi effettuati dai dati da quando sono raccolti tramite sensori a quando vengono elaborati per trarne informazioni.

30 Qual è la differenza tra dati e informazioni?

31 Quali sono le tecnologie abilitanti per IoT?

32 Perché spesso è necessario usare un gateway?

33 Quali sono le differenza tra una tradizionale architettura Internet e IoT?

34 Quali sono i principali fattori di criticità per la sicurezza dei sistemi IoT?

35 Come è strutturato un sistema IoT? Quali sono le componenti fondamentali?

36 Che cosa lega IoT, Intelligenza Artificiale e Cloud Computing?

Verifica delle ABILITÀ

37 Progetta un sistema IoT per la gestione di una serra intelligente, utilizzando sensori di umidità e di luce. Specifica:

- come utilizzare i sensori;
- i protocolli utilizzati;
- eventuali attuatori.

Disegna la rete ipotizzando che i dati rilevati siano inviati a un server in cloud.
Realizza la rete utilizzando Packet Tracer.

38 Analizza i sistemi IoT che possono essere utilizzati in una Smart City e sintetizza le informazioni riportandole in tabella.

Sistema	Ambito di utilizzo	Vantaggi	Schema di funzionamento
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

Disegna la rete di uno dei sistemi individuati.
Realizza la rete con Packet Tracer.

39 Progetta una sistema di domotica di una casa su due piani con giardino.
La casa deve essere dotata dei seguenti dispositivi intelligenti:
lampioni, antifurto, ventilatori, termostato, apertura automatica delle porte e delle finestre.

Motiva la scelta degli apparati di rete utilizzati.

Esercizi in più

Internet of Things

Abstract

In recent years there has been a great development in the field of the Internet of Things (IoT): a system of intelligent objects connected to the Internet and communicating with each other or with other systems without the intermediation of human intervention. One of the most relevant objectives of the IoT is to collect data via sensor devices. Depending on the situations, the collected data can be processed locally (fog computing) in order to be immediately used for quick decision-making, or they can be sent to servers in the cloud with the aim of being analyzed to get information. Data are in fact the fuel of artificial intelligence and come from various sources, including the IoT.
In order to do this, connectivity, Cloud Computing systems and data analysis technologies are needed.

Questions

Answer all questions

1 What is the Internet of Things?

2 How are data collected from objects?

3 What are IoT's goals?

4 Describe the architecture of IoT.

Choose the correct answer

5 IoT uses:
- a personal computers
- b microcontrollers
- c laptop
- d mainframe

6 Sensors can be considered:
- a input peripherals
- b data analysis devices
- c output peripherals
- d artificial intelligence algorithms

7 The critical factors of IoT security are:
- a size of devices
- b quantity, quality, placement of devices
- c architecture in layers
- d there are no particular critical factors

8 The gateway:
- a is interposed between objects and servers
- b is interposed between servers and routers
- c solves security problems
- d is a Cloud Computing device

Crosswords

Across

4 Detects data from the physical world

6 The servers to which the collected data is transmitted are located there

7 IoT model serving citizens

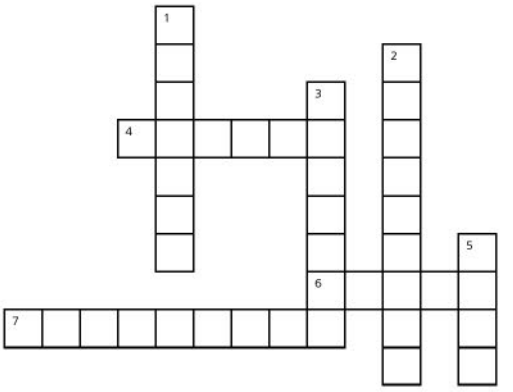
Down

1 Connecting IoT devices together

2 IoT model for home automation

3 It is a risk factor in IoT systems

5 Data processing level near the sensors



Verifica delle COMPETENZE

Tema 3

1 Rispetto alla virtualizzazione, discuti i vantaggi relativi ad affidabilità e sicurezza.

2 Discuti il problema della migrazione di macchine virtuali.

3 Discuti i vantaggi della virtualizzazione dei server nelle aziende.

4 Consulta il Web per risolvere il problema su "come scegliere un server virtuale". Riporta le principali caratteristiche da considerare.

5 Discuti gli aspetti legati al Cloud Computing erogato tramite Cloud pubblico.

6 Discuti il problema dell'esternalizzazione dei dati relativamente alle soluzioni in Cloud Computing pubblico.

7 Consulta il Web per cercare informazioni su un uso consapevole dei servizi in Cloud e riporta in una tabella i punti principali, indicando anche i siti da cui hai tratto le informazioni.

8 Consulta il Web per trovare informazioni su come gestire i dati in una soluzione in Cloud e riporta in una tabella i punti principali, indicando anche i siti da cui hai tratto le informazioni.

---

9 Consulta siti e risorse web alla ricerca di documenti che parlino della dematerializzazione, cioè della trasformazione di un documento da materiale a immateriale per essere elaborato e conservato nel Cloud ed essere fruibile in qualsiasi momento da qualsiasi luogo. Analizza criticamente le informazioni ottenute e completa la tabella seguente.

1. Sicurezza delle transazioni economiche, modalità di pagamento e criptovalute
2. Tutela dei dati e della privacy
3. Velocità della rete
4. Comportamenti in rete
5. Nuovi modelli di business
6.
7.

10 Caso di studio – Software per il monitoraggio di flotte aziendali.

"Visirun" è un localizzatore GPS per il controllo satellitare per flotte aziendali.

1. Accedere al sito aziendale (`https://www.verizonconnect.com/it/`).
2. Prendere in esame le funzioni elencate e aggiungerne altre.
3. Completare la tabella seguente evidenziando per ogni funzione pro e contro e dandone una valutazione in termini di qualità e prezzo.

Funzioni	Pro/contro/note	Valutazione
Gestione missioni e percorsi pianificati. Posizione veicoli in tempo reale con informazioni sul traffico		...../10
Percorso veicoli		...../10
Consumi carburante		...../10
Controllo ore di guida in tempo reale da tachigrafo e via GPS		...../10
Eventi e allarmi anche via messaggi		...../10
Sicurezza		...../10
Controllo temperature trasporti refrigerati		...../10
Manutenzione mezzi e scadenze		...../10
Collegamenti		...../10

11 Caso di studio – Biblioteche Scolastiche Innovative (BSI)

La biblioteca didattica si è evoluta da semplice ambiente per la lettura di libri cartacei a uno spazio articolato con vari servizi per la socializzazione e il lavoro di gruppo.

Il progetto BSI prevede:

- Postazioni informatiche e multimediali insonorizzate.
- Uno spazio per il lavoro di gruppo.
- Una postazione per il docente con uno spazio di lavoro dedicato e la possibilità di controllare da remoto il lavoro degli studenti.
- Un software per monitoraggio, gestione, organizzazione e collaborazione, che consente l'interazione tra la lavagna e i monitor degli studenti (ad esempio, NetSupport School).
- Un angolo per incontri informali e momenti di relax con musica di sottofondo.
- Possibilità di collegamento BYOD (*Bring Your Own Device*) per tutti.
- Collegamento a Internet e ad altre aule didattiche dello stesso plesso, con la possibilità di condivisione della lavagna.
- Possibilità di registrazione delle lezioni per usufruirne in tempo differito via streaming.
- Disporre di un Learning Management System (ad esempio, Moodle) per salvare i lavori degli studenti.

Inoltre (IoT):

- Comfort degli studenti garantito: temperatura, umidità e luci dell'ambiente si regolano automaticamente in base ai parametri ambientali e al numero di studenti presenti.

Compito:
disegna uno schema della BSI e progetta la topologia di rete utilizzando, per esempio, Packet Tracer.

Orientamento al lavoro

ORIENTAMENTO STEM Tema 3

L'ecosistema IoT (Internet of Things)

Contesto

Negli ultimi anni tutta la società è stata coinvolta in un percorso di evoluzione digitale che impatta su tutti i segmenti industriali e di erogazione servizi sia per le imprese sia per l'utente finale. Gli obiettivi di questa evoluzione (che molti definiscono una nuova rivoluzione industriale) è migliorare l'efficienza dei processi produttivi e di vendita, la creazione di nuovi servizi e la definizione di un diverso approccio al cliente, con particolare attenzione all'interazione tra cliente e chi eroga il servizio, inclusa la pubblica amministrazione. Tutto questo è permesso da alcuni abilitatori tecnologici quali il Cloud, l'Intelligenza Artificiale e l'Internet of Things (IoT), ovvero la possibilità di raccogliere dati in maniera capillare e massiva da sensori dislocati anche nei punti più remoti o in condizioni estreme. Tutto ciò sta influenzando non solo il mondo del lavoro ma il modo in cui vivremo nel futuro (e già in parte viviamo).

Intervista a

Paolo Bossi, ingegnere nucleare. Ha iniziato da subito a lavorare nel mondo delle telecomunicazioni, primariamente con funzioni di marketing di prodotto in aziende fornitrici di apparato. Entrato in Infostrada al suo inizio come architetto di rete dati e IP, passato poi in Wind come marketing B2B, è arrivato a esserne il responsabile per la parte grandi clienti. È poi passato come TLC Product Manager in Vimpelcom/Veon ad Amsterdam. Attualmente collabora con alcune aziende e startup nel mondo dell'IoT e dell'Intelligenza Artificiale.

Quali sono i settori aziendali che si occupano di Internet of Things?

L'evoluzione digitale interessa tutti i settori aziendali, anche quelli che potrebbero sembrare lontani come, per esempio, l'area Human Resource. Pensando più specificamente all'IoT, il mondo della produzione e automazione industriale ne è forse uno dei principali attori: sensori distribuiti sulla catena produttiva rilevano i vari parametri di interesse permettendo una maggior efficienza e anche una maggior sicurezza. Anche l'agricoltura fa uso dell'IoT: sensoristica distribuita sui campi permette una rilevazione dettagliata delle condizioni ambientali regolando di conseguenza in maniera più opportuna l'erogazione di acqua, fertilizzanti, e così via. Ma di esempi ve ne sono tantissimi.

Chi sono i clienti e i fornitori?

La complessità e la necessità di avere competenze molto diversificate fanno sì che si creino degli ecosistemi di fornitori che si alleano per rispondere in maniera completa alla richiesta del cliente finale. Spesso in queste alleanze il ruolo di fornitore/cliente si scambia a seconda del contesto. È importante sottolineare come l'obiettivo sia erogare un servizio e non vendere un prodotto.

Qual è il mercato oggi e qual è la previsione per i prossimi anni?

A livello mondiale i dati di mercato dell'IoT danno una crescita anno su anno a due cifre, sia per ciò che concerne il fatturato sia per gli elementi connessi; ma anche l'Italia ha un trend simile. Un aspetto frenante è il *know how* delle persone, la mancanza di un certo tipo di professionalità che rallenta lo sviluppo delle aziende.

Qual è la figura professionale che è richiesta in questo ambito?

Primariamente tecnici informatici, data analyst, figure professionali che sappiano coniugare elettronica, meccanica e informatica (meccatronici). Persone che abbiamo anche una visione economica del contesto, in grado quindi di coniugare tecnica con efficienza economica.

Che tipo di formazione deve avere?

Come detto prima principalmente diplomati in informatica, elettronica, meccatronica e ingegneri di vario tipo. La lingua inglese è indispensabile.

Ci racconta un po' la sua esperienza, la sua storia, il rapporto con colleghi?

Sono entrato in azienda in un periodo in cui non si aveva la posta elettronica (al massimo X.400), i programmi più evoluti erano i text editor e le centrali

di telecomunicazioni erano, in alcuni casi, ancora analogiche e non digitali. In Italia vi erano ancora fabbriche che producevano apparati TLC con migliaia di operai e grandi operatori del settore. Una parte del sapere era ancora tramandata da persone con esperienza aziendale. Oggi abbiamo un mondo molto più rapido e semplice per tanti aspetti, ma è evidente a tutti come siamo diventati in Italia (e quasi in tutta Europa) soltanto un mercato nel quale a vendere sono altri. Il *know how* non nasce ormai più qui. L'aspetto fortemente positivo è però la possibilità di accedere abbastanza facilmente a questo *know how*, almeno a un primo livello, da parte di tutti, tramite quell'enorme biblioteca di Babele che è Internet. Vedo anche in Italia tante startup sui temi più innovativi che fanno sperare in un futuro non completamente grigio.

La cosa più bella e quella più brutta della sua esperienza lavorativa?

Le esperienze più positive che ho avuto vengono quando un progetto complesso viene portato a compimento e le aspettative dei clienti sono raggiunte. Nel mio caso sicuramente il lancio della rete nazionale dial-up di Infostrada. Le negative, quando un buon progetto fallisce per motivi esterni, diciamo politici, anche quando tutto è ormai positivamente indirizzato. Mi è capitato un paio di volte ed è molto demoralizzante.

È contento del suo lavoro? Lo sceglierebbe di nuovo?

Difficile domanda. Probabilmente sì, ma in alcuni momenti specifici avrei fatto un altro tipo di scelta.

Sfida finale

ORIENTAMENTO STEM

Tema 3

XOLOMON – Monitoraggio del livello di un fiume a carattere torrentizio

Scenario

Il progetto nasce da un caso reale: la necessità di monitorare un tratto di un fiume a carattere torrentizio che attraversa luoghi densamente urbanizzati (Figura 1).
In caso di esondazione, per la conformazione del territorio, le acque rischiano di isolare la zona rendendo difficoltosa l'evacuazione di persone, animali e cose che vi restano intrappolate.
Il sistema consente il monitoraggio continuo del livello, della portata e di altri parametri fisici del fiume in un punto particolare del suo tragitto.
Lo scopo del progetto non è solo quello di rilevare e segnalare, in loco, eventuali situazioni di criticità, ma anche quello di trasmettere in Cloud i dati raccolti per ulteriori analisi statistiche e di previsione.
I dati rappresentano, nella logica IoT e dei big data, il "carburante" che serve agli algoritmi di analisi per estrarre le informazioni utili a prevedere e prevenire eventi catastrofici.



Fig. 1 Il fiume da monitorare.

Obiettivi

- **Tenere sotto controllo la portata del fiume in modo da intervenire tempestivamente per mitigare situazioni critiche.**

Consegna

1. Studiare le basi del progetto proposto, individuando i passaggi chiave, le tecnologie e i protocolli utilizzati.
2. Applicare il modello a un contesto simile, per esempio rilevare l'inquinamento atmosferico, la qualità del suolo in un ambito agricolo, ecc.

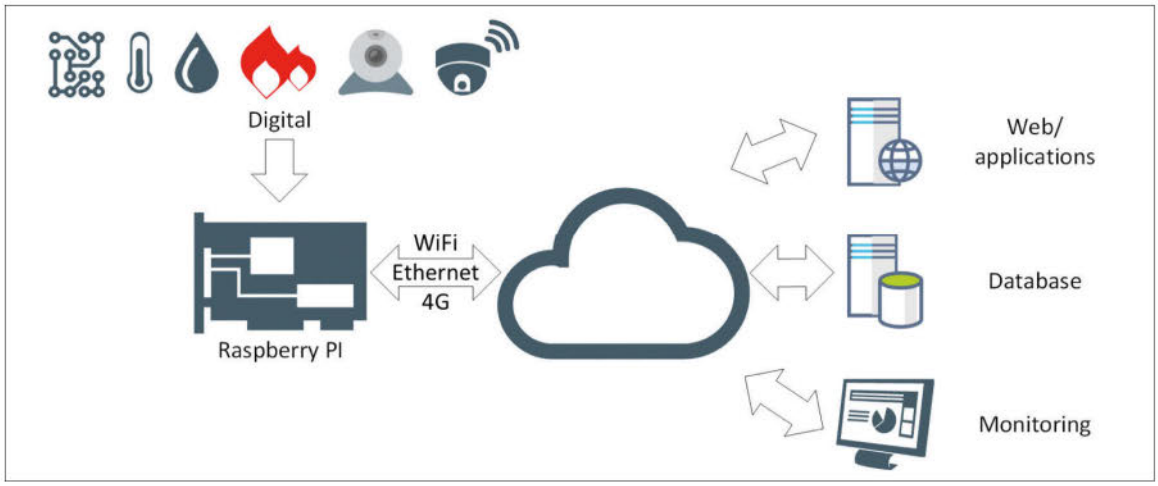
Il progetto

La Figura 2 illustra il principio di funzionamento della rete di acquisizione e trasmissione dei dati (2a) e l'interfaccia Web per l'utente con i grafici dei dati rilevati (2b).
Sostanzialmente la rete è divisa in tre parti secondo il classico schema di acquisizione ed elaborazione dati, tipico dei sistemi IoT:

- una parte locale in cui vengono rilevati i dati con sensori collegati direttamente a un microcontrollore che ne fa una pre-elaborazione e si collega in Internet;
- una parte remota, con i server in cloud, a cui i dati vengono inviati e dove vengono salvati ed elaborati;
- le applicazioni con cui gli utenti finali possono accedere alle informazioni.

La parte locale di acquisizione dati utilizza un microcontrollore Raspberry Pi. La scelta è motivata dal fatto che la centralina di rilevamento deve essere a basso costo, versatile e aperta a nuove esigenze che possono

a



b

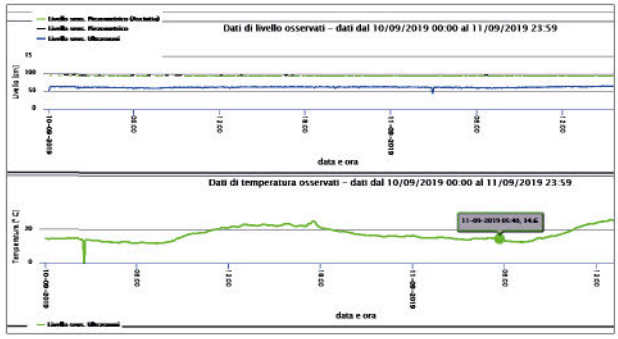


Fig. 2 Il progetto rientra nella logica IoT. Il sistema *Machine-to-Machine* è basato su un dispositivo Raspberry Pi che invia i dati in Cloud. È possibile accedere da remoto al server dei dati via Web e tramite App per dispositivi mobili. (**a.**) La logica per la rilevazione e l'elaborazione dei dati prevede sensori (ed eventuali attuatori) per la rilevazione dei parametri fisici; la loro elaborazione locale per una gestione più efficiente (edge/fog computing); l'invio a una piattaforma remota per lo sviluppo di applicazioni cloud-based; (**b.**) l'interazione con gli utenti via Web o App su dispositivi mobili.

sorgere nel tempo (per esempio nuovi tipi di controlli per l'inquinamento e non solo la portata del fiume, collegamenti locali fra più dispositivi per rendere più efficiente il controllo, la possibilità di agire su attuatori locali, come motori, serrande, segnalatori di allerta, da remoto).

I dati rilevati, opportunamente formattati, vengono inviati al server, sfruttando Web Service, dove vengono opportunamente elaborati. Le informazioni ricavate (grafici, medie, modelli di previsione) vengono rese pubbliche e possono essere visualizzate dagli utenti, che siano semplici cittadini o istituzioni come la Protezione Civile e i Comuni. L'applicazione web (corredata da un'app) mostra il livello del fiume, le soglie di attenzione e gli allarmi. Inoltre, in caso di emergenza, invia messaggi e e-mail agli attori coinvolti.
In locale il sistema (**Figura 3**) dispone anche di un display, che oltre a mostrare i dati raccolti, risulta molto comodo per la messa in funzione del sistema e per i test di manutenzione.
In teoria basterebbe un solo sensore per rilevare l'altezza del fiume e agire di conseguenza.

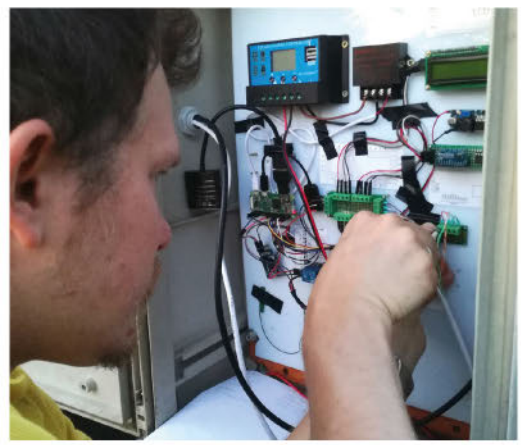
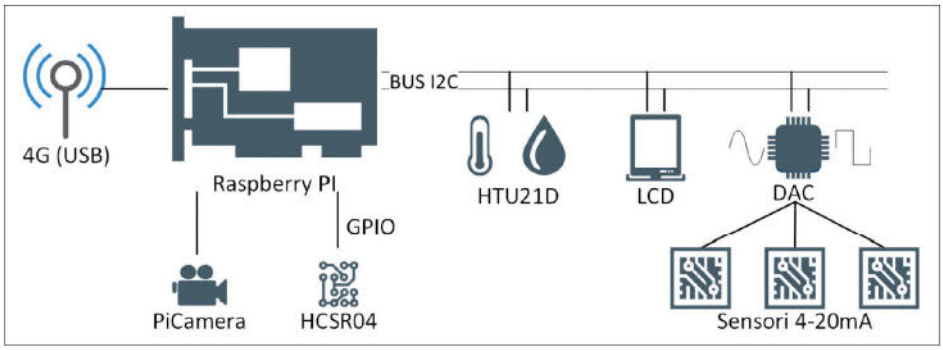


Fig. 3 Il montaggio a campo della centralina con i diversi dispositivi e il display.

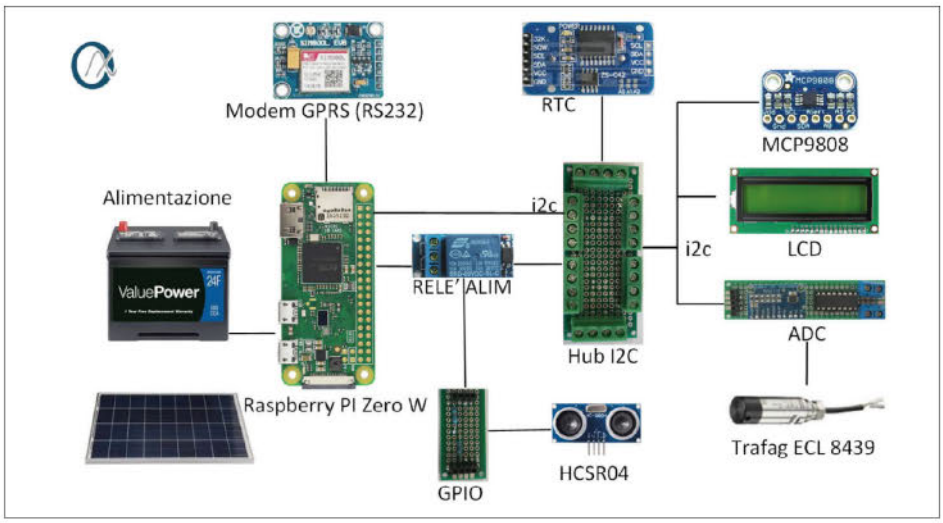
notabene

Il progetto è stato realizzato effettivamente, con la collaborazione del Dipartimento di Ingegneria Civile e Ambientale (DICA) del Politecnico di Milano, e premiato dalla Regione Lombardia.

a



b



➜ **Fig. 4** (**b**) Lo schema logico con i bus di acquisizione e i sensori; (**b**) la rappresentazione grafica della scheda di implementazione.

Purtroppo nella realtà le cose sono ben diverse e la scelta di sensori multipli diventa, se non obbligatoria, fortemente consigliata, per alcuni vantaggi:

- ridondanza. In caso di guasto o malfunzionamento di un sensore, un altro continua a inviare dati permettendo un'affidabilità maggiore.
- Rilevazione di dati diversi che, nel loro complesso, permettono di ottenere una informazione esaustiva.
- Scalabilità e intercambiabilità dei sensori. Sensori diversi possono essere aggiunti nel tempo. Per esempio non solo per controllare la portata del fiume, ma anche per rilevare l'inquinamento dell'acqua tramite l'analisi chimica o l'odore del fiume per rilevare tracce di inquinamento in tempo reale.

Componente	Tipologia	Interfaccia
MCP9808 – temperatura digitale	Sensore	I2C
HCSR04 – distanza ultrasuoni	Sensore	Digitale personalizzata
LCD Display	Display	Personalizzata/ I2C
Sonda Trafag	Sensore	Analogica in corrente (4-20 mA)
ADS1115	Convertitore ADC	I2C

↑ **Tab. 1** Sensori e loro caratteristiche.

Il sistema di acquisizione/hardware

La **Figura 4**, insieme alla **Tabella 1**, mostra lo schema logico di acquisizione dati a campo con i sensori coinvolti nel processo.

File aggiuntivi
Codice completo pronto per l'esecuzione

Problemi svolti
Implementazione del codice in Python

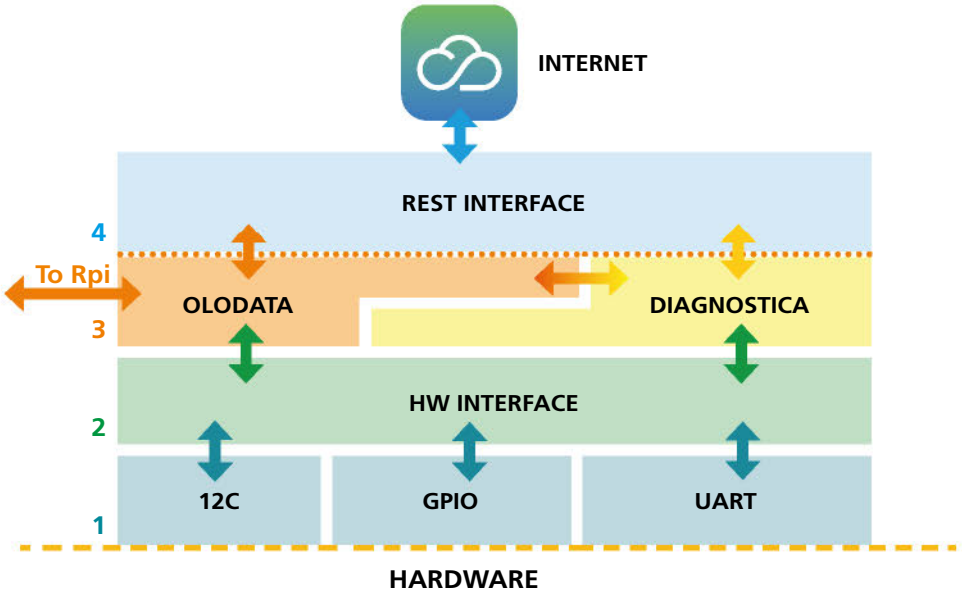


Fig. 5 Gli strati software per l'acquisizione dei dati dai sensori e il loro trasferimento in cloud.

Il sistema di acquisizione /software

Il software è stato pensato a livelli indipendenti e collaboranti (Figura 5).
Ciascuno strato software dialoga con quello immediatamente sottostante e fornisce funzionalità a quello soprastante.
Il modello prevede quattro strati ed è stato pensato per permettere sia la comunicazione con altri dispositivi Raspberry (lasciando campo aperto a una eventuale soluzione con un Raspberry "master" che coordina gli altri ad esso collegati), sia la comunicazione con Internet, con la possibilità di accedere a un server remoto tramite API di tipo RESTFul.

- **Livello 1**. Contiene le librerie di comunicazione per le diverse interfacce:
  - **Blocco I2C**. Contiene le librerie per interfacciarsi ai componenti che utilizzano tale bus come mezzo di comunicazione;
  - **Blocco GPIO**. Contiene il software necessario alla gestione dei componenti non I2C;
  - **Blocco UART**. Permette di utilizzare l'UART presente su Raspberry.
- **Livello 2**. Ha lo scopo di rendere trasparente l'accesso alle varie periferiche occupandosi di gestire le chiamate alle diverse librerie di comunicazione.
- **Livello 3**. Contiene due componenti:
  - **Diagnostica**. Ha lo scopo di raccogliere informazioni sullo stato di salute del dispositivo e delle periferiche ad esso collegate;
  - **Olodata** (opzionale). Implementa il protocollo di comunicazione che permette al dispositivo di comunicare con altri Raspberry.
- **Livello 4** (REST Interface). Permette di comunicare con le API RESTFul messe a disposizione da un ente terzo.

Note di implementazione del software

Il software per la raccolta e l'invio dei dati è stato scritto interamente in Python.
Sfruttando le possibiltà offerte dal sistema operativo Raspbian è stato possibile pianificare, tramite crontab, l'esecuzione dei diversi processi anziché scrivere un unico programma "a ciclo infinito", evitando il blocco del sistema di acquisizione qualora vi sia un problema in un segmento di codice.
Nei materiali digitali sono riportati alcuni stralci di codice che illustrano i meccanismi più significativi di acquisizione e trasmissione dati, facilitati dalle librerie di gestione dei vari componenti.

Interroghiamo l'Intelligenza Artificiale

Tema 3

Tu e un tuo compagno o una tua compagna scegliete 5 domande dall'elenco.

Successivamente, lavorando individualmente, interrogate l'AI usando due chatbot diverse. Ciascuno conserva le schermate con le risposte e riassume le risposte ottenute. Infine, confrontate le risposte. Le chatbot hanno dato risposte analoghe? Oppure ci sono state differenze? Quando tu e il tuo compagno o la tua compagna avete riassunto le risposte della chatbot, avete considerato come importanti gli stessi concetti?

1. Come l'Intelligenza Artificiale può migliorare i processi di backup e il ripristino dei dati?
2. In che modo l'algoretica, o etica degli algoritmi, può aiutarci a riflettere su trasparenza, equità, inclusività, privacy?
3. In che modo gli algoritmi di machine learning possono essere addestrati per riconoscere comportamenti sospetti?
4. Cos'è un Data Center e quale ruolo svolge nell'infrastruttura di rete?
5. Cosa si intende per virtualizzazione all'interno di un Data Center?
6. Cos'è il Cloud Computing e quali sono le sue caratteristiche principali?
7. Spiega la differenza tra Data Center on-premises e cloud-based.
8. Quali sono i vantaggi di utilizzare un Data Center rispetto a un'infrastruttura locale?
9. Come viene garantita la sicurezza fisica e logica nei Data Center?
10. Come fare a mitigare la minaccia rappresentata dagli utenti interni di una rete che hanno alti privilegi di accesso?
11. La configurazione errata dei servizi Cloud è una delle più comuni vulnerabilità. Come l'Intelligenza Artificiale potrebbe aiutare a evitare il problema?
12. Cos'è una CDN (*Content Delivery Network*) e come si collega al cloud computing?
13. Utilizzando tecniche di analisi predittiva, l'Intelligenza Artificiale come può identificare potenziali vulnerabilità?
14. Qual è il ruolo delle API nel Cloud Computing?
15. Le interfacce e le API esposte che non sono adeguatamente protette possono consentire accessi non autorizzati? Come fare per mettere in sicurezza il sistema?
16. Cos'è l'Internet of Things (IoT) e quali sono i suoi ambiti di applicazione?
17. Spiega il ruolo dei sensori e degli attuatori in un dispositivo IoT.
18. Spiega il concetto di Smart City e come l'IoT contribuisce al suo sviluppo.
19. Quali sono i rischi di sicurezza associati ai dispositivi IoT?
20. In che modo l'Intelligenza Artificiale potrebbe automatizzare il processo di aggiornamento dei dispositivi IoT, per applicare tempestivamente patch di sicurezza?
21. Come vengono gestiti i grandi volumi di dati generati dai dispositivi IoT?
22. Quali sono i vantaggi e le sfide dell'integrazione di IoT e Cloud Computing?

La cyber war e la nostra vita

Spunti di riflessione

Pace e guerra
Riflettiamo su questi estratti di esperti di cyber sicurezza e sulle conseguenze di ciò che viene affermato, in particolare...

> «Tra pace e guerra non esiste un sottile confine, ma una vasta zona grigia, dove gli stati danno vita a quella che viene definita competizione strategica, utilizzando in diverse combinazioni i quattro elementi che formano il potere di uno stato: diplomatico, militare, economico e informativo. Proprio quest'ultimo fattore, complice la pervasività delle tecnologie digitali, ha assunto una rilevanza senza precedenti.»
>
> Alessandro Curioni, "Intelligenza artificiale, etica e conflitti", "Il Sole 24 ore", 21 settembre 2024

> «Colpendo un obiettivo fisico con un numero sufficiente di bombe tutte uguali finirò per distruggerlo anche se fosse l'Everest. In una guerra convenzionale questa affermazione è sempre vera, in un conflitto cyber è quasi sempre falsa.»
>
> Alessandro Curioni, Aldo Giannuli, *Cyber War: la guerra prossima ventura*, Mimesis 2019

Guerra convenzionale vs Cyber War
Questi estratti ci forniscono un quadro chiaro delle complesse dinamiche della cyber guerra e della sua crescente influenza. Per comprendere meglio queste differenze, possiamo confrontare le caratteristiche della guerra convenzionale, della cyber war e della guerra ibrida. La **Tabella 1** permette di definire e mettere a confronto le caratteristiche comuni e le diversità tra questi tipi di conflitti.

Attività per lo studente
Obiettivi

L'approfondimento di questo tema ti consentirà di:

- esaminare le caratteristiche delle guerre convenzionali, cyber e ibride, identificando le similitudini e le differenze;
- valutare come gli elementi del potere di uno Stato (diplomatico, militare, economico e informativo) si combinano nei vari tipi di conflitti;
- considerare le implicazioni etiche e strategiche dell'utilizzo delle tecnologie digitali nei conflitti moderni e il loro impatto sulla sicurezza globale.

Nuclei tematici fondamentali e suggerimenti per l'approfondimento

- Come si evolvono i conflitti nel contesto delle nuove tecnologie digitali? Esiste una trasformazione nella natura del campo di battaglia?
- Come cambia il concetto di "nemico" nelle guerre cyber e ibride rispetto ai conflitti convenzionali? Quali sono le difficoltà nell'identificare gli aggressori?
- Quali sono le differenze tra gli ordigni fisici e le armi informatiche? In che modo queste differenze influenzano le strategie di difesa e attacco?
- Fai un'analisi comparativa tra le strategie di difesa utilizzate nelle guerre convenzionali e quelle utilizzate nei conflitti cyber e ibridi.
- Discuti il problema della sicurezza delle infrastrutture critiche nel contesto dei cyber attacchi e delle operazioni ibride.

- Completa **Tabella 1** introducendo nuove voci che rispecchiano le tue osservazioni. Ad esempio:
  - Strategie di propaganda (social, giornali, radio, TV).
  - Coinvolgimento, diretto e indiretto, dei civili.
  - Collaborazioni tra hacker e gruppi criminali informatici.
  - Durata e costi del conflitto.

Fasi operative

Fase	Attività	Fase	Attività
1 **Analisi preliminare (individuale)** 	Ogni studente, lavorando individualmente: • ricerca sul Web e/o tramite AI informazioni relative alla Cyberwar; • sintetizza e organizza le informazioni raccolte, evidenziando i nuclei tematici fondamentali individuati.	3 **Condivisione dell'elaborato (in team di 2/3 studenti)** 	Ogni gruppo presenta alla classe e all'insegnante il proprio elaborato.
2 **Produzione di un elaborato (in team di 2/3 persone)** 	La classe viene suddivisa in gruppi composti da 2-3 persone. Ogni gruppo produce un elaborato (documento testuale, documento multimediale, video, presentazione...) che spieghi i nuclei tematici individuati nella fase precedente. Per ogni nucleo tematico si può includere: • un breve video (2-3 minuti) tratto dal Web; • un testo di 15-20 righe; • un'infografica; • immagini esplicative. È opportuno alternare momenti di lavoro "in presenza" e momenti di lavoro "da remoto"; ad esempio: • organizzazione del gruppo, scelta del tipo di elaborato, suddivisione dei compiti → in presenza; • produzione dell'elaborato e preparazione dell'esposizione orale → da remoto (individualmente o in modo collaborativo); • controllo finale dell'elaborato prodotto e simulazione della sua presentazione alla classe → in presenza.	4 **Riflessione conclusiva (tutta la classe)** 	**Per quali motivi il lavoro fatto sul confronto tra guerre convenzionali e cyberwar ti fa essere un migliore cittadino attivo?** Confrontati con il resto della classe e rifletti su come le guerre convenzionali e cyberwar ti permettono di comprendere meglio le dinamiche complesse dei conflitti moderni. Questo studio ti aiuta a: • Essere informato. Conoscere le diverse tipologie di conflitto ti rende un cittadino più consapevole delle minacce globali e delle strategie di difesa necessarie. • Sviluppare pensiero critico. Analizzare e confrontare le varie caratteristiche dei conflitti ti aiuta a sviluppare capacità di analisi critica e valutazione delle informazioni. • Promuovere la cittadinanza digitale. Capire l'importanza della sicurezza informatica e il ruolo della cyberwar ti spinge a promuovere comportamenti responsabili we sicuri online.
		5 **Valutazione** 	Ogni gruppo valuta il lavoro degli altri esprimendo un giudizio su completezza, chiarezza espositiva, originalità, collaborazione. L'insegnante valuta i lavori usando i criteri di valutazione definiti e tenendo conto delle valutazioni degli studenti. È possibile assegnare un bonus per particolari aspetti emersi dal lavoro presentato.

Tab. 1

Guerra convenzionale (Fisica)	Cyber War	Guerra ibrida
Definizione		
• Conflitto armato tradizionale. Gli schieramenti sono chiaramente definiti e visibili, e l'uso delle armi è evidente e diretto. • La strategia spesso prevede attacchi frontali con l'obiettivo di sopraffare il nemico e occupare il territorio.	• Guerra silenziosa; le armi sono invisibili e gli schieramenti sono di difficile identificazione. • Le operazioni si svolgono principalmente nel cyberspazio e comprendono spionaggio, sabotaggio e attacchi informatici. • Gli aggressori si infiltrano nelle reti e nei sistemi informatici, spesso restando sconosciuti per lunghi periodi, e attaccano di sorpresa. • Gli obiettivi sono generalmente infrastrutture critiche, dati sensibili e la destabilizzazione dei sistemi.	• Combina elementi della guerra fisica e cyber per ottenere effetti strategici. • Spesso inizia con attacchi informatici per destabilizzare e confondere il nemico, seguiti da operazioni militari tradizionali per concludere il conflitto e consolidare il controllo.
Campo di battaglia		
• Il confronto è frontale. • Le forze armate si scontrano faccia a faccia sul campo di battaglia. • Lo spionaggio si realizza attraverso operazioni segrete per raccogliere informazioni sul nemico.	• Il confronto avviene "dietro le quinte", nelle reti informatiche e nei sistemi digitali. • Gli attacchi sono mirati e strategici, focalizzati sull'identificazione e lo sfruttamento delle vulnerabilità nei sistemi dell'avversario.	• Il campo di battaglia è sia fisico che virtuale, con operazioni coperte e aperte che sfruttano vulnerabilità in entrambe le dimensioni per ottenere il massimo impatto.
Dov'è il nemico?		
• Visibile e frontale, direttamente sul campo di battaglia.	• Non si sa. Il nemico è nascosto nelle reti e nei sistemi informatici. • Gli aggressori penetrano in modo subdolo nelle infrastrutture digitali di un'organizzazione o di uno Stato, utilizzando malware, phishing, o altre tecniche di ingegneria sociale per ottenere accesso e poi rimanere nascosti. • Una volta infiltrati, possono restare dormienti per mesi o anni senza essere rilevati, raccogliendo informazioni, monitorando attività e rendendo i sistemi vulnerabili a futuri attacchi. • Presenza invisibile e persistente, estremamente difficile da individuare e neutralizzare.	• Può essere ovunque: sul campo, in rete, nei media. • Gli attacchi informatici possono precedere e facilitare operazioni fisiche, rendendo difficile per l'avversario capire dove e quando si verificherà il prossimo colpo.
Tipo di Ordigni		
• Bombe fisiche che causano danni fisici devastanti e permanenti. • Il caso più evidente è una bomba termonucleare.	• Bombe logiche, armi informatiche che producono effetti temporanei (es. attacchi DDoS), come se una fabbrica o un aeroporto riprendesse le attività subito dopo essere stato bombardato. • Bombe personalizzate costruite sfruttando i punti deboli (vulnerabilità) degli obiettivi. • Attacchi a hardware e software di dispositivi d'uso comune (telefoni, sistemi IoT, sistemi indossabili…).	• Combinazione di armi fisiche e cyber, ad esempio attacchi DDoS per destabilizzare le difese seguiti da attacchi fisici per consolidare il danno e l'occupazione.
Vantaggi/svantaggi dei difensori		
Vantaggio: • Chi difende conosce bene il proprio territorio e può sfruttarne al meglio le caratteristiche geografiche. • I difensori possono preparare fortificazioni, trincee e altre strutture difensive. • I difensori sono più vicini alle loro linee di rifornimento. • Le truppe difensive possono essere più motivate a proteggere la loro terra. • I difensori possono posare trappole e mine terrestri davanti all'aggressore. Svantaggio: • Uno Stato non può disegnare la geografia del proprio territorio per posizionare ostacoli naturali.	Vantaggio: • Il campo di battaglia può essere progettato a discrezione di chi difende, con hardware, software, reti e sistemi di supporto combinati e modificabili nel tempo. Per chi si difende, si tratta di un'opportunità da sfruttare per costringere il nemico a un faticoso lavoro di ricognizione, peraltro costellato da incertezze. Il costante aggiornamento dei sistemi può diventare fondamentale. Svantaggio: • Chi difende è spesso svantaggiato poiché non sa di essere stato attaccato e quando, dove e da chi.	Vantaggio • Può combinare metodi per massimizzare l'efficacia e confondere l'avversario. Svantaggio: • Richiede coordinazione e aumenta il rischio di escalation e danni collaterali.

Le parole dei Social

Spunti di riflessione

Il modello di comunicazione

Il modello di comunicazione di Shannon, che abbiamo descritto già nel primo volume, è uno dei più utilizzati per descrivere il processo di comunicazione. Questo modello si concentra principalmente sugli aspetti tecnici della trasmissione dell'informazione (trasmettitore, ricevitore, canale, ecc.), senza affrontare direttamente l'implicito e il non detto della comunicazione, elementi cruciali tra esseri umani, poiché spesso il significato di un messaggio non risiede solo nelle parole che diciamo, ma anche nel contesto in cui le pronunciamo. Ad esempio:

- Marco: "C'è una festa stasera. Vieni?"
- Marta: "Domani ho la verifica".

In questo caso, Marta non dice esplicitamente che non andrà alla festa, ma Marco intuisce comunque che, probabilmente, Marta non parteciperà.

Etimologia dei termini

Molti termini utilizzati dai social media, pur avendo una parentela con il significato originale, si basano su un contesto diverso che può portare a significati inediti. Proviamo a vedere un esempio partendo dall'etimologia della parola "post", che, originariamente, deriva dal latino *postis*, che significa "palo" o "colonna". Nel contesto dei social media, però, ha assunto il significato di "messaggio pubblicato online".

notabene

Etimologia ha il significato di "studio dell'origine delle parole, del loro significato nel tempo e della loro evoluzione". Deriva dal greco *étymos*, "intimo" e *lógos*, "studio" e, di fatto, racconta la storia delle parole e ci fornisce delle immagini con cui fare confronti e operare metafore.

I termini dei social e il loro significato originale

La **Tabella 2** permette di confrontare alcuni termini, tra i più utilizzati sui social, e riflettere sul significato originale rispetto a quello più recente, permettendoci di fare dei confronti e metterne in discussione l'utilizzo.

Attività per lo studente

Obiettivi

L'approfondimento di questo tema ti consentirà di:

- analizzare l'evoluzione dei termini utilizzati sui social media e confrontarli con i loro significati originali per comprendere meglio l'impatto del linguaggio digitale sulla comunicazione moderna;
- comprendere le implicazioni che i termini utilizzati nei social comportano nella vita quotidiana e metterne in discussione l'utilizzo;
- riflettere sulle sfide etiche legate all'utilizzo delle nuove tecnologie e su come queste possano influenzare la società e le interazioni umane.

Nuclei tematici fondamentali e suggerimenti per l'approfondimento

- Come evolvono gli spazi pubblici? Esiste una trasformazione digitale dei luoghi di incontro?
- Come evolve il concetto di comunità? Si nota della superficialità nelle relazioni on-line?
- Quali sono le differenze tra condivisione fisica e digitale? Esiste un'etica della condivisione online?
- Fai un'analisi comparativa tra agorà antiche e moderne piattaforme social.
- Studia le relazioni sociali nell'era digitale e approfondisci gli effetti dei social media sulle relazioni personali e sulla comunità.
- Discuti il problema della condivisione di contenuti senza consenso.
- Completa la **Tabella 1** introducendo nuove voci che rispecchiano la tua esperienza sui social, come *memoria*, *fake*, *code sharing*, *hashtag*, *tag*, *algoritmo* ecc., riferendoti anche a letture come quella del libro di Marco Balzano *Le parole sono importanti*, Einaudi Editore.

Fasi operative

<table>
<tr><th>Fase</th><th>Attività</th><th>Fase</th><th>Attività</th></tr>
<tr><td>1
Analisi preliminare (individuale)
</td><td>Ogni studente, lavorando individualmente:
• ricerca sul web e/o tramite AI informazioni relative ai termini utilizzati nei social confrontati con il loro significato originale;
• sintetizza e organizza le informazioni raccolte, evidenziando i nuclei tematici fondamentali individuati.</td><td>3
Condivisione dell’elaborato (in team di 2/3 studenti)
</td><td>Ogni gruppo presenta alla classe e all’insegnante il proprio elaborato</td></tr>
<tr><td rowspan="2">2
Produzione di un elaborato (in team di 2/3 persone)
</td><td rowspan="2">La classe viene suddivisa in gruppi composti da 2-3 persone.
Ogni gruppo produce un elaborato (documento testuale, documento multimediale, video, presentazione...) che spieghi i nuclei tematici individuati nella fase precedente.
Per ogni nucleo tematico si può includere:
• un breve video (2-3 minuti) tratto dal Web;
• un testo di 15-20 righe;
• un’infografica;
• immagini esplicative.
È opportuno alternare momenti di lavoro “in presenza” e momenti di lavoro “da remoto”; ad esempio:
• organizzazione del gruppo, scelta del tipo di elaborato, suddivisione dei compiti → in presenza;
• produzione dell’elaborato e preparazione dell’esposizione orale → da remoto (individualmente o in modo collaborativo);
• controllo finale dell’elaborato prodotto e simulazione della sua presentazione alla classe → in presenza.</td><td>4
Riflessione conclusiva (tutta la classe)
</td><td>Per quali motivi il lavoro fatto sul confronto tra lo stesso termine utilizzato nei social media e il suo significato originale ti fa essere un migliore cittadino attivo?
Confrontati con il resto della classe e rifletti su come questo studio ti permetta di comprendere meglio le dinamiche complesse e a più dimensioni della comunicazione moderna.
Questo studio ti aiuta a:
• capire come evolvono i termini nel mondo digitale, rendendoti più consapevole e attento;
• studiare l’etimologia dei termini e apprezzare le loro radici storiche, esaminare le differenze tra il significato originale e quello moderno e riflettere sulle conseguenze etiche dell’uso delle parole e su come possono influenzare il comportamento.
• essere consapevole del significato preciso dei termini per renderti un cittadino digitale più responsabile, capace di promuovere un uso rispettoso e costruttivo del linguaggio online;
• confrontare le tue riflessioni con quelle dei tuoi compagni di classe favorendo il dialogo e lo scambio di idee, arricchendo la comprensione collettiva e sviluppando le competenze di comunicazione e collaborazione.</td></tr>
<tr><td>5
Valutazione
</td><td>Ogni gruppo valuta il lavoro degli altri esprimendo un giudizio su completezza, chiarezza espositiva, originalità, collaborazione.
L’insegnante valuta i lavori usando i criteri di valutazione definiti e tenendo conto delle valutazioni degli studenti. È possibile assegnare un bonus per particolari aspetti emersi dal lavoro presentato.</td></tr>
</table>

Tab. 2

Significato Originale	Significato Nuovo
Piazza	
Luogo di incontro e scambio. Nell'antica Grecia, agorà era il termine con il quale si indicava la piazza principale della polis, dove i cittadini si riunivano per discutere di affari pubblici, commerciare e socializzare.	La piazza si trasforma in piattaforma digitale dove gli utenti possono postare aggiornamenti, commentare e partecipare a discussioni su vari argomenti.
Social (Sociale)	
La parola "sociale" deriva dal latino "socius," che significa "compagno" o "alleato." Questo termine implica un senso di comunità e collaborazione, dove le persone si alleano per un obiettivo comune o per supportarsi reciprocamente. Ad esempio, le attività sociali come le feste di quartiere o le riunioni di famiglia sono occasioni per rafforzare i legami e costruire un senso di appartenenza.	Il concetto di alleanza e compagnia è spesso sostituito da interazioni superficiali, come i "like", che sono segnali di consenso rapido e spesso privo di profondità. Ad esempio, una persona può mettere "like" a una foto senza realmente approfondire il contenuto o partecipare all'esperienza dell'autore del post, ma semplicemente per segnalare la propria presenza.
Condivisione	
La parola "condivisione" deriva dal latino "cum dividere", che significa "spartire insieme con altri." Questo termine implica l'atto di dividere qualcosa con altre persone, creando un senso di partecipazione e comunità. La condivisione è vista come un atto di generosità e collaborazione. Ad esempio, condividere il cibo con amici e parenti durante una festa o condividere la fatica di un cammino insieme.	Condividere contenuti online, come foto, video e pensieri, è un modo per ottenere una presenza digitale. Questa forma di condivisione è più una "moltiplicazione" di contenuti che non una "divisione". Spesso avviene senza nemmeno chiedere il permesso ai destinatari (che magari neppure sono interessati). Molti utenti condividono aspetti della loro vita quotidiana, senza considerare l'impatto o il consenso degli altri coinvolti nelle immagini o nei post. Inoltre, non sempre le persone sono informate sugli argomenti che trattano. Non esiste un riferimento autorevole e, anche se è vero che in democrazia tutti possono pronunciarsi, dovrebbero farlo solo se conoscono quello di cui trattano.
Amicizia	
Relazione di affetto reciproco tra persone. La radice "am" significa "amare" o "voler bene" ed è alla base di molte parole (amicizia, amore, amico) legate all'affetto e alla cura delle persone. L'amicizia si fa, si costruisce ("accatastare e mettere insieme"). Tanto è vero che i legami si misurano dalla loro solidità e quando finiscono si dice che si rompono. Cicerone scrisse un intero trattato in cui esplorava la natura dell'amicizia e dell'impegno necessario per costruirla e mantenerla.	Connessione virtuale, spesso superficiale. Sui social, le persone possono avere centinaia di "amici," molti dei quali sono semplici conoscenti o neppure questo. Queste relazioni virtuali spesso mancano dell'impegno e della costanza che caratterizza le amicizie tradizionali. Sul Web l'"amicizia" si dà o si chiede, ma non si costruisce. È molto probabile che dopo la "concessione" dell'amicizia si passi ad altro, perché non c'è più niente da fare.
Storia	
In prima battuta è il racconto di eventi passati, ma, per usare le parole di Alessandro Baricco, «una storia è il campo di energia prodotto nell'animo di uno di noi dall'imprevista vibrazione di una tessera di mondo». Questo concetto molto articolato dimostra come la storia non sia solo una semplice cronaca di eventi, ma un intreccio di emozioni, significati e interpretazioni che risuonano nell'animo umano.	Le "storie" sui social permettono agli utenti di raccontare la loro giornata o un evento specifico attraverso una serie di immagini o video brevi e relativamente poco strutturati. Tuttavia cercano di offrire uno spaccato immediato e visivo della vita quotidiana. Ad esempio nelle "storie" che durano 24 ore, gli utenti mostrano la foto o il video del caffè mattutino o di un paesaggio mozzafiato, con l'intenzione di narrare un'esperienza immediata della loro vita.

Esame di Stato

Guida allo svolgimento dell'esame di Stato

Requisiti fondamentali di Progettazione reti

Per affrontare con competenza la seconda prova scritta di Sistemi e Reti dell'Esame di Stato occorre costruirsi mentalmente uno schema dei passaggi logici che, dalle specifiche dei requisiti presenti in modo più o meno esplicito nelle richieste della prova, conducano alla progettazione della rete e al relativo software.
Spesso la prova che viene assegnata impone allo studente di avere una visione globale e aperta del sistema. I casi proposti partono da situazioni reali che vanno analizzate, interpretate e sintetizzate. Le varie parti (LAN, WAN, applicazioni software, database e sicurezza) devono essere integrate in un unico sistema capace di rispondere alle richieste del testo.
È utile strutturare il progetto basandosi su un'impostazione che presenti uno schema generale a cui aggiungere la propria esperienza maturata durante gli anni scolastici, ottenendo così una giusta sintesi di competenze acquisite sia in ambito formale, qual è quello scolastico, sia in ambito informale.

Occorre anche evidenziare che spesso le tracce d'esame proposte dal Ministero presentano aspetti della realtà descritti nel testo non univocamente interpretabili. In questi casi è necessario formulare delle ipotesi ragionevoli, né troppo limitative né troppo complesse, che consentano di comprendere e circoscrivere il tema proposto. Le ipotesi aggiuntive devono essere realistiche e legate al caso specifico.
Nel caso in cui le richieste siano generiche, occorre fare scelte ponderate, in linea con il programma svolto durante l'anno, tenendo conto del tempo a disposizione.
La realizzazione di una pagina web, o di un'applicazione web, e del codice a essa associato deve semplicemente fornire una traccia, o dei casi prova, che dimostrino la competenza raggiunta, senza cadere nell'errore di pensare alla realizzazione di un progetto completo e dettagliato.

In questa sede forniremo alcuni spunti di progettazione relativi alle tracce e alle simulazioni degli ultimi anni. Per prima cosa, ricordiamo quali sono i criteri generali di progettazione di una rete.

Che cosa significa progettare una rete

Il percorso da seguire per la progettazione di una rete (anche in funzione della sua dimensione) è quello classico mostrato in **Figura 1**.
In essa sono rappresentati gli elementi attraverso i quali si sviluppa l'analisi del progetto di rete e che vogliamo analizzare in dettaglio nei prossimi paragrafi:

- Definizione dei requisiti
- Progettazione e pianificazione
- Realizzazione del progetto
- Gestione e controllo del lavoro
- Rilascio del sistema e proseguimento



Fig. 1 Percorso di progettazione della rete: dai requisiti alla realizzazione e rilascio.

Definizione dei requisiti

La comprensione dei requisiti permette di definire:

- Numero di nodi e utenti (dimensionamento della rete)
- Topologia, modalità di accesso, disposizione geografica dei nodi e delle aree da collegare

- Tipo di traffico (dati, voce, video) e banda a disposizione
- Modalità e tipologia della connessione a Internet
- Vincoli (architettonici, tecnologici, legali, di spesa)
- Livello di sicurezza e policy
- Espansione e modifiche previste nel tempo
- Know-how del personale addetto alla gestione della rete

Progettazione e pianificazione

La progettazione dell'architettura di rete deve confrontarsi non solo con vincoli di natura tecnica ed economica.
In particolare, deve tener conto delle infrastrutture di supporto alla rete ed eventualmente dell'inserimento nel progetto della loro modifica o realizzazione. Pertanto si dovranno considerare:

- vincoli della struttura (passaggi, canaline, montanti, scavi tra edifici, antenne, accessi protetti, nuove costruzioni)
- punti di alimentazione elettrica (potenza, ridondanza, topologia)
- controllo della temperatura e dell'umidità degli ambienti con il sistema di condizionamento, se necessario
- controllo perimetrale e protezione degli accessi ai locali dedicati
- obblighi di legge per le norme antincendio e di sicurezza sul lavoro e quanto viene richiesto dall'organizzazione interna all'azienda
- esperienza, autonomia e cultura tecnica del personale e di eventuali consulenti

Realizzazione

La realizzazione di una rete deve seguire i principi del Project Management, quali:

- un progetto tecnico di realizzazione dettagliato (blueprint)
- un piano dettagliato temporale con la descrizione delle parti realizzabili in parallelo (diagramma di Gantt) e le scadenze intermedie ("milestone")
- un controllo accurato del rispetto dell'avanzamento del progetto durante la sua realizzazione
- il rilascio di mappe dettagliate della realizzazione su supporto informatico in formato digitale
- il rilascio dei certificati di legge
- un piano di prove per l'accettazione delle varie componenti della rete
- le fasi di messa in funzione e collaudo

Gestione e rilascio

Una volta progettata la rete è necessario attivare un piano di follow-up per un controllo costante del funzionamento, al fine di correggere eventuali errori di progettazione. È necessario poi seguire costantemente l'evoluzione del suo utilizzo e l'innovazione tecnologica per mantenere sempre aggiornata la rete.
In particolare occorre tenere sotto controllo due aspetti.

- **Problemi organizzativi e di coordinamento (cose e persone)**: se è stata fatta una buona pianificazione delle attività da fare e se per ognuna di queste sono stati definiti chiaramente la responsabilità e il periodo di esecuzione, si dovrebbero avere pochi problemi organizzativi e di coordinamento; le fasi di definizione degli obiettivi e di pianificazione sono le attività più importanti nella gestione di un qualsiasi progetto.
- **Difficoltà e soddisfazioni e anche... errori**: le difficoltà si superano facilmente se ci sono buona intesa e buono spirito di collaborazione tra gli stakeholders; certamente occorre prevedere nel piano di lavoro qualche possibile ritardo nell'esecuzione dei lavori, dovuto a volte a banalità o a fraintendimenti; per questo è indispensabile fare una buona pianificazione e una previsione dei rischi.
  Gli errori fanno parte del lavoro e sono utili per poter individuare problemi che non erano stati previsti nella fase di progettazione. Tali errori possono diventare una fonte preziosa di apprendimento e di miglioramento.

Traccia per la progettazione di una rete

I punti che seguono forniscono una traccia che facilita lo studente nell'elaborazione del progetto di rete che costituisce la spina dorsale del tema d'esame.

Inquadramento generale

- Ambito
- Contesto
- Modalità di finanziamento e costi (specificare l'entità dei costi, la fonte, le modalità di finanziamento)
- Dimensionamento dell'utenza effettiva
- Modalità di fruizione dei servizi offerti
- Filosofia di impiego
- Soluzioni organizzative (specificare quali figure professionali sono coinvolte nell'uso della rete)
- Modalità di accesso (libero, regolamentato, con policy, ...)
- Analisi bisogni/benefici
- Riferimenti al modello ISO/OSI

Vincoli e progetto della rete

- Integrazione con eventuali altre reti preesistenti
- Vincoli
- Distanze (comprensorio, edificio, ...)
- Dimensionamento: specificare che cosa si vuole collegare in rete (aree funzionali, numero di host fissi, numero di host mobili wireless, numero di stampanti, server, sottoreti di interconnessione, domini di accesso, ...)
- Schema della topologia della rete
- Apparati di rete, la cui scelta deve tener conto di alcuni parametri fondamentali:
  - velocità e numero di porte di interfaccia presenti su uno switch o su un router
  - costo di un dispositivo (in funzione delle sue caratteristiche: velocità, tecnologia, sicurezza, opzioni, ridondanza, affidabilità, ...) e dei cavi di collegamento
  - scalabilità con la possibilità di inserire nuovi moduli e di espandere il numero delle porte per rispondere a nuove esigenze e collegamenti con nuove reti
  - caratteristiche di funzionamento e servizi offerti: sicurezza, qualità del servizio (QoS)
  - NAT, DHCP.
- Indirizzamento (reti/sottoreti/host). Ricordiamo che tutti gli host all'interno di una rete devono avere un indirizzo univoco. Lo schema di indirizzamento IP deve essere pianificato, documentato e infine conservato.
  Gli indirizzi possono essere privati e pubblici e l'assegnazione può avvenire manualmente (come si fa di norma con server o dispositivi intermedi), oppure tramite DHCP per i terminali utenti che possono essere abilitati ad accedere a Internet. Se si usano procedure standard (per esempio l'assegnazione di indirizzi prestabiliti ai server o a certi insiemi di terminali), non solo è più facile per l'amministratore di rete risalire a errori e malfunzionamenti, ma anche rilevare intrusioni ed essere pronti a intervenire in caso di attacco.
- Virtual Lan

Confine con l'esterno

- Connessione con la rete Internet
- Velocità di connessione
- Configurazione router: IP pubblico, range di IP privati (DHCP), IP del default gateway, maschere
- Configurazione VPN
- Configurazione firewall e proxy
- Configurazione NAT

Cablaggio strutturato

- Distanze • Scelta dei mezzi trasmissivi • Velocità richieste • Riferimenti alle normative internazionali • Schema logico (dorsali, concentratori, uscita EF)

Sistemi di sicurezza adottati

- Controllo degli accessi e contrasto delle minacce:
  - minacce ambientali, con temperature e umidità fuori norma
  - minacce elettriche ed elettromagnetiche, con variazioni di tensione, scariche elettriche, disturbi radio
  - minacce ai sistemi hardware, con danni ai server e agli apparati di rete e al cablaggio
- Documento delle "norme che regolano l'accesso e l'uso" (policy)
- Individuazione dei responsabili
- Definizione dell'ambiente di prova e di produzione
- Backup e aggiornamenti del software
- RAID (Redundant Array of Independent Disks) per garantire la tolleranza ai guasti
- Ridondanza, necessaria a garantire l'affidabilità della rete per sopperire a eventuali guasti. Per questo è consigliata la duplicazione dei dispositivi critici, come switch e router e il collegamento con la rete esterna
- Authentication, Authorization and Accounting: i servizi utilizzati per l'identificazione di un utente, l'autorizzazione alle attività da svolgere in osservanza alle regole di policy, la misura delle risorse che l'utente consuma durante l'accesso
- Firewall (con filtraggio dei pacchetti, applicazioni, URL, Stateful Inspection)
- Proxy
- DMZ
- VPN, protocolli sicuri (HTTPS, SSL, ...), crittografia e certificati, SSH
- Log degli accessi e degli errori

Gestione dei servizi

- Server interni/esterni
- Sistemi operativi
- Servizi forniti: DBMS, HTTPS, SMTP, POP3, ...
- Applicazioni client-server
- Hosting
- Housing
- Cloud/Virtualizzazione

Gestione della rete

- Gestione utenti • Amministratore di rete • Manutenzione hardware e software • Responsabili dei dati sensibili • Analisi del traffico tramite l'uso di applicazioni e protocolli (SNMP), per poter intervenire tempestivamente in situazioni critiche e ottenere informazioni sulla vulnerabilità dei sistemi e sulla possibilità di contrastare eventuali attacchi • Documentazione delle operazioni svolte

Sviluppo applicazioni

Le applicazioni si sviluppano su tre livelli.

- Modello dei dati:
  - definizione del modello concettuale (per esempio modello E/R)
  - modello logico (per esempio modello relazionale)
- Logica di funzionamento:
  - realizzazione e codifica delle funzioni che operano sui dati
  - architettura client-server
- Interfaccia utente:
  - analisi di usabilità e accessibilità
  - interfaccia per applicazioni web e/o per sistemi mobili

Prove d'esame

In questa sezione proponiamo temi d'esame completi di soluzione, simulazioni ministeriali e simulazioni di prove d'esame da cui è possibile prendere spunto in vista della preparazione all'esame.

La preparazione della seconda prova scritta dell'esame di Stato

La seconda prova scritta dell'esame di Stato si compone di due parti:

- la **Parte prima**, che propone di progettare la gestione automatizzata di una procedura riferita a un contesto reale;
- la **Parte seconda**, che propone quattro quesiti, a due dei quali – a scelta – lo studente deve rispondere per iscritto.

Per imparare a risolvere la prova scritta, ti forniamo le soluzioni dei temi d'esame proposti, per evidenziare il metodo generale di analisi del problema e di progettazione della sua soluzione che dovrai acquisire e consolidarne poi l'apprendimento.

Ti ricordiamo che i pdf ministeriali delle seconde prove scritte si possono scaricare dal sito del ministero, all'indirizzo: https://www.istruzione.it/esame_di_stato/ selezionando l'anno di interesse e la voce "Istituti Tecnici".

ESAME DI STATO LUGLIO 2024

Indirizzo: ITIA – INFORMATICA E TELECOMUNICAZIONI – Articolazione: INFORMATICA
Tema di: SISTEMI E RETI

Parte prima

L'amministrazione di una Regione italiana, attraverso una società appositamente creata, ha recentemente sviluppato una infrastruttura di comunicazione in fibra ottica, allo scopo di fornire connettività a banda larga ad Enti locali, scuole e strutture sanitarie pubbliche presenti in tutto il suo territorio. In particolare, in ambito sanitario, la società gestisce anche un data-center che raccoglie tutti i dati sanitari dei cittadini residenti in regione, relativi alle prestazioni sanitarie erogate dalle strutture pubbliche (fascicolo sanitario elettronico).
I dati raccolti nel fascicolo sanitario elettronico di ciascun paziente possono essere di vari formati e dimensioni in quanto riguardano, ad esempio, gli accertamenti diagnostici (es. ecografia), le visite specialistiche (es. visita cardiologica) e la relativa documentazione (referto, immagini diagnostiche, video ...).
All'interno della componente M6C2 "Innovazione, ricerca e digitalizzazione del Servizio Sanitario Nazionale", prevista dalla Missione 6 del PNRR, la Regione intende estendere la rete in fibra già esistente, per offrire il servizio di connettività a banda larga a tutte le strutture sanitarie private convenzionate, in modo che anche i dati da loro prodotti possano direttamente confluire nel *data-center* regionale.
In tal modo, tutti i cittadini ed i medici chiamati a curarli, sia presso strutture sanitarie pubbliche che presso quelle private convenzionate, avranno a disposizione in un unico luogo virtuale (il fascicolo sanitario elettronico) tutte le informazioni sanitarie di loro interesse.
Per differenziare le diverse tipologie di strutture connesse alla rete (Enti locali, scuole e strutture sanitarie pubbliche e private), la società regionale che gestisce l'infrastruttura in fibra ha adottato un piano di indirizzamento utilizzando sottoreti della rete 10.0.0.0/8; in particolare, a questo nuovo servizio di connettività verso le strutture sanitarie private convenzionate è stata assegnata la sottorete 10.100.0.0/16. Questa sottorete sarà finalizzata esclusivamente all'interazione con il data-center delle strutture sanitarie private convenzionate, ma non offrirà loro servizi di accesso generalizzato ad Internet.

Utilizzando gli indirizzi consentiti da questa sottorete, il progetto dovrà pertanto dettagliare un piano di indirizzamento che permetta di connettere un numero di strutture sanitarie private convenzionate che si stima essere intorno alle 2000 in regione (con possibili incrementi futuri), assegnando a ciascuna di esse la disponibilità di un minimo di 8 indirizzi complessivi.
Ogni struttura sanitaria privata convenzionata ovviamente dispone già di una propria infrastruttura di rete locale interna. La società regionale di gestione fornirà a tali strutture private convenzionate un dispositivo per la connessione alla rete regionale, configurato e controllato da remoto dalla società regionale stessa. Il progetto dovrà garantire che ciascuna struttura collegata non possa accedere alle reti di tutte le altre strutture connesse alla rete in fibra regionale.
Il candidato analizzi la realtà di riferimento e, formulate le opportune ipotesi aggiuntive, contribuisca alla stesura del progetto svolgendo i seguenti punti:

Punto 1 sviluppi una descrizione di massima, anche supportata da uno schema grafico, dell'infrastruttura di rete in fibra pre-esistente (che connette Enti locali, scuole e strutture sanitarie pubbliche) e di come questa si evolverà per implementare il nuovo servizio per le strutture sanitarie private convenzionate, con opportune esemplificazioni degli indirizzamenti IP adottati;

Punto 2 indichi la tipologia e le caratteristiche hardware (es: numero e tipologia delle singole porte) del dispositivo che sarà fornito ad ogni struttura sanitaria privata convenzionata, nonché i dettagli relativi alla eventuale configurazione di rete delle sue porte; espliciti anche i servizi che ritiene debbano essere configurati su tale dispositivo;

Punto 3 considerando le caratteristiche della LAN pre-esistente in una ipotetica struttura sanitaria privata convenzionata, specifichi con quali eventuali apparati aggiuntivi o riconfigurazioni degli apparati già esistenti tale rete verrà connessa con la rete in fibra regionale, esemplificando opportunamente;

Punto 4 data la natura sensibile dei dati trattati, espliciti le principali misure che è opportuno adottare per garantirne un trattamento con adeguata sicurezza, sia per la loro archiviazione che per i trasferimenti da e per il data-center; in particolare il candidato specifichi le modalità e la schedulazione temporale con cui le strutture sanitarie trasferiscono al data-center regionale i dati delle prestazioni sanitarie da loro effettuate.

Parte seconda

Quesito I *In relazione al tema proposto nella prima parte, si prevedano le strategie da adottare in caso di malfunzionamenti della connessione in fase di trasferimento dati e sui sistemi di archiviazione, allo scopo di evitare possibili perdite di dati.*

Quesito II *In relazione al tema proposto nella prima parte, il candidato descriva le possibili forme di autenticazione qualificata (a più fattori) per consentire al singolo cittadino di consultare via web tutti i dati del proprio fascicolo sanitario elettronico (accertamenti e visite specialistiche).*

Quesito III *Una piccola azienda dispone di un normale collegamento ad Internet a banda larga, con un router a cui è assegnato un solo indirizzo IP pubblico statico. Nella rete interna alla piccola azienda esiste un web server locale che si vuole rendere accessibile da Internet sia tramite protocollo HTTP che HTTPS, e si vuole rendere gestibile da remoto tramite protocollo SSH. Il candidato descriva la configurazione del router necessaria per raggiungere lo scopo, motivando nel dettaglio le scelte fatte ed elencando i comandi utilizzabili.*

Quesito IV *All'interno di una azienda con una propria LAN, un tecnico di help-desk riceve la segnalazione di un utente circa l'impossibilità di "navigare su Internet". Si descrivano i passi e gli opportuni strumenti da utilizzare per individuare tre possibili cause del problema.*

SVOLGIMENTO DELLA PROVA

Parte prima – Soluzione

Dalla lettura del testo emerge che:

- la Regione intende estendere la rete in fibra già esistente, per offrire il servizio di connettività a banda larga a tutte le strutture sanitarie private convenzionate, in modo che anche i dati da loro prodotti possano direttamente confluire nel datacenter regionale;
- ogni struttura sanitaria privata convenzionata ovviamente dispone già di una propria infrastruttura di rete locale interna. La società regionale di gestione fornirà a tali strutture private convenzionate un dispositivo per la connessione alla rete regionale, configurato e controllato da remoto dalla società regionale stessa.

Per iniziare occorre, quindi, aggregare alla rete esistente nei diversi centri privati, il collegamento in fibra ottica con il datacenter regionale.

Punto 1

Infrastruttura della rete preesistente

La rete regionale preesistente in fibra ottica, utilizza dispositivi di rete come router e switch per collegare i vari enti al data center regionale.
Nota: l'ipotesi è che la rete in fibra ottica sia privata.
La società regionale che gestisce l'infrastruttura in fibra ha adottato un piano di indirizzamento utilizzando sottoreti della rete **10.0.0.0/8**. La distribuzione degli indirizzi IP è la seguente:

- Rete regionale: `10.0.0.0/8`
- Sottoreti (esempio)
  - Enti locali `10.10.0.0/16`
  - Enti scolastici `10.20.0.0/16`
  - Strutture sanitarie pubbliche `10.30.0.0/16`

Lo schema semplificato è mostrato in **Figura 1**.

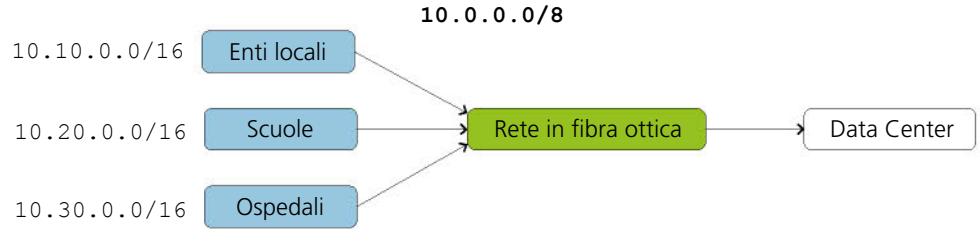


Fig. 1 Schema semplificato della rete preesistente.

Evoluzione con nuova configurazione per le strutture sanitarie private

Per il nuovo servizio di connettività verso le strutture sanitarie private convenzionate è stata assegnata la **sottorete** `10.100.0.0/16`. La **nuova** distribuzione degli indirizzi IP è (**Figura 2**):

- Rete regionale: `10.0.0.0/8`
- Sottoreti (esempio)
  - Enti locali `10.10.0.0/16`
  - Enti scolastici `10.20.0.0/16`
  - Strutture sanitarie pubbliche `10.30.0.0/16`
  - Strutture sanitarie private convenzionate `10.100.0.0/16`

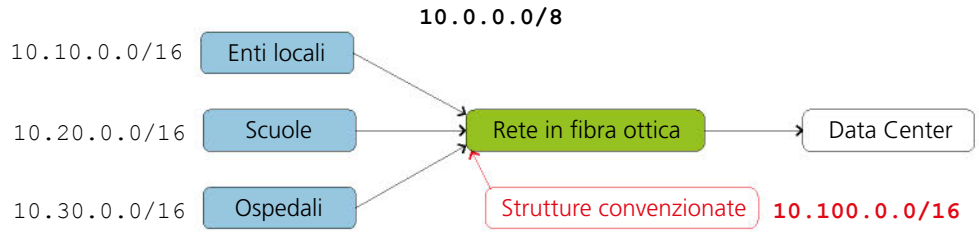


Fig. 2 Schema semplificato con i nuovi collegamenti di rete.

La **figura 3** mostra un esempio semplificato del nuovo collegamento di una struttura convenzionata alla rete regionale in fibra ottica.

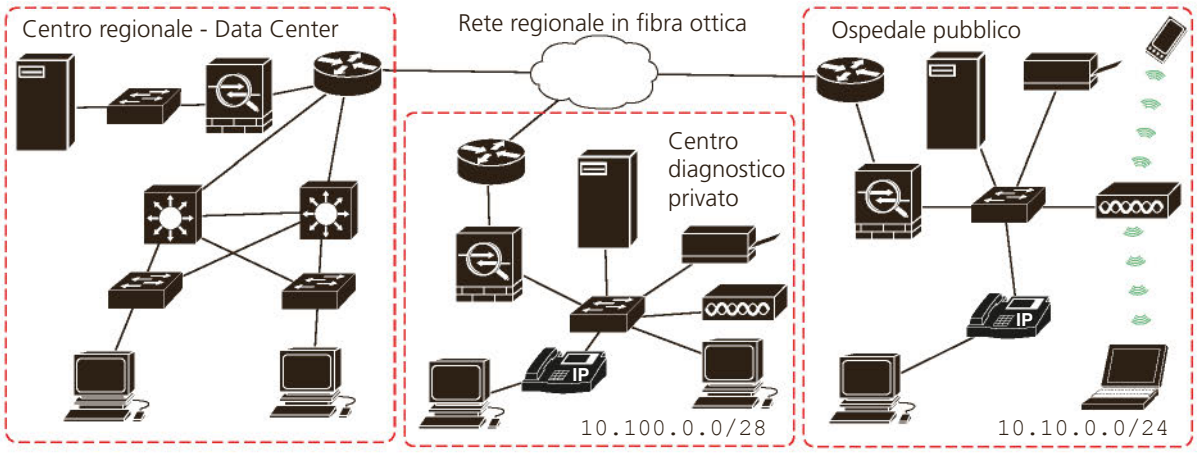


Fig. 3 Esempio di nuovo collegamento.

Calcolo degli Indirizzi

Richiesta del testo

- Sottorete Assegnata: 10.100.0.0/16
- Numero di Strutture Sanitarie Private Convenzionate: 2000 (con possibili incrementi futuri).
- Indirizzi Minimi per Struttura: 8.
- 2000 -> 2048 (211) sottoreti minime-> 16+11=27 -> /27 -> 25=32 -> 30 host (32-2=30 host, poiché 2 sono riservati per indirizzi di rete e broadcast).

Dettagli del Piano di Indirizzamento

- Ipotesi: per possibili incrementi futuri in modo da avere più sottoreti:
  - **/28. Ogni sottorete possiede 16 indirizzi (14 utilizzabili) per un totale di 4096 sottoreti**.

Indirizzi di Rete e delle sottoreti

```
Network:    10.100.0.0/16          00001010.01100100   .00000000.00000000
Netmask:    255.255.0.0/16
Broadcast:  10.100.255.255         00001010.01100100   .11111111.11111111
HostMin:    10.100.0.1             00001010.01100100   .00000000.00000001
HostMax:    10.100.255.254         00001010.01100100   .11111111.11111110
Host per rete: 65534
```

```
Sottoreti
Rete 1
Netmask:    255.255.255.240 = 28    11111111.11111111.11111111.1111 0000
Network:    10.100.0.0/28           00001010.01100100.00000000.0000 0000
Broadcast:  10.100.0.15             00001010.01100100.00000000.0000 1111
HostMin:    10.100.0.1              00001010.01100100.00000000.0000 0001
HostMax:    10.100.0.14             00001010.01100100.00000000.0000 1110
Hosts/Net:  14

Rete 2
Network:    10.100.0.16/28          00001010.01100100.00000000.0001 0000
Broadcast:  10.100.0.31             00001010.01100100.00000000.0001 1111
HostMin:    10.100.0.17             00001010.01100100.00000000.0001 0001
HostMax:    10.100.0.30             00001010.01100100.00000000.0001 1110
Hosts/Net:  14
….
Rte 1000
Network:    10.100.62.128/28        00001010.01100100.00111110.1000 0000
Broadcast:  10.100.62.143           00001010.01100100.00111110.1000 1111
HostMin:    10.100.62.129           00001010.01100100.00111110.1000 0001
HostMax:    10.100.62.142           00001010.01100100.00111110.1000 1110
Hosts/Net:  14
        …..
```

Punto 2

I dispositivi hardware forniti alle strutture private convenzionate, necessari per connettersi alla nuova rete sono: **router**, **firewall** e **switch**. Una ipotesi minima può prevedere quanto segue.

Tipologia e Caratteristiche Hardware del dispositivo di collegamento alla rete

Per semplicità, si propone l'utilizzo di un router con firewall integrato con caratteristiche professionali. Un unico dispositivo permette una gestione semplificata e la riduzione dei costi hardware, pur offrendo la possibilità di una configurazione e manutenzione centralizzate.
In caso di richieste di sistemi con maggiori prestazioni rispetto a un dispositivo combinato, si può considerare di separare le funzioni di routing e firewall su due dispositivi collegati fra loro come in Figura 3. Ciò permette di aggiornare o sostituire uno dei dispositivi senza influenzare l'altro, anche se i costi sono maggiori. Tuttavia, le funzionalità di base rimangono sostanzialmente le stesse per entrambe le scelte.

Caratteristiche Hardware del dispositivo di collegamento

- Porte LAN: Minimo 8 porte Gigabit Ethernet, espandibili fino a 16 porte.
- Porte WAN: 2 porte Gigabit Ethernet per la connessione alla rete regionale e per la ridondanza (se una delle porte WAN fallisce, l'altra può prendere il suo posto per garantire la continuità del servizio).
- Porte PoE: Supporto per PoE (Power over Ethernet) su alcune porte per alimentare dispositivi come telefoni VoIP o access point wireless.
- Porte USB: 1 porta USB.

Configurazione delle Porte

Le porte WAN1 e WAN2 sono utilizzate per la connessione alla rete regionale con connessione tramite cavi in fibra ottica.
Nota: le porte WAN possono essere collegate a moduli SFP (Small Form-factor Pluggable) per supportare il collegamento tra dispositivi di rete, come switch e router, e cavi in fibra ottica. Sono utilizzati per le connessioni a lunga distanza e possono raggiungere e superare velocità di 1 Gbps.

La configurazione delle porte di un router è ottenuta applicando a essa i comandi che associano indirizzi, maschere e funzioni. Ad esempio, nel caso di un router CISCO con sistema operativo IOS, alcuni dei comandi principali riguardano quanto segue.

- Configurazione IPv4 dell'interfaccia Gig0/0 (gli indirizzi IP sono puramente indicativi e a titolo di esempio).

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address x.x.x.x k.k.k.k
```

- Attivazione di protocolli di routing BGP su linea seriale.

```
Router(config)#interface Serial1/0
Router(config-if)#ip address x.x.x.x z.z.z.z
```

- Abilitazione BGP per Autonomous System 65000

```
Router(config)#router bgp 65000
```

- Individuazione del router «neighbor» (routerISP) con indirizzo y.y.y.y, presente nell'AS 10000

```
Router(config-router)# neighbor y.y.y.y remote-as 10000
```

Punto 3

Il dispositivo che combina router e firewall viene fornito già **preconfigurato** alla struttura privata convenzionata, in modo tale da stabilire una connessione **VPN** con il datacenter regionale e inviare in modo sicuro i dati del fascicolo sanitario elettronico, garantendo la riservatezza delle informazioni.

Schema di Configurazione

Router

- **Protocolli di Routing**. Utilizza protocolli come OSPF (Open Shortest Path First) o BGP (Border Gateway Protocol) per aggiornare e mantenere le tabelle di routing.
- **Gestione della Banda**. Permette di controllare e allocare la larghezza di banda disponibile tra i vari dispositivi e applicazioni sulla rete.
- **Gestione Remota**. Consente agli amministratori di rete di configurare, monitorare e gestire il router da una postazione remota. Tra le caratteristiche principali vi sono:
  - un'interfaccia web accessibile tramite browser, che permette di configurare e monitorare il dispositivo da remoto;
  - accesso SSH per eseguire le configurazioni;
  - aggiornamenti del firmware gestiti da remoto per garantire tempestività per sicurezza e funzionalità.
- **Servizio DHCP**.

Firewall

- **Regole di Firewall**. Il controllo del traffico in entrata e in uscita garantisce che solo il traffico autorizzato possa passare.
  Ad esempio, un firewall ASA che consente il traffico da un'interfaccia con un livello di sicurezza più elevato (in questo caso, l'interfaccia "inside" con livello di sicurezza 100) a un'interfaccia con un livello

di sicurezza inferiore (in questo caso, l'interfaccia "outside" con livello di sicurezza 0) utilizza comandi del tipo:

```
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#ip address x.x.x.x k.k.k.k
ciscoasa(config-if)#nameif inside
```

- **Ispezione del Traffico**. L'analisi dei pacchetti di dati identifica e blocca le attività sospette o dannose.
- **Filtro dei Contenuti**. La blacklist consente il controllo dei siti web non autorizzati o potenzialmente dannosi, come gioco d'azzardo, social media, o contenuti per adulti.
- **Monitoraggio e log**. Permette la rilevazione e l'analisi del traffico di rete in tempo reale per identificare anomalie e la registrazione di tutte le attività di rete, inclusi tentativi di accesso e modifiche alla configurazione.
- **QoS (Quality of Service)**. Consente la classificazione del traffico di rete in base alla sua importanza, con assegnazione di priorità più alta al traffico critico, come le videochiamate di telemedicina, rispetto ad altre attività meno critiche come il trasferimento di file.
- **VPN (Virtual Private Network)**. Il tunnel VPN protegge i dati da intercettazioni e accessi non autorizzati, stabilendo una connessione sicura tra la struttura sanitaria e la rete regionale.
  Il collegamento VPN è di tipo Site-to-Site. Tra i vantaggi c'è quello che gli utenti non devono configurare nulla sui loro dispositivi, poiché la connessione è gestita direttamente dai dispositivi preimpostati. Il tunnel utilizza il protocollo di sicurezza IPsec (Internet Protocol Security) che cripta i dati trasmessi, garantendo che solo i destinatari autorizzati possano accedere ai dati.

Switch

Gli switch devono essere configurati per supportare la VLAN e garantire la separazione del traffico, con la creazione di VLAN tagging sulle porte dei dispositivi che devono accedere alla rete regionale. Gli switch dovranno essere configurati per supportare, ad esempio, il traffico di rete regionale la VLAN 10. L'utilizzo della modalità trunk permette di ottimizzare l'uso delle porte degli switch e garantire che il traffico di rete sia correttamente separato e gestito.

Dispositivi di Rete

Devono essere configurati con indirizzi IP validi appartenenti alla sottorete 10.100.0.0/28 per PC, server e dispositivi medici.

Punto 4

Data la natura sensibile dei dati trattati, occorre garantire un trattamento adeguato sia per i dati a riposo (archiviati) sia per il loro transito verso il datacenter regionale.

Crittografia dei Dati

- **Crittografia a Riposo**. Prevede l'utilizzo di algoritmi di crittografia come AES (Advanced Encryption Standard) nei dispositivi di storage.
- **Crittografia in Transito**. Prevede l'utilizzo di protocolli IPSec e/o TLS per la crittografia dei dati durante il trasferimento tra dispositivi e reti.

Controllo degli Accessi

- **Autenticazione Multifattoriale (MFA)** è una tecnologia di sicurezza per verificare l'accesso ai sistemi che contengono dati sensibili.
- **Privilegi basati sui ruoli** consentono l'accesso solo agli autorizzati.

Backup e Ripristino

- **Backup Regolari** dei dati sono necessari per prevenire la perdita di informazioni in caso di guasti hardware o attacchi informatici.
- **Piani di Ripristino/Disaster Recovery** servono a garantire la continuità operativa in caso di incidenti o attacchi.
- **Politiche di conservazione** dei dati prevedono modalità e tempi di conservazione conformi alle normative.

Formazione del Personale

- **Formazione** del personale sulla sicurezza informatica dei dati e sui rischi legati alla possibilità di attacchi cibernetici deve essere adeguata e aggiornata.
- **Schedulazione Temporale del Trasferimento Dati**. I dati delle prestazioni sanitarie possono essere trasferiti al data-center regionale su base giornaliera o secondo le esigenze (tipo di dati, loro importanza) e i requisiti normativi. La pianificazione dei trasferimenti durante le ore di bassa attività (durante la notte) serve per minimizzare l'impatto sulle operazioni quotidiane delle strutture sanitarie.

Parte seconda – Risposte ai quesiti

Quesito I *In relazione al tema proposto nella prima parte, si prevedano le strategie da adottare in caso di malfunzionamenti della connessione in fase di trasferimento dati e sui sistemi di archiviazione, allo scopo di evitare possibili perdite di dati.*

Per evitare possibili perdite di dati in caso di malfunzionamenti della connessione durante il trasferimento dei dati e sui sistemi di archiviazione, è necessario adottare una serie di strategie preventive e correttive, tra cui:

- **strategie preventive**
  - backup regolari;
  - crittografia dei dati a riposo e in transito;
  - ridondanza dei sistemi (RAID e server di backup e dispositivi di rete);
  - sistemi di monitoraggio per rilevare tempestivamente eventuali anomalie o malfunzionamenti.
- **strategie correttive**
  - ripristino dei dati con piani di Disaster Recovery;
  - meccanismi di failover di rete per garantire la continuità del trasferimento dei dati;
  - diagnostica di rete (strumenti come ping, tracert, nslookup ecc.);
  - aggiornamenti software e patch di sicurezza.

Quesito II *In relazione al tema proposto nella prima parte, il candidato descriva le possibili forme di autenticazione qualificata (a più fattori) per consentire al singolo cittadino di consultare via web tutti i dati del proprio fascicolo sanitario elettronico (accertamenti e visite specialistiche).*

Per accedere al fascicolo sanitario regionale occorre utilizzare un metodo di autenticazione a più fattori. Questo metodo aumenta il livello di sicurezza combinando tra loro tecniche diverse che usano tecnologie differenti che rientrano in tre categorie: "qualcosa che sai", "qualcosa che hai", "qualcosa che sei".
L'utilizzo dello SPID e della carta d'identità Elettronica (CIE) fa parte dei metodi di autenticazione forte.

- **SPID (Sistema Pubblico di Identità Digitale)**. Permette ai cittadini di accedere ai servizi online delle pubbliche Amministrazioni con un'unica identità digitale. È un sistema di autenticazione che garantisce la protezione dei dati personali, non consentendo alcun tipo di profilazione. Per i cittadini italiani l'identità SPID è rilasciata dai Gestori di identità digitale (Identity Provider), soggetti privati accreditati

da AgID che forniscono le identità digitali e gestiscono l'autenticazione degli utenti. È possibile richiedere l'identità SPID a uno dei gestori disponibili che, dopo aver verificato i dati del richiedente, emette l'identità digitale, rilasciando le credenziali.
- **CIE (Carta di Identità Elettronica)**. È utilizzata per accedere ai servizi pubblici digitali. Tale sistema si sovrappone all'uso dello SPID in quanto equivale tecnicamente a uno SPID di livello 3 utilizzato per i servizi di importanza critica.

Quesito III *Una piccola azienda dispone di un normale collegamento ad Internet a banda larga, con un router a cui è assegnato un solo indirizzo IP pubblico statico. Nella rete interna alla piccola azienda esiste un web server locale che si vuole rendere accessibile da Internet sia tramite protocollo HTTP che HTTPS, e si vuole rendere gestibile da remoto tramite protocollo SSH. Il candidato descriva la configurazione del router necessaria per raggiungere lo scopo, motivando nel dettaglio le scelte fatte ed elencando i comandi utilizzabili.*

Accesso al server web dall'esterno

Una possibile soluzione è quella di progettare una DMZ per separare il server web con accesso pubblico dal resto della LAN. Una DMZ può essere realizzata con:
- un firewall singolo in cui si devono configurare tre interfacce: una verso la rete Internet (outside), una verso la LAN protetta (INSIDE) e una verso la DMZ. Le richieste che provengono da Internet sono deviate verso la zona demilitarizzata. In caso di attacco, saranno compromessi solo i servizi collegati al server pubblico, proteggendo così i dati privati presenti in LAN;
- due firewall: il primo firewall filtra il traffico esterno alla DMZ e consente il traffico esclusivamente verso la DMZ, mentre il secondo consente solo il traffico dalla DMZ alla rete interna. Se un attaccante riesce a compromettere il primo firewall, deve ancora superare il secondo per accedere alla rete interna;
- la tecnica del por forwarding. Questa tecnica è utilizzata nei router per indirizzare il traffico di rete da una porta specifica dell'indirizzo IP pubblico del router a una porta specifica di un dispositivo all'interno della rete locale (LAN).

Il testo chiede esplicitamente la configurazione di un router. Procediamo, quindi, nella progettazione di una DMZ per isolare l'area pubblica della rete aziendale e proteggere l'area privata da accessi esterni. Deve essere consentito l'accesso da qualunque host esterno verso il server web e fermato ogni accesso esterno verso la l'area privata.
Per consentire l'accesso dall'esterno al server web interno all'organizzazione e fermare qualunque altro ingresso, occorre agire sul router dell'organizzazione in ingresso.
Definiamo una ACL da impostare sull'interfaccia esterna del router in ingresso (per esempio interfaccia g0/0). Supponendo che l'indirizzo IP del server web sia `192.168.3.2`, i comandi da utilizzare sono:

```
interface g0/0
access-list 100 permit tcp any host 192.168.3.2 eq 80
access-list 100 permit tcp any host 192.168.3.2 eq 443
access-list 100 permit tcp any host 192.168.3.2 eq 22
interface g0/0
ip access-group 100 in
```

dove:
80 è la porta HTTP
443 è la porta HTTPS
22 è la porta SSH

Per la gestione del server da remoto via SSH occorre abilitare un server SSH e collegarsi da un qualsiasi client utilizzando, per esempio una applicazione come PuttY. Non occorre specificare che è bloccato qualunque altro ingresso perché, se non è specificata una regola da applicare, il pacchetto è scartato.

Quesito IV *All'interno di una azienda con una propria LAN, un tecnico di help-desk riceve la segnalazione di un utente circa l'impossibilità di "navigare su Internet". Si descrivano i passi e gli opportuni strumenti da utilizzare per individuare tre possibili cause del problema.*

Il tecnico di help-desk, quando riceve la segnalazione di un utente che non riesce a navigare su Internet, può seguire i seguenti passi e utilizzare i relativi strumenti software per individuare tre possibili cause del problema.

- **Verifica delle connessioni fisiche**
  - Assicurarsi che tutti i cavi Ethernet siano collegati correttamente e che non ci siano danni visibili.
  - Verificare anche che il WiFi sia attivo e funzionante.
  - Riavviare il computer dell'utente e il router per assicurarsi che eventuali problemi temporanei vengano risolti.
- **Verifica delle impostazioni di rete**
  - Con il comando `ipconfig /all`, controllare l'indirizzo IP, la subnet mask, il gateway predefinito e i server DNS. Assicurarsi che l'indirizzo IP sia corretto e che il computer abbia ottenuto un indirizzo IP valido dal server DHCP.
- **Test di connettività**
  - Con il comando `ping`:
  - pingare il gateway (ad esempio, ping `192.168.1.1`) per verificare se c'è un'interruzione di rete o se il WiFi non funziona;
  - pingare un nome di dominio (come `www.google.com`) per verificare la risoluzione DNS. Se il ping al dominio non funziona ma il ping all'indirizzo IP funziona, potrebbe esserci un problema con il server DNS;
  - pingare il server DNS. Ad esempio: ping `1.1.1.1`.
- **Verifica del Server DHCP**
  - Con i comandi `ipconfig /release` e `ipconfig /renew`, rilasciare e rinnovare l'indirizzo IP per assicurarsi che il computer stia ottenendo un indirizzo IP dal server DHCP.
- **Verifica del Server DNS**
  - Con il comando `nslookup`: `nslookup www.google.com` verificare che il server DNS stia risolvendo correttamente i nomi di dominio.
- **Tracciamento del percorso di rete**
  - Con il comando `tracert` (ad esempio `tracert www.google.com`) tracciare il percorso dei pacchetti verso un sito web per identificare dove potrebbe esserci un'interruzione nella rete.

Strumenti utilizzati (applicazioni che si aprono nel prompt dei comandi di Windows)

- **Ipconfig** visualizza e gestisce la configurazione degli indirizzi IP del computer.
- **Ping** testa la connettività di rete e la latenza.
- **Nslookup** interroga i server DNS e verifica la risoluzione dei nomi di dominio.
- **Tracert** traccia il percorso dei pacchetti e identifica eventuali problemi lungo il percorso.

Possibili cause del problema

1. **Problemi di configurazione IP**: l'indirizzo IP non è corretto o non è stato assegnato dal server DHCP.
2. **Problemi di risoluzione DNS**: il server DNS non risolve correttamente i nomi di dominio.
3. **Problemi di connettività di rete**: vi sono interruzioni lungo il percorso di rete o problemi con il gateway predefinito.

Nota: per la risoluzione dei problemi di rete si può fare riferimento all'approfondimento: Trobleshooting.



Approfondimento
Troubleshooting

ESAME DI STATO LUGLIO 2019

Indirizzo: ITIA – INFORMATICA E TELECOMUNICAZIONI – Articolazione: INFORMATICA
Tema di: INFORMATICA e SISTEMI E RETI

Parte prima

Per favorire il turismo culturale, l'Assessorato al Turismo di una città d'arte di medie dimensioni intende realizzare un'infrastruttura tecnologica che offra ai visitatori un servizio per la fruizione di contenuti multimediali che descrivono i "punti di interesse" (Point Of Interest = POI) di tipo monumentale (es. chiese, luoghi storici, ...) e artistico (es. musei, mostre, ...) distribuiti nel centro storico della città.
Per il servizio, si è deciso di erogare i contenuti multimediali sotto forma di pagine web, secondo due possibili formati denominati "pagina multimediale di base" e "pagina multimediale avanzata".

Nella pagina multimediale di base sono previsti:

- un video di presentazione breve del POI della durata tipica di un minuto esclusivamente in italiano con sottotitoli in inglese;
- un massimo di tre immagini relative al POI (es. dettagli architettonici, quadri, ...) con relativa didascalia in italiano ed inglese.

Nella pagina multimediale avanzata sono previsti:

- un video di presentazione approfondita del POI della durata tipica di cinque minuti in una fra 7 possibili lingue compreso l'italiano;
- una galleria di una ventina di immagini con relativa descrizione (tipicamente intorno ai 500 caratteri) in una fra 7 possibili lingue compreso l'italiano.

Il visitatore, acquistando il servizio in uno dei chioschi (InfoPoint) dislocati nella città, riceverà un biglietto con cui potrà avere accesso ai due tipi di pagina sulla base di tre possibili tariffe:

- "tariffa base": permette la fruizione di una pagina multimediale di base per ciascun POI;
- "tariffa intermedia": consente la fruizione di pagine multimediali avanzate per tre POI a scelta dell'utente e pagine di base per gli altri;
- "tariffa piena": consente la fruizione di pagine multimediali avanzate per ogni POI della città.

Il biglietto acquistato riporta la password di accesso ai contenuti, univoca per ciascun visitatore, associata al tipo di tariffa pagata e con validità giornaliera.
In relazione alle funzionalità che il servizio dovrà offrire, l'Assessorato richiede che siano soddisfatti i seguenti vincoli progettuali:

- la consultazione delle pagine multimediali sia abilitata esclusivamente ai dispositivi (minitablet) forniti all'atto dell'acquisto del biglietto, previa consegna di un documento di identità o di un numero di carta di credito valida;
- per facilitare l'aggiornamento periodico dei contenuti esistenti e l'inserimento di nuovi, gli stessi non siano memorizzati sui dispositivi utilizzati dagli utenti ma su sistemi server;
- l'accesso alle pagine multimediali sia effettuabile solo dopo l'inserimento, all'inizio della visita, della password presente nel biglietto;
- l'accesso alle pagine multimediali relative ad un POI debba avvenire solo in prossimità o all'interno del POI stesso;
- la restituzione dei dispositivi (minitablet) possa avvenire presso l'InfoPoint che ha in custodia il documento di identità oppure presso un qualsiasi InfoPoint se il visitatore ha optato per lasciare il numero di carta di credito valida.

Il candidato analizzi la realtà di riferimento e, fatte le opportune ipotesi aggiuntive, individui una soluzione che a suo motivato giudizio sia la più idonea a sviluppare i seguenti punti:

Punto 1 il progetto, anche mediante rappresentazioni grafiche, dell'infrastruttura tecnologica ed informatica necessaria a gestire il servizio nel suo complesso, dettagliando:

a) l'architettura della rete e le caratteristiche del o dei sistemi server, motivando anche la scelta dei luoghi in cui installare questi ultimi;

b) le modalità di comunicazione tra server e dispositivi consegnati ai visitatori, descrivendo protocolli e servizi software da implementare per gestire la rete e fornire le pagine;

c) gli elementi dell'infrastruttura utili a limitare la fruizione delle pagine multimediali esclusivamente in prossimità o all'interno dei POI a cui si riferiscono;

Punto 2 il progetto della base di dati per la gestione del servizio sopra descritto: in particolare si richiedono il modello concettuale ed il corrispondente modello logico;

Punto 3 la progettazione delle pagine web che consentono all'utente, in possesso di biglietto con tariffa base, la fruizione dei contenuti multimediali relativi al POI presso cui si trova, codificandone una porzione significativa in un linguaggio a scelta;

Punto 4 l'analisi di massima delle possibili modalità di gestione delle tre fasce tariffarie, delle opzioni offerte all'utente per la scelta dei tre POI nel caso della tariffa intermedia, e della scelta della lingua nel caso delle tariffe intermedia e piena.

Parte seconda

Il candidato risponda a due quesiti a scelta tra quelli sotto riportati.

Quesito I *In relazione al tema proposto nella prima parte, si vuole offrire ai visitatori la possibilità di inserire via web un commento ed un voto di gradimento su ogni POI visitato. Effettuata a tale scopo una opportuna integrazione della base di dati, si realizzi, codificandola in un linguaggio a scelta, una pagina web che consente la visualizzazione della media dei voti ricevuti da ciascun POI.*

Quesito II *In relazione al tema proposto nella prima parte, si discuta la possibilità di allargare la fruizione dei contenuti multimediali anche ai dispositivi personali degli utenti. In particolare, si analizzino le seguenti due ipotesi alternative:*

- *uso limitato ai soli dispositivi (minitablet) forniti all'atto dell'acquisto del biglietto, come sopra descritto: si individuino possibili soluzioni per impedire l'accesso alle pagine multimediali attraverso dispositivi non forniti dagli InfoPoint;*
- *uso consentito ai dispositivi personali degli utenti (es. smartphone): si descriva una possibile integrazione del servizio volta a consentire la fruizione dei contenuti direttamente ad un singolo dispositivo di proprietà del visitatore, pur mantenendo i vincoli di fruibilità in base alla tariffa associata al biglietto.*

Quesito III *Nella realizzazione e gestione di una base di dati accessibile da categorie di utenti con differenti ruoli, sono di rilevante importanza gli aspetti relativi alla sicurezza dei dati. Ad esempio, si supponga che nella realtà scolastica il personale della "Segreteria Alunni" non debba accedere ai dati del personale docente, il personale della "Segreteria Docenti" non debba accedere all'elenco dei fornitori della scuola ecc. Il candidato approfondisca la tematica proposta discutendo gli strumenti offerti dai sistemi DBMS per creare utenze che abbiano un accesso libero alla totalità dei dati o limitato a parte di essi, in termini di operazioni consentite, in base al ruolo ricoperto nell'organizzazione. Produca quindi esempi significativi, nel contesto proposto della segreteria scolastica, nel linguaggio fornito dal DBMS di sua conoscenza.*

Quesito IV *Per le aziende che dispongono di sedi dislocate in varie località sorge spesso la necessità di consentire al personale l'accesso ai sistemi da postazioni remote. Il candidato discuta le tipologie e i protocolli di accesso remoto ai sistemi, indicando in particolare le possibilità offerte dalle connessioni VPN. Sviluppi poi esempi nel caso di una azienda che ha due sedi operative e agenti commerciali che, muovendosi sul territorio, hanno necessità di collegarsi al sistema informativo aziendale.*

SVOLGIMENTO DELLA PROVA

Parte prima – Soluzione

Punto 1

Per iniziare occorre analizzare la "realtà di riferimento", ipotizzare una soluzione e costruirne un modello che la rappresenti.

Il **Punto 1.c** ci informa di "*limitare la fruizione delle pagine multimediali esclusivamente in prossimità o all'interno dei POI*". Partiamo da questo elemento per costruire intorno la rete e i collegamenti. Tra le diverse soluzioni possibili quella che risulta più immediata, perché non coinvolge altri dispositivi, è quella di acquisire la posizione geografica del POI sfruttando la geolocalizzazione del tablet in dotazione e scambiando i dati con il server in cloud (**Figura 1**). Nel caso di particolari problemi o di difficoltà di collegamento all'interno degli edifici, occorrerà ricorrere a soluzioni basate su QR code o Beacon BLE (*Bluetooth Low Energy*).

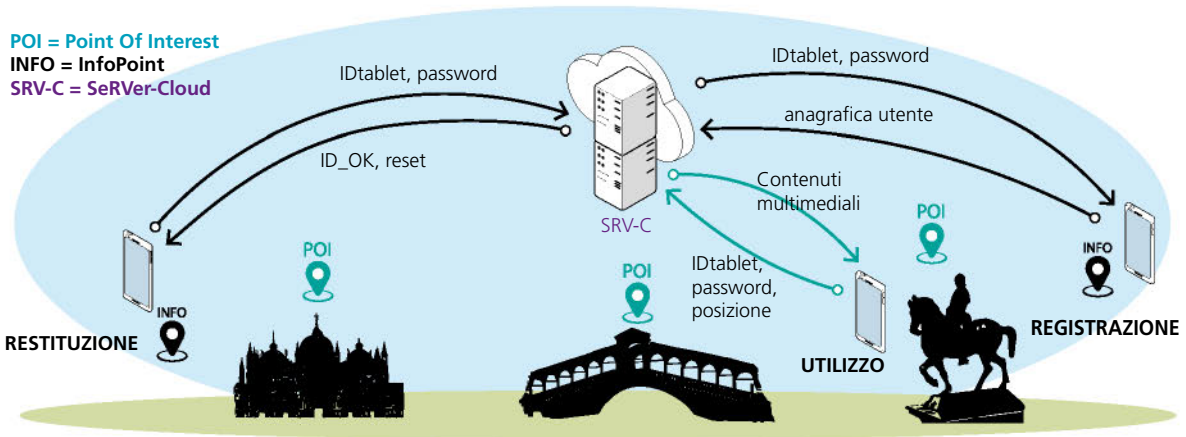


Fig. 1 Il modello della realtà di riferimento. La rappresentazione grafica è lo strumento che meglio sintetizza le caratteristiche di un progetto. È la mappa che contiene i macroelementi di cui è composto il progetto, ne sintetizza il funzionamento e, soprattutto, indica al progettista le interazioni e le relazioni con gli altri partecipanti. Sarà poi l'analisi dettagliata di ciascun elemento ad approfondirne i comportamenti. Le mappe, come scrive Alessandro Baricco, «apparentemente servono a navigare, a viaggiare, a portare una carovana al di là del deserto e una chiatta fino alla foce del fiume: ma in realtà servono a viaggiare nel cervello degli umani, e spesso sono la radiografia del loro cuore».

Quando un visitatore si trova nelle vicinanze di un POI (identificato univocamente), il tablet, che si trova nello stato di **UTILIZZO**, invia al server in cloud, tramite HTTPS, la propria posizione, il proprio codice identificativo (per esempio l'indirizzo MAC, e le credenziali dell'utente con la password che gli era stata assegnata al momento della registrazione. Il server, fatti gli opportuni controlli, invia i contenuti relativi al punto di interesse in questione.
Il tablet potrà, inoltre, trovarsi nei seguenti altri due stati.

- **REGISTRAZIONE** quando, all'interno di un InfoPoint, sarà registrato l'utente e gli sarà assegnata la password che gli permetterà di accedere ai servizi. Ogni InfoPoint, POI e minitablet possiede un identificatore univoco (che, nel caso del tablet, potrebbe coincidere con il suo indirizzo MAC).
- **RESTITUZIONE** quando, al contrario, il tablet sarà restituito all'InfoPoint. I suoi dati saranno inviati al server per un controllo di congruità e, se confermato, il tablet sarà logicamente tolto dal circuito per essere riassegnato a un nuovo visitatore.

Il **Punto 1.a** ci invita a precisare "*l'architettura della rete e le caratteristiche del o dei sistemi server*". Si tratta di utilizzare una soluzione basata su un'architettura client-server, con cui il tablet si interfaccia al server web, piattaforma LAMP.

Anche in questo caso sono possibili diverse soluzioni che vanno dalla gestione di una piattaforma in hosting che ospita i servizi richiesti a un data center interno. La prima soluzione è poco costosa, ma non dà la possibilità di supportare un numero di utenti elevato ed è difficilmente scalabile. La seconda prevede la disponibilità di sistemi hardware con tutte le difficoltà e i costi di manutenzione che ciò implica. Il cloud, almeno in questo contesto, sembra essere la soluzione più moderna ed efficace in quanto è on-demand, facilmente scalabile in funzione del numero di visitatori, ampliabile nei servizi, facilmente gestibile e protetta in termini di sicurezza. È affidabile e offre la continuità del servizio. Il server web è raggiungibile dagli utenti in qualsiasi momento e da qualsiasi luogo per fornire le pagine richieste.

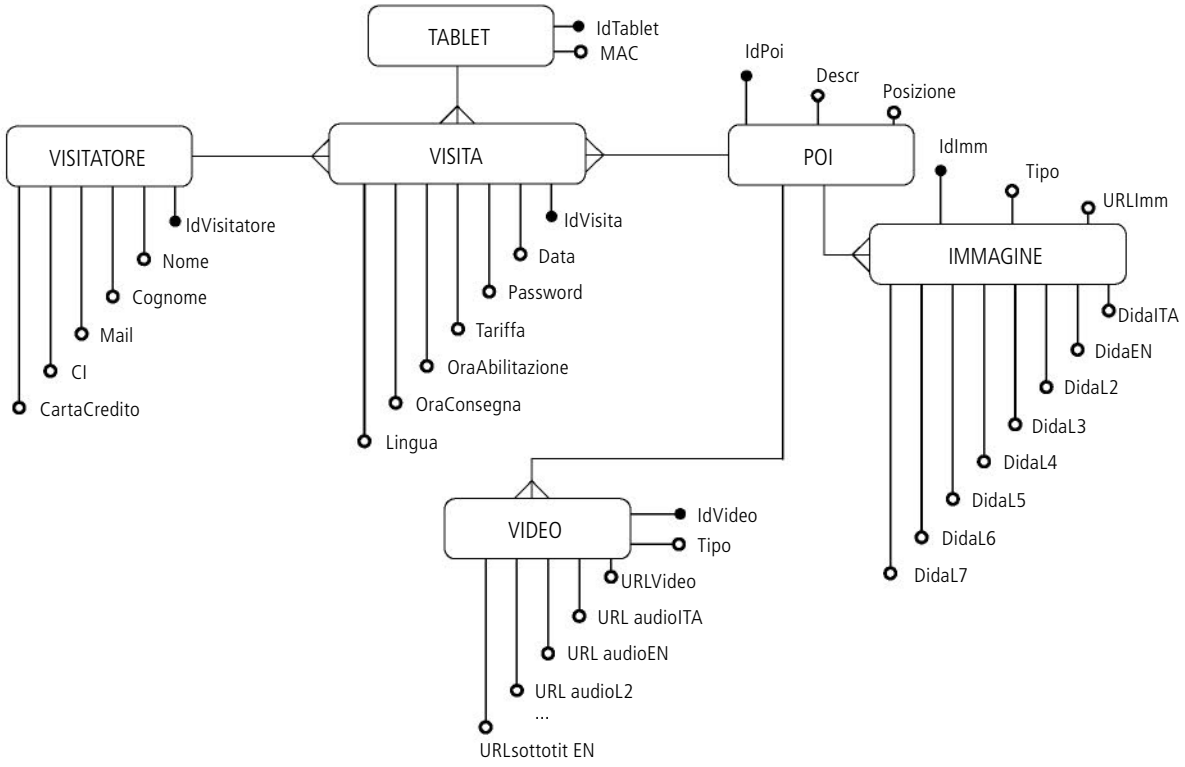
Il **Punto 1.b** chiede di precisare le *"modalità di comunicazione tra server e dispositivi consegnati ai visitatori"*. Si può supporre che i tablet dispongano di una applicazione dedicata, personalizzabile nella lingua desiderata, con la mappa della città e dei POI, che abbiano una connessione 4G e si colleghino direttamente in Internet o, in alternativa, con un collegamento WiFi (supposto che i tablet dispongano degli SSID delle reti WiFi di tutti i POI) accedano all'Acces Point del POI che, a sua volta, è connesso alla rete Internet via fibra o wireless. Il secondo caso presenta, forse, dei costi di gestione inferiori, ma la semplicità del primo caso può essere vincente in termini di praticità e costi di installazione dei dispositivi per la connettività.
Il protocollo utilizzato dagli utenti per accedere alle pagine web, base e avanzate, è HTTPS. La scelta di utilizzare una VPN in questo contesto appare fuori luogo per il tipo dei dati trasmessi e per il servizio da erogare.

Punto 2

Relativamente al progetto della base di dati per la gestione del servizio, si suppone che:

- la data di acquisto del biglietto corrisponda alla data in cui viene effettuata la visita e alla data in cui viene abilitato il tablet e generata la password;
- la tariffa è codificata con 0 (base) 1 (intermedia) 2 (piena);
- la lingua è codificata con 3 caratteri al massimo: ITA, EN, ...

Modello concettuale



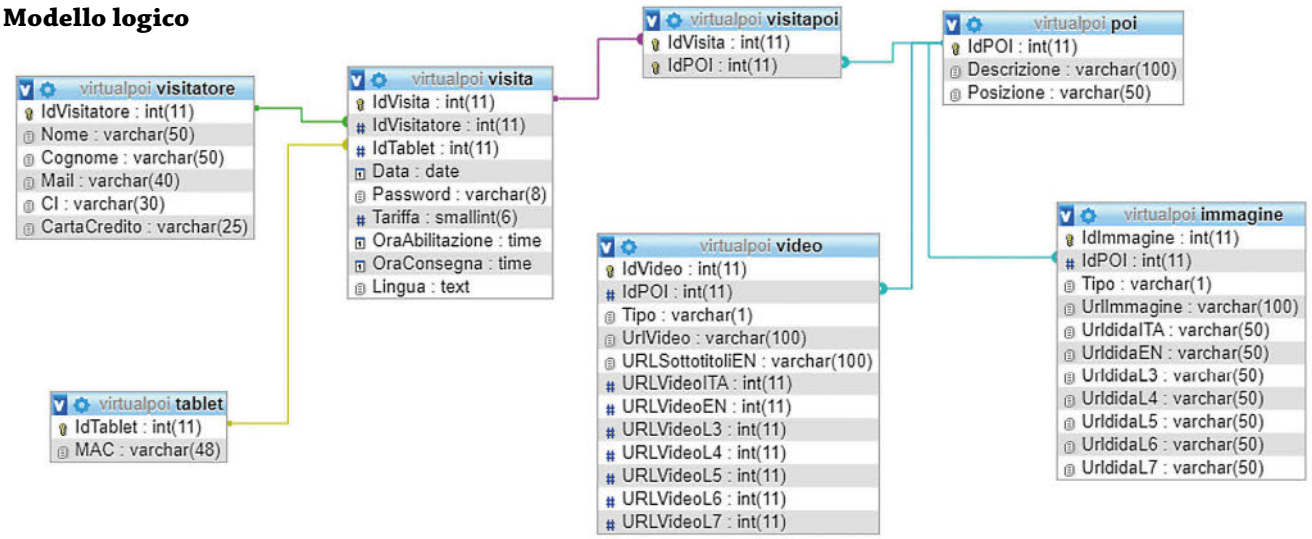
Entità

- Visitatore: persona che si registra al servizio offerto dall'Assessorato del Turismo.
- Visita: servizio erogato dall'Assessorato del Turismo.
- Tablet: dispositivo mobile fornito all'utente per effettuare una visita.
- POI: punto di interesse.
- Immagine: se il tipo è "b" (base) allora è una fotografia di un particolare del POI, se il tipo è "a" (avanzato" allora è una galleria di immagini; in entrambi i casi viene fornito l'URL.
- Video: filmato di un POI. Se il tipo è "b" è valorizzato l'URL dei sottotitoli in inglese e quello dell'audio italiano, se tipo è "a" vengono valorizzati gli URL delle 7 lingue.

Associazioni

- VISITATORE / VISITA 1:N: un visitatore effettua una o più visite, una visita è effettuata da un visitatore.
- TABLET/VISITA 1:N: un tablet è usato in una visita, una visita usa un tablet.
- VISITA/POI N:M: una visita coinvolge uno o più POI, un POI è coinvolto in una o più visite.
- POI/IMMAGINE 1:N: un POI è rappresentato con una o più immagini, un' immagine rappresenta un POI.
- POI/VIDEO 1:N: un POI è descritto in uno o più video, un video descrive un POI.

Modello logico



Punto 3

Per quanto riguarda la progettazione delle pagine web, di seguito viene data la bozza di soluzione.
Parametri in ingresso: idpoi, password, idvisita.
Trova URL dell'immagine e visualizza immagine.

```
<!DOCTYPE html>
<html>
<head>
<title> visualizza POI </title>
</head>
<body>

<?php
//
```

```
// assegnare i valori in base al progetto
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "virtualpoi";

// Crea connessione al database
$conn = new mysqli($servername, $username, $password, $dbname);

// controlla connessione
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
// id del POI rilevato in base alla posizione, come parametri vengono passati
// il biglietto e la password.
$idpoi=$_GET ['idpoi'];
$password=$_GET['password'];
$visita=$_GET['visita'];

$stringa= "select * from Visita where password= '$password' and
idVisita=$visita and tariffa=0;";

$result = $conn->query($stringa);

if ($result->num_rows > 0) {
      //esiste biglietto con password corretta
      $riga = $result->fetch_assoc();
      echo "autorizzazione concessa " ;
      $stringa1= "select * from Immagine where Tipo= 'b' and idPOI=$idpoi";
      $result = $conn->query($stringa1);
      if ($result ->num_rows > 0) {
            $riga = $result->fetch_assoc();
      echo "<img src =" . $riga['UrlImmagine'] . "/>" ;}
      else {echo"non ci sono immagini";}


} else {
    echo "autorizzazione non concessa";
}
$conn->close();

?>
</body>
</html>
```

Analogamente si procede con il video.

Punto 4

Questo punto prevede la possibilità di creare una pagina web (un form) che propone una scelta tra le diverse tariffe e, in base a una data scelta, offre una serie di servizi (POI e lingue).

Parte seconda – Risposte ai quesiti

Quesito 1 *In relazione al tema proposto nella prima parte, si vuole offrire ai visitatori la possibilità di inserire via web un commento e un voto di gradimento su ogni POI visitato. Effettuata a tale scopo una opportuna integrazione della base di dati, si realizzi, codificandola in un linguaggio a scelta, una pagina web che consente la visualizzazione della media dei voti ricevuti da ciascun POI.*

Per poter mantenere un commento e un voto dato da un visitatore durante una visita a un POI, aggiungiamo due campi alla tabella "VisitaPOI":

- commento;
- voto (il voto è un numero compreso tra 1 e 5).

La query per ottenere la media dei voti è:

```
SELECT avg(voto),IdPOI
from visitapoi
group by IdPOI;
```

PAGINA WEB

```
<!DOCTYPE html>
<html>
<head>
<title> media voti </title>
</head>
<body>

<?php

//asegnare i valori in base al progetto
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "virtualpoi";

// Crea connessione al database
$conn = new mysqli($servername, $username, $password, $dbname);

// controlla connessione
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

$stringa= "SELECT IdPOI,avg(voto) as media from visitapoi group by IdPOI;";

$result = $conn->query($stringa);

if ($result->num_rows > 0) {
    $riga = $result->fetch_assoc();

    echo "<table border = 1>";
    echo "<tr> <th> POI </th> <th> media dei voti </th> </tr>";
    echo "<tr> <td>". $riga['IdPOI']." </td> <td>". $riga['media']." </td> </tr>";
    while($riga = $result->fetch_assoc()) {
    echo "<tr> <td>". $riga['IdPOI']." </td> <td>". $riga['media']." </td>  </tr>";
    }
```

Quesito II *In relazione al tema proposto nella prima parte, si discuta la possibilità di allargare la fruizione dei contenuti multimediali anche ai dispositivi personali degli utenti. In particolare, si analizzino le seguenti due ipotesi alternative:*

- *uso limitato ai soli dispositivi (minitablet) forniti all'atto dell'acquisto del biglietto, come sopra descritto: si individuino possibili soluzioni per impedire l'accesso alle pagine multimediali attraverso dispositivi non forniti dagli InfoPoint;*
- *uso consentito ai dispositivi personali degli utenti (es. smartphone): si descriva una possibile integrazione del servizio volta a consentire la fruizione dei contenuti direttamente ad un singolo dispositivo di proprietà del visitatore, pur mantenendo i vincoli di fruibilità in base alla tariffa associata al biglietto.*

Nella prima alternativa ogni dispositivo si fa riconoscere dal server, inviandogli, oltre ai dati di registrazione, il proprio identificativo (IdTablet).
Nella seconda alternativa i visitatori potrebbero scaricare sui propri dispositivi personali, un'app dedicata che, previa registrazione, ottenga una password (a scadenza e non utilizzabile su più dispositivi contemporaneamente) e un codice identificativo, nel momento del pagamento del servizio.
In un'ottica più ampia, fatte le dovute distinzioni, questo caso potrebbe forse rientrare nella categoria più generale di Bring Your Own Device – BYOD, in cui gli utenti, appartenenti a un'organizzazione, utilizzano i dispositivi personali per accedere ai sistemi che sono loro riservati.

Quesito III *Nella realizzazione e gestione di una base di dati accessibile da categorie di utenti con differenti ruoli, sono di rilevante importanza gli aspetti relativi alla sicurezza dei dati. Ad esempio, si supponga che nella realtà scolastica il personale della "Segreteria Alunni" non debba accedere ai dati del personale docente, il personale della "Segreteria Docenti" non debba accedere all'elenco dei fornitori della scuola ecc. Il candidato approfondisca la tematica proposta discutendo gli strumenti offerti dai sistemi DBMS per creare utenze che abbiano un accesso libero alla totalità dei dati o limitato a parte di essi, in termini di operazioni consentite, in base al ruolo ricoperto nell'organizzazione. Produca quindi esempi significativi, nel contesto proposto della segreteria scolastica, nel linguaggio fornito dal DBMS di sua conoscenza.*

L'accesso ai dati può essere controllato (a livello di DBMS) definendo degli utenti e dando loro permessi per accedervi. Per fare questo utilizziamo i comandi SQL:

- `create user`
- `grant (revoke)`

Esempi:
```
create user "pluto"
IDENTIFIED BY "psw01";
GRANT ALL ON video TO
pluto
```

Con il commando GRANT è possibile assegnare a un utente il permesso di eseguire comandi SQL su una determinata tabella, o parte di essa; REVOKE revoca i permessi.
I possibili permessi che possono essere assegnati con GRANT sono qui sotto indicati.

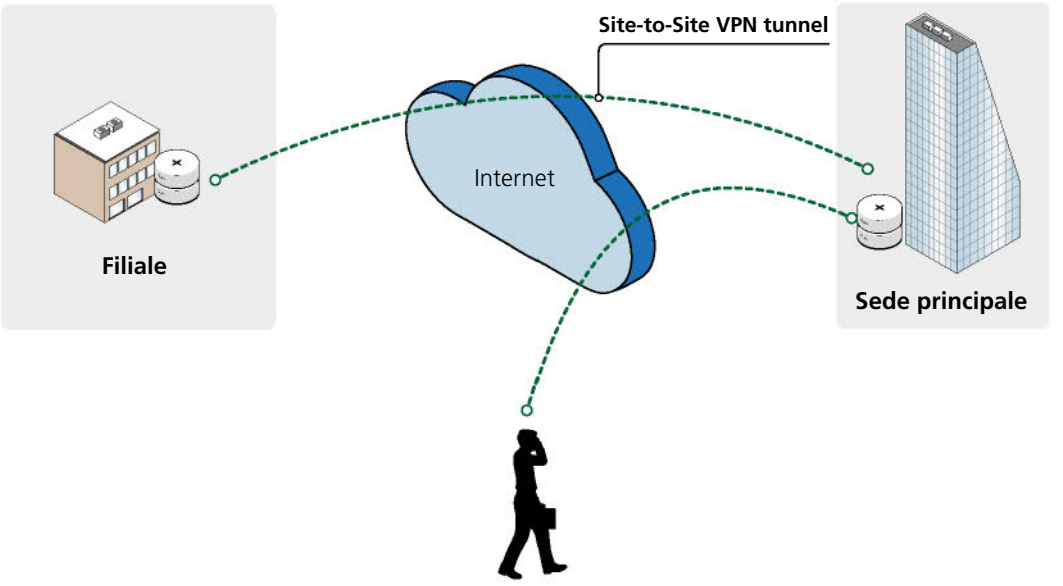
PERMESSO	ISTRUZIONI
ALL	tutte esclusa GRANT
ALTER	ALTER TABLE
CREATE	CREATE TABLE
CREATE TEMPORARY TABLES	CREATE TEMPORARY TABLE
CREATE VIEW	CREATE VIEW
DELETE	DELETE
DROP	DROP TABLE

PERMESSO	ISTRUZIONI
INDEX	CREATE INDEX, DROP INDEX
INSERT	INSERT
LOCK TABLES	LOCK TABLES
SELECT	SELECT
SHOW VIEW	SHOW CREATE VIEW
UPDATE	UPDATE
USAGE	nessuna
GRANT OPTION	GRANT, REVOKE

Quesito IV *Per le aziende che dispongono di sedi dislocate in varie località sorge spesso la necessità di consentire al personale l'accesso ai sistemi da postazioni remote. Il candidato discuta le tipologie e i protocolli di accesso remoto ai sistemi, indicando in particolare le possibilità offerte dalle connessioni VPN. Sviluppi poi esempi nel caso di una azienda che ha due sedi operative e agenti commerciali che, muovendosi sul territorio, hanno necessità di collegarsi al sistema informativo aziendale.*

La VPN (Virtual Private Network) è una rete privata virtuale che utilizza una rete pubblica per collegare tra loro terminali remoti come se appartenessero alla stessa rete locale . Ci possono essere due diverse soluzioni (Figura 2).

- **VPN ad accesso remoto** che permette di accedere a risorse remote di una LAN, per esempio a un dipendente (l'agente commerciale, nel nostro caso) di un'organizzazione fisicamente distante dalla sede aziendale. Necessitano di un "client VPN" che l'azienda stessa installa sul dispositivo utilizzato dall'utente per collegarsi (tablet, laptop) in modo da assicurare le regole di accesso ai propri server.
- **VPN Site-to-Site** che collegano in modo sicuro due o più sedi operative dislocate sul territorio, utilizzando la rete Internet. Il tunnel è stabilito tra apparati (gateway – router) delle sedi remote, con lo scopo di impedire l'intercettazione del dato aziendale trasmesso. A differenza delle VPN ad accesso remoto, i dispositivi remoti non necessitano di un client VPN, ma inoltrano il traffico attraverso i gateway VPN.



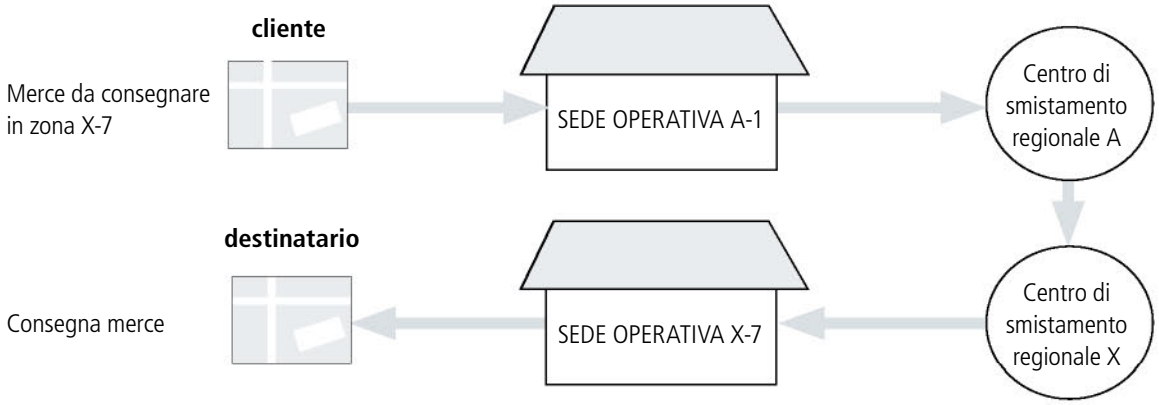
↑ **Fig. 2** Le due sedi operative (VPN Site-to-Site) e gli agenti commerciali (VPN ad accesso remoto).

ESAME DI STATO LUGLIO 2018

Indirizzo: ITIA – INFORMATICA E TELECOMUNICAZIONI – Articolazione: INFORMATICA
Tema di: SISTEMI E RETI – Tipologia C

Parte prima

La società FastDelivery si occupa della spedizione di pacchi su tutto il territorio nazionale, per varie tipologie di clienti (privati cittadini, ditte, operatori di commercio elettronico, ...).
FastDelivery possiede proprie Sedi Operative (SO) in molte città italiane anche di piccole-medie dimensioni. In tali sedi, dotate di magazzino, gli addetti si occupano del ritiro dei pacchi da spedire che vengono loro affidati dai clienti, oltre che della consegna ai destinatari finali dei pacchi loro smistati dalle altre Sedi Operative di FastDelivery.
Ogni SO invia i pacchi da spedire al proprio Centro di Smistamento Regionale (CSR) di riferimento, e riceve dal CSR i pacchi da consegnare ai destinatari finali nella propria zona.
Il disegno illustra il percorso di un pacco tra due differenti regioni. Per esempio, un cliente di Voghera (Lombardia) chiede di consegnare un pacco a un destinatario di Barletta (Puglia): il pacco verrà preso in carico dalla SO di Voghera (A-1 nel disegno) che la inoltrerà al CSR di Milano (A nel disegno), che a sua volta lo inoltrerà al CSR di Bari (X nel disegno) che infine la inoltrerà alla SO di Barletta (X-7 nel disegno) per la consegna al domicilio del destinatario finale.



FastDelivery vuole automatizzare maggiormente il processo di raccolta, smistamento e consegna. In particolare, ai fini del tracciamento, vuole introdurre un sistema di identificazione dei pacchi che consenta all'azienda, ai clienti e ai destinatari di seguirne la posizione nel loro percorso fino a destinazione.
Quando un cliente (mittente) vuole spedire un pacco, effettua una richiesta online: dalla SO più vicina, un trasportatore, recandosi presso il cliente per il ritiro, trasmette al sistema la presa in carico della spedizione. Un apposito algoritmo, già esistente, provvede a definire il percorso per la consegna di ciascun pacco. In ciascun passaggio del trasporto, il pacco viene prima preso in carico in ingresso e poi tracciato in uscita dai magazzinieri della SO o del CSR che gestisce il pacco stesso. Il trasportatore che porta a termine una consegna raccoglie la firma del destinatario e la trasmette al sistema di tracciamento.

Il candidato, fatte le opportune ipotesi aggiuntive:

Punto 1 ipotizzi come potrà essere organizzata operativamente la nuova procedura di gestione informatizzata dei pacchi (acquisizione dei dati di mittente e destinatario, presa in carico dal mittente, metodi di identificazione e procedure operative di tracciamento in ciascuna SO e CSR fino alla consegna, tipologia delle informazioni raccolte, rilevamento dell'avvenuta consegna);

Punto 2 illustri il progetto dell'infrastruttura informatica necessaria per realizzare la gestione automatizzata dei pacchi e consentirne la tracciabilità, dettagliando:
a) dispositivi utilizzati da trasportatori e magazzinieri per lo svolgimento delle proprie attività;

b) modalità di comunicazione tra i sistemi;
c) organizzazione dei server di raccolta dati e offerta dei servizi informativi; si sviluppino e discutano due o più ipotesi alternative, di cui una totalmente interna all'azienda e una che contempli anche il ricorso a servizi Cloud, scegliendone una motivatamente;

Punto 3 approfondisca gli aspetti legati alla sicurezza delle strumentazioni, dei dati gestiti e del servizio offerto nel caso in esame, e discuta le misure che ritiene utili per garantire la continuità del servizio (aspetti di *business continuity* e *fault tolerance*).

Parte seconda

Quesito I *In relazione al tema proposto nella prima parte, si vuole permettere a un utente di conoscere l'attuale stato della spedizione (l'elenco di SO o CSR da cui è già transitato il pacco e l'eventuale stato di avvenuta consegna). Il candidato progetti lo schema concettuale e il modello logico della porzione di base di dati necessaria; progetti poi le pagine web che consentono di ottenere le informazioni richieste, scrivendo in un linguaggio a scelta il codice di una parte significativa.*

Quesito II *In relazione al tema proposto nella prima parte, la società FastDelivery è interessata anche a poter monitorare gli spostamenti dei propri automezzi sulla strada in tempo reale. Il candidato illustri quali potrebbero essere le soluzioni tecnologiche disponibili e le modalità e i protocolli utilizzati nella comunicazione tra automezzi e centrale operativa.*

Quesito III *Le sfide poste dalla necessità di assicurare in qualsiasi momento l'accessibilità dei dati agli utenti autorizzati hanno portato allo sviluppo di metodologie di gestione note come clusterizzazione delle risorse hardware e virtualizzazione delle risorse software. Il candidato illustri in cosa consistono queste metodologie e analizzi vantaggi e svantaggi di ciascuna, anche con esemplificazioni applicative.*

Quesito IV *Le comunicazioni via e-mail spesso necessitano dell'applicazione di specifiche precauzioni per la sicurezza. Si descrivano le possibili minacce alle comunicazioni via e-mail e i principali protocolli e servizi per garantire la loro sicurezza.*

SVOLGIMENTO DELLA PROVA

Di seguito ti mostriamo una **traccia della soluzione** relativa alla prima parte e la risposta al primo quesito, soffermandoci – come abbiamo detto – sul **metodo generale di analisi del problema proposto e di progettazione della sua soluzione**.

Parte prima – Soluzione

La soluzione della prima parte si articola in due passi fondamentali:
A. la lettura del testo e l'individuazione delle parole chiave;
B. lo sviluppo dei 3 punti assegnati dal tema ministeriale.

A. LA LETTURA DEL TESTO E L'INDIVIDUAZIONE DELLE PAROLE CHIAVE

Per iniziare occorre leggere attentamente il testo e individuare le parole chiave su cui concentrare l'attenzione.

- FastDelivery si occupa della spedizione di pacchi su tutto il **territorio nazionale**.
- FastDelivery ha una struttura come quella proposta dalla traccia con **Sedi Operative** (**SO**), **Centro di Smistamento Regionale** (**CSR**).

- FastDelivery necessita di un'infrastruttura informatica (sia hardware che software) che permetta l'**identificazione dei pacchi** che consenta all'azienda, ai clienti e ai destinatari di seguirne la posizione nel loro percorso fino a destinazione.
- Quando un cliente (mittente) vuole spedire un pacco, effettua una **richiesta online**.
- Un apposito algoritmo, già esistente, provvede a definire il percorso per la consegna di ciascun pacco.
- In ciascun passaggio del trasporto, il pacco viene **prima preso in carico in ingresso e poi tracciato in uscita dai magazzinieri della SO o del CSR**.
- Il trasportatore che porta a termine una consegna **raccoglie la firma del destinatario e la trasmette al sistema di tracciamento**.

B. SVILUPPO DEI TRE PUNTI ASSEGNATI DAL TEMA MINISTERIALE

Punto 1

La definizione della sequenza dell'invio informatizzato del pacco

Con queste premesse possiamo ipotizzare la **sequenza di invio del pacco**.

- Il cliente (mittente), dopo essersi registrato sul sito web aziendale, compila il form relativo all'invio del pacco: caratteristiche del pacco, dati del destinatario ecc.
- Il server del sistema centrale rileva la richiesta, individua la Sede Operativa coinvolta che incarica un corriere a recarsi presso il cliente per prendere in carico il pacco.
- Il corriere si reca presso il cliente e ritira il pacco. Il corriere possiede un dispositivo mobile dedicato (o un'App su un tablet) collegato in rete con 4G, con il quale può registrare, tramite la rete Internet, il pacco ricevuto e inviarlo al sistema centrale. Viene anche emesso uno scontrino con un codice a barre che viene applicato al pacco e che ne permette l'identificazione lungo tutto il tragitto dal mittente al destinatario attraverso SO e CRS. (Un altro modo di identificare il pacco sarebbe quello di applicargli un'etichetta RFID.)
- Il corriere deposita il pacco presso SO. Il magazziniere, che dispone di un'applicazione software, legge l'etichetta con una pistola e registra l'ordine sul sistema centrale in modo che il pacco possa essere tracciato.
- Il pacco è inviato al CSR di competenza e, da qui, alla SO di destinazione. Per ogni stazione, i dati presenti sull'etichetta permettono di aggiornare il database del sistema centrale.
- Un corriere viene incaricato di portare il pacco al destinatario. Lo fa firmare e registra la consegna allo stesso modo di quanto fatto al momento della presa in carico del pacco e il database centrale viene aggiornato.

Punto 2

Il progetto dell'infrastruttura informatica necessaria

Il dettaglio dell'infrastruttura informatica dettagliato nei punti a), b) e c) può essere proposto come segue.

- Il servizio, come è naturale, sfrutta la rete Internet a cui ci si collega tramite dispositivi fissi (tipicamente dalle LAN presenti in SO e CSR) e mobili in 4G o WiFi (WPA-2), e ADSL nelle abitazioni dei clienti.
- Il server centrale non necessariamente deve risiedere in un CSR ed esporre i servizi di registrazione tramite un server web in DMZ, ma, meglio ancora, potrebbe essere in Cloud, con tutti i vantaggi che ne derivano, dai costi scalabili in funzione delle risorse e del numero di utenti che usufruiscono del servizio, alla continuità del servizio (24/24), al backup dei dati, alla sicurezza informatica e alla facilità di gestione.
- Un portale web in HTTPS per gli utenti.
- Un'applicazione RESTful dedicata e protetta per le applicazioni dei dispositivi mobili in dotazione al corriere. Anche in questo caso si può optare per HTTPS, anche se si può immaginare di collegare i dispositivi al server centrale tramite "Virtual Private Network (VPN)". In questo caso il dispositivo mobile del corriere potrebbe essere dotato di un client VPN, che non solo fornisce l'accesso sicuro (SSL), ma costringe, per esempio, un utente a connettersi solo all'infrastruttura aziendale, e dispone di firewall e antivirus.

Punto 3

La continuità del servizio

- Per gli aspetti relativi a **fault tolerance** si possono prevedere metodi di ridondanza RAID (Redundant Array of Independent Disks) e mirroring, con duplicazioni di memorie di massa e anche di server e apparati di rete.
- Per quanto riguarda la **business continuity**, cioè la capacità per una organizzazione di garantire l'erogazione dei propri servizi anche in caso di eventi avversi, è bene fare riferimento alle normative internazionali che, come ISO 22301 e successive, indicano le linee guida da seguire in caso di incidenti che potrebbero causare l'interruzione delle attività. Queste raccomandazioni non si riferiscono solo ad apparati e risorse fisiche, ma anche a persone e fornitori esterni, per la determinazione di un processo che potrebbe rivelarsi vitale addirittura per la sopravvivenza aziendale.
  Naturalmente nel caso si delegassero i servizi a un sistema in Cloud queste attività sarebbero coperte dal fornitore di servizi che, tipicamente, offre un "Business Continuity Plan", che contiene le procedure di risposta, recupero e ripristino delle attività a seguito di un'interruzione.

La Figura 1 presenta lo schema di massima dell'infrastruttura.

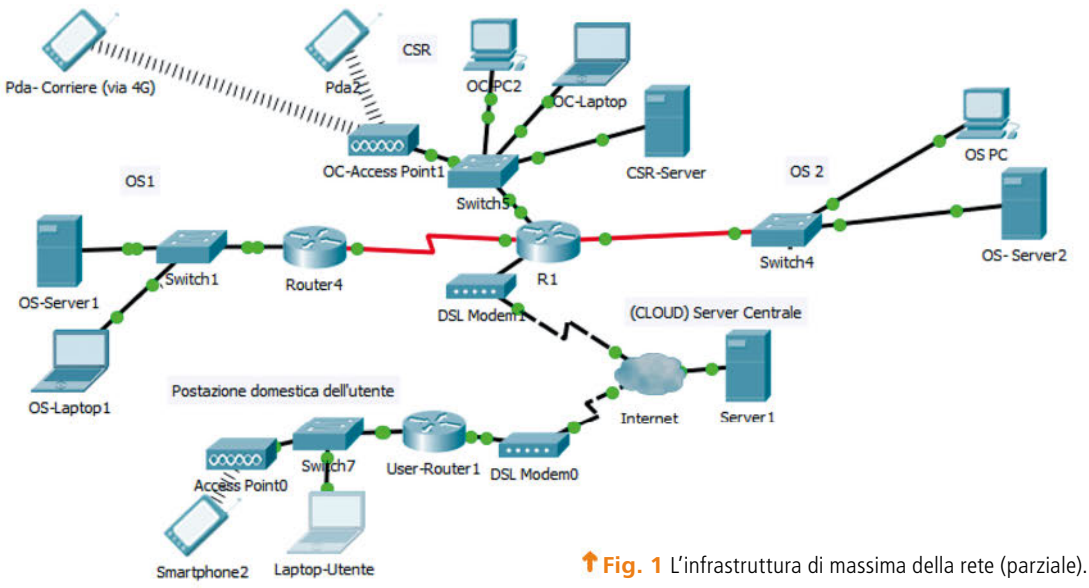


Fig. 1 L'infrastruttura di massima della rete (parziale).

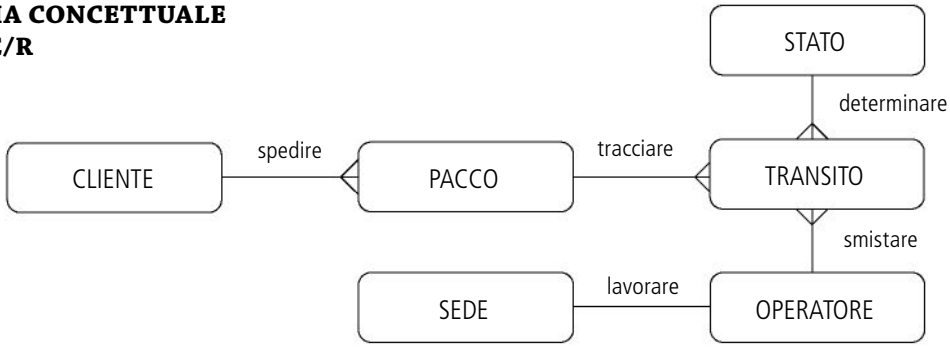
Parte seconda – Risposte ai quesiti

Quesito I *In relazione al tema proposto nella prima parte, si vuole permettere a un utente di conoscere l'attuale stato della spedizione (l'elenco di SO o CSR da cui è già transitato il pacco e l'eventuale stato di avvenuta consegna). Il candidato progetti lo schema concettuale e il modello logico della porzione di base di dati necessaria; progetti poi le pagine web che consentono di ottenere le informazioni richieste, scrivendo in un linguaggio a scelta il codice di una parte significativa.*

Il quesito chiede di progettare:

1. lo **schema concettuale** della porzione di basi di dati necessaria;
2. il **modello logico** della porzione di basi di dati necessaria;
3. le **pagine web** per ottenere le informazioni richieste, scrivendo in un linguaggio a scelta il codice di una parte significativa.

1. SCHEMA CONCETTUALE
Modello E/R



Attributi delle entità

- Cliente (CodCli, NomeCli, CognomeCli, Indirizzo, CodCity, UserID, Password).
- Pacco (CodPacco, Peso, NomeDest, CognomeDest, IndirizzoDest, CityDest).
- Sede (CodSede, Nome, Indirizzo, City).
- Stato (CodStato, Descrizione).
- Operatore (CodOperatore, Nome, Cognome, Tipo).
- Transito (CodPacco, CodStato, DataOra).

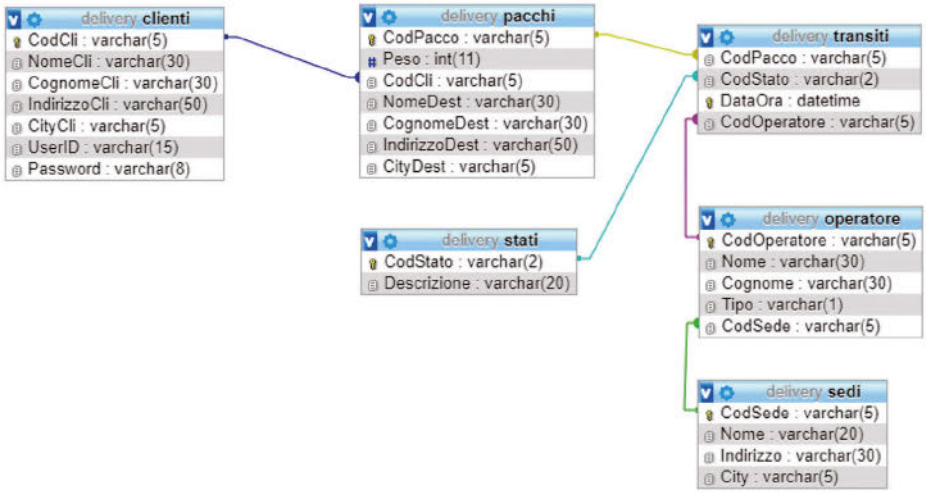
Descrizione delle entità

- Cliente: persona fisica o giuridica che si è registrata al sito web.
- Pacco: bene tangibile, oggetto trasportabile.
- Sede: luogo di raccolta dei pacchi; SO oppure CSR.
- Stato: condizione in cui può trovarsi un pacco: dal ritiro presso il cliente mittente alla consegna presso il destinatario finale.
- Transito: identifica il passaggio di un determinato pacco in un determinato stato.
- Operatore: personale dell'azienda che lavora in una sede. Può essere un trasportatore o un magazziniere.

Regole di lettura

- Un cliente spedisce uno o più pacchi, un pacco è spedito da un cliente.
- Un pacco è tracciato in uno o più transiti, un transito traccia un pacco.
- Uno stato determina uno o più transiti, un transito è determinato da uno stato.
- Un operatore smista un transito, un transito è smistato da un operatore.
- Un operatore lavora in una sede, in una sede lavorano uno o più operatori.

2. MODELLO LOGICO



Osservazioni

- La tabella "Stati" contiene i 10 possibili stati in cui può trovarsi un pacco:

s1	RITIRATO	**s6**	ARRIVATO ALLA CSR2
s2	ARRIVATO ALLA SO1	**S7**	PARTITO DALLA CSR2
s3	PARTITO DALLA SO1	**S8**	ARRIVATO ALLA SO2
s4	ARRIVATO ALLA CSR1	**S9**	IN CONSEGNA
s5	PARTITO DALLA CSR1	**SF**	CONSEGNATO

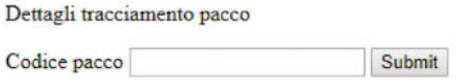
- Quando il cliente prenota un ritiro, l'algoritmo calcola il percorso e popola automaticamente la tabella "Transiti" con i 10 possibili stati in cui il pacco potrà trovarsi, lasciando null nel campo data.
  A ogni passaggio la riga corrispondente al pacco e allo stato sarà aggiornata dall'operatore (trasportatore in ingresso, magazziniere in uscita) con la data/ora del movimento.

3. PAGINE WEB

Di seguito forniamo il codice essenziale per la realizzazione delle pagine web. Potrebbe essere correlato di apposita interfaccia utente e layout adeguato.

pacco.html

form per richiedere il codice del pacco da tracciare




```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<title>trova pacco</title>
</head>
<body>
<p>Dettagli tracciamento pacco</p>
<form  method="post" action="cercastato.php">
 <label>Numero pacco <input type="text" name="numpacco" /></label>
 <input type="submit" name="invia" />
 </p>
</form>
</body>
</html>
```

cercastato.php

Codice php che, dato il codice del pacco, visualizza gli stati in cui il pacco si è trovato prima della data/ora corrente.

```
<!DOCTYPE html>
<html>
<head>
<title> letturadati </title>
</head>
<body>

<?php

//assegnare i valori in base al progetto
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "delivery";

// Crea connessione al database
$conn = new mysqli($servername, $username, $password, $dbname);

// controlla connessione
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

$numpacco=$_POST ['numpacco'];

$adesso=date("Y-m-d h:i:s");

$stringa= "select * from operatore o,transiti t, stati st, sedi s";
$stringa=$stringa . " where o.codoperatore = t.codoperatore and
s.codsede=o.codsede and t.codstato=st.codstato and dataora < '$adesso'
and codpacco='$numpacco' order by dataora desc";
$result = $conn->query($stringa);

if ($result->num_rows > 0) {
      $riga = $result->fetch_assoc();
      echo "codice pacco : " .$riga["CodPacco"].  "<p>";
      echo "<table border = 1>";
      echo "<tr> <th> data </th> <th> stato</th> <th> sede </th></tr>";
   echo "<tr> <td>". $riga['DataOra']." </td> <td>". $riga['Descrizione']."
</td> <td>". $riga['Nome']." </td> </tr>";
    while($riga = $result->fetch_assoc()) {
      echo "<tr> <td>". $riga['DataOra']." </td> <td>". $riga['Descrizione']."
</td> <td>". $riga['Nome']." </td> </tr>";
    }
      echo "</table>";
} else {
    echo "0 results";
}
$conn->close();
?>
</body>
</html>
```

SIMULAZIONE MINISTERIALE APRILE 2019

Indirizzo: ITIA – INFORMATICA E TELECOMUNICAZIONI – Articolazione: INFORMATICA
Tema di: INFORMATICA e SISTEMI E RETI

Parte prima

La compagnia ferroviaria *EasyTrain*, che ha sede in una nazione europea, fornisce, previa prenotazione online obbligatoria, servizi di viaggio a lunga percorrenza sul territorio nazionale. Una volta registrati sul portale web della compagnia, la prenotazione è effettuabile online: l'utente, dopo l'accesso mediante credenziali, può procedere ad acquistare un viaggio, selezionando carrozza e posto ed effettuando il relativo pagamento tramite carta di credito.
Il titolo di viaggio (biglietto) corrispondente alla prenotazione può essere stampato al termine della stessa, è comunque inviato all'utente via e-mail in formato PDF e riporta in chiaro: i dati dell'utente, i dati del viaggio ed un codice di prenotazione univoco (PU). Gli stessi dati sono codificati anche in un QR code per una più comoda lettura ottica del biglietto. Inoltre, il solo codice PU può essere inviato via SMS sul cellulare dell'utente su sua richiesta.
Il personale di servizio sul treno, ad ogni stazione, effettua la verifica dei biglietti dei viaggiatori saliti a bordo, confermando la presenza di ciascun viaggiatore ed il posto occupato. La verifica di un biglietto avviene online tramite una applicazione su dispositivi mobili in dotazione al personale; l'applicazione consente di acquisire i dati mediante lettura ottica del QR code o, in mancanza, tramite digitazione del codice PU.
Per rendere più confortevole il viaggio, la compagnia *EasyTrain* fornisce su tutte le carrozze un servizio di WiFi gratuito, a cui i viaggiatori possono accedere attraverso le stesse credenziali di accesso al portale di acquisto dei biglietti.
EasyTrain mette anche a disposizione dei viaggiatori un catalogo, frequentemente aggiornato, di una trentina di film, visualizzabili sul dispositivo mobile del viaggiatore stesso. Ciascun film in catalogo è descritto da una scheda che, oltre al titolo, riassume le caratteristiche del film quali genere, durata, attori principali, breve descrizione della trama, trailer. Per aggiornare il catalogo, EasyTrain si basa anche sulle statistiche di visualizzazione dei film da parte dei viaggiatori.
La qualità della connessione ad Internet offerta all'utente può evidenziare problemi a causa di diversi fattori quali, ad esempio, le caratteristiche del territorio attraversato, il numero di utenti collegati e le tecnologie impiegate. La visione dei film non dovrà essere soggetta a tali problematiche di connessione Internet.

Il candidato analizzi la realtà di riferimento e, fatte le opportune ipotesi aggiuntive, individui una soluzione che a suo motivato giudizio sia la più idonea per sviluppare i seguenti punti:

Punto 1 il progetto, anche mediante rappresentazioni grafiche, dell'infrastruttura tecnologica ed informatica necessaria a gestire il servizio nel suo complesso, dettagliando:
a) le modalità di comunicazione tra le varie componenti, relativamente alle operazioni di validazione dei biglietti sul treno e di accesso alla rete tramite credenziali da parte dei viaggiatori, descrivendo canali, dispositivi, protocolli e servizi di rete e motivando le scelte effettuate;
b) le soluzioni hardware e software per garantire una visione fluida e continuativa dei film sui dispositivi mobili dei viaggiatori indipendentemente dalle condizioni sopra esposte che influiscono sulla qualità della connessione ad Internet;

Punto 2 il progetto della porzione della basi di dati per la gestione del catalogo dei film e della loro fruizione da parte dei viaggiatori: si richiede in particolare il modello concettuale e il corrispondente modello logico;

Punto 3 la codifica in linguaggio SQL delle seguenti interrogazioni:
a) elenco dei film in catalogo ordinati per genere ed anno di produzione;
b) elenco in ordine alfabetico degli utenti che non hanno mai visualizzato alcun film;
c) dato un intervallo di tempo tra due date, produrre il titolo che ha registrato il maggior numero di visualizzazioni.

Parte seconda

Il candidato risponda a due quesiti a scelta tra quelli sotto riportati.

Quesito I *In relazione al tema proposto nella prima parte, in particolare al punto 3, si progettino le pagine che consentono, forniti eventuali parametri, la visualizzazione del risultato dell'esecuzione di una delle tre query. Il candidato codifichi le pagine stesse utilizzando linguaggi a sua scelta.*

Quesito II *In relazione al tema proposto nella prima parte, si consideri che* EasyTrain *per motivi di sicurezza è tenuta a mantenere un registro dei siti visitati dai viaggiatori attraverso la connettività WiFi a loro riservata. Si discutano le possibili soluzioni, anche tenendo conto degli aspetti legati alla privacy.*

Quesito III *Dato il seguente schema logico*
FARMACO (COD_F,NOME_F,DATA_PREPARAZIONE,DATA_SCADENZA,PREZZO)
COMPONENTE (COD_C,NOME_C,DESCRIZIONE)
CONTIENE (ID_FARMACO,ID_COMPONENTE,QUANTITA_C)
si chiede di:

a) disegnare il diagramma del modello concettuale corrispondente;
b) definire in linguaggio SQL il modello fisico corrispondente tenendo conto dei vincoli di integrità referenziali e/o vincoli di dominio;
c) esporre il significato delle varie tipologie di vincoli che si possono riscontrare nella progettazione delle basi di dati e dei riflessi che essi hanno sulle operazioni di inserimento, aggiornamento e cancellazione.

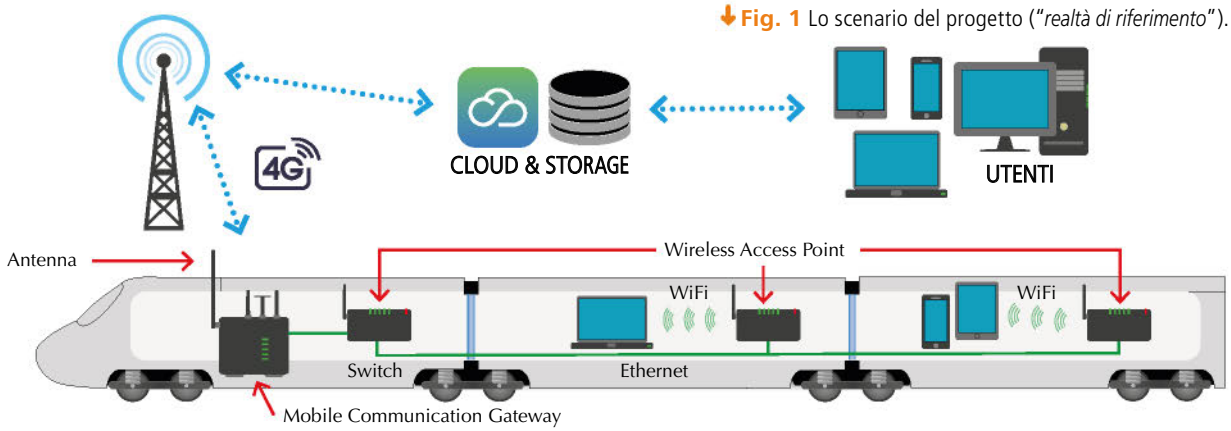
Quesito IV *In una azienda dotata di diversi uffici, alcuni dipendenti collegano impropriamente via cavo i laptop personali ai "punti di rete" della Lan aziendale, allo scopo di attivare, negli stessi laptop,* hot spot *WiFi "open" (senza protezioni) con cui fornire connessione per altri dispositivi, o propri o di eventuali ospiti non autorizzati. Il candidato tratti le conseguenze negative che una simile pratica può comportare per l'azienda e proponga soluzioni tecniche ed organizzative che potrebbero essere adottate per prevenire tali abusi.*

SVOLGIMENTO DELLA PROVA

Parte prima – Soluzione

Il metodo più diffuso per fornire connettività ai vagoni di un treno è il collegamento con le reti classiche 4G, le stesse utilizzate per i telefoni cellulari (alternativamente si potrebbe disporre di collegamento via satellite o tramite ponti radio dedicati). Una o più antenne esterne sono collegate a un dispositivo di comunicazione interno (router con un firewall per la sicurezza). Una rete interna Ethernet, che fa da dorsale, collega gli switch presenti nelle carrozze (**Figura 1**).

Fig. 1 Lo scenario del progetto ("*realtà di riferimento*").



Agli switch, presenti nelle carrozze, sono collegati gli Access Point (che possono disporre di un cavo radiante come antenna distribuita) che collegano i dispositivi mobili tramite WiFi.
(Il rilevatore GPS, non previsto nel compito, è comunque un interessante elemento a corredo).

Vincoli di progetto

- Copertura cellulari: è più intensa nei centri urbani e meno diffusa in periferia. Questo causa problemi di connettività.
- Gallerie (**Figura 2**) e condizioni geografiche (colline, montagne): possono limitare il segnale (*).
- Qualità del segnale della rete cellulare.
- Numero di passeggeri a bordo di una carrozza.
- Velocità del treno il quale, lanciato sopra i 200 chilometri orari, aggancia un ripetitore ogni qualche decina di secondi con spostamento delle connessioni e rischio di cali di segnale.

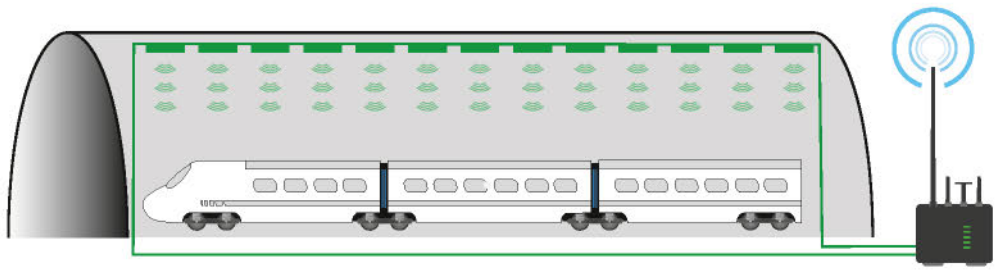


Fig. 2 Sempre più spesso le gallerie vengono "illuminate" con ripetitori radio che forniscono un sistema di copertura che è in grado di accorpare sistemi di soccorso radio e comunicazioni mobili proteggendoli da interferenza.

Punto 1

Nella sua essenza la rete, fatte le dovute precisazioni precedenti, può essere paragonata a una classica rete di edificio con cablaggio strutturato (vedi tema d'esame 2016) in orizzontale, con le carrozze al posto dei piani dell'edificio e con dorsale di collegamento effettuata con cavi Cat7 tramite Power over Ethernet (POE).
La rete comprende i seguenti dispositivi:

- un router di collegamento a Internet (Mobile Communication Gateway) che fornisce comunicazioni 4G/LTE affidabili con la possibilità di aggregazione dell'ampiezza di banda e che integra anche un firewall con meccanismi di sicurezza;
- un server dedicato che eroga i contenuti multimediali ai passeggeri.
- Su ogni carrozza del treno sono installati:
  - uno switch collegato alla dorsale
  - un access point (AP) (eventualmente con ripetitori) per il collegamento wireless dei dispositivi mobili

Tema d'esame 2016

Punto 1.a

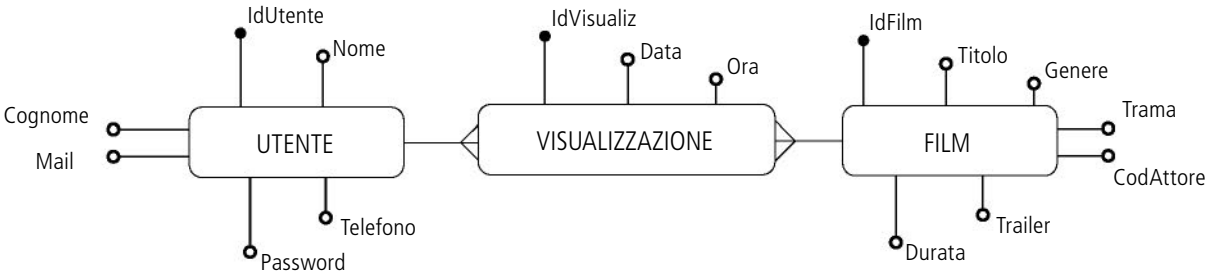
- I canali (**Figura 1**) comprendono: la rete 4G, la dorsale interna, i collegamenti WiFi.
- L'accesso dei passeggeri al server web della compagnia (che potrebbe essere in cloud) avviene dietro presentazioni delle credenziali ottenute con la registrazione del viaggio e utilizza il protocollo HTTPS.
- La gestione centralizzata dei diversi AP è garantita da un wireless LAN controller in collaborazione con il server RADIUS per il monitoraggio e l'autenticazione degli utenti (userID, indirizzo IP, indirizzo MAC, durata connessione...) e la gestione del roaming. La sicurezza per l'accesso alla rete WiFi interna (802.11x) è garantita dallo standard WPA2 (IEEE 802.11i).
- Il controllo del personale di bordo per la validazione dei biglietti avviene con un dispositivo mobile che ha la possibilità di leggere il QR-code o di inserire il codice del biglietto. Il collegamento con il cloud avviene utilizzando un tunnel VPN (con protocollo SSL). Il server in cloud, con servizio SaaS, espone delle API Restful per l'accesso alle risorse e lo scambio dei dati da validare.

Punto 1.b

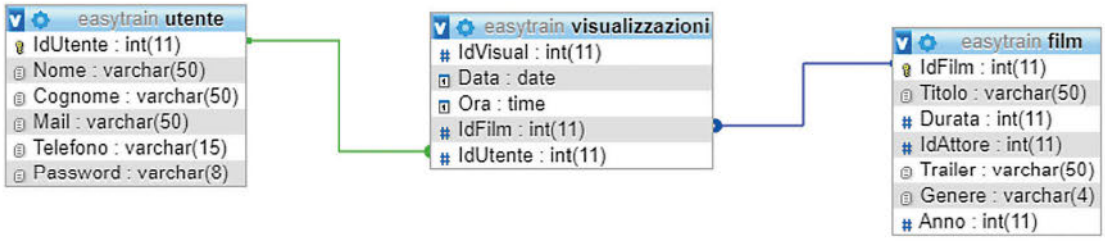
Un **server locale** presente sul treno potrebbe essere una soluzione pratica immediata per usufruire dei film ottenendo una visione fluida slegata dalla rete mobile e dai relativi problemi di collegamento e di banda. Rimane la necessità di aggiornare il server con i nuovi film e il catalogo online in tempi differiti rispetto alla loro visione. Si potrebbe anche ipotizzare, prendendo spunto dai server VOD (video-on-demand) e dalla "rete per la distribuzione dei contenuti – CDN" (CDN), di dotare il server locale di una web caching per il buffering dei film. Se un cliente scarica un film, questo è inserito nel server locale. Un secondo cliente che desidera lo stesso film lo preleva direttamente dalla cache del server locale con un tempo di risposta e una fluidità nettamente superiore. Naturalmente bisognerà dimensionare il server (o i server) in funzione dl numero di utenti che, statisticamente, scaricano i film. Inoltre, per migliorare il download da Internet potrebbero essere predisposte più antenne per ricevitori 4G che andrebbero a contribuire all'aggregazione delle singole bande in modo da aumentare la banda globale servendosi di un router di bilanciamento.

Punto 2

Modello concettuale



Modello logico



Punto 3

Codifica in linguaggio SQL

La codifica del linguaggio SQL delle interrogazioni ai punit a), b) e c) è sotto riportato.

```
Query a
SELECT titolo, genere, Anno from film order BY genere, anno

Query b
select cognome,Nome
from utente u, (select idutente as novis
                                  from utente
                                  where idutente not in (
                                              select idutente
                                              from visualizzazioni)
                                                          ) t1
where u.idutente =novis
order by cognome, nome
```

```
Query c
select max(totvis) as masvis, t1.idfilm, titolo
from (

select   v.idfilm, count(*) as totvis
from visualizzazioni v
where data between '2019-03-01' and '2019-03-31'
group by idfilm) t1, film f
where t1.idfilm = f.idfilm
```

Parte seconda – Risposte ai quesiti

Quesito I *In relazione al tema proposto nella prima parte, in particolare al punto 3, si progettino le pagine che consentono, forniti eventuali parametri, la visualizzazione del risultato dell'esecuzione di una delle tre query. Il candidato codifichi le pagine stesse utilizzando linguaggi a sua scelta.*

Elenco dei film in catalogo ordinati per genere e anno di produzione:

```
<!DOCTYPE html>
<html>
<head>
<title> elenco film </title>
</head>
<body>

<?php
//elenco dei film in catalogo ordinati per genere ed anno di produzione
//assegnare i valori in base al progetto
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "easytrain";

// Crea connessione al database
$conn = new mysqli($servername, $username, $password, $dbname);
// controlla connessione
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

$stringa= "SELECT titolo, genere, Anno from film order BY genere, anno";

$result = $conn->query($stringa);

if ($result->num_rows > 0) {
      $riga = $result->fetch_assoc();

      echo "<table border = 1>";
      echo "<tr> <th> titolo </th> <th> genere </th> <th> anno </th>
</tr>";
```

```
      echo "<tr> <td>". $riga['titolo']." </td> <td>". $riga['genere']." </
td> <td>". $riga['Anno']." </td> </tr>";
    while($riga = $result->fetch _ assoc()) {
      echo "<tr> <td>". $riga['titolo']." </td> <td>". $riga['genere']." </
td> <td>". $riga['Anno']." </td> </tr>";
    }
      echo "</table>";
} else {
      echo "0 results";
}
$conn->close();

?>
</body>
</html>
```

Elenco in ordine alfabetico degli utenti che non hanno mai visualizzato alcun film:

```
<!DOCTYPE html>
<html>
<head>
<title> elenco film </title>

</head>
<body>
<?php
//elenco dei film in catalogo ordinati per genere ed anno di produzione
//assegnare i valori in base al progetto
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "easytrain";

// Crea connessione al database
$conn = new mysqli($servername, $username, $password, $dbname);

// controlla connessione
if ($conn->connect _ error) {
    die("Connection failed: " . $conn->connect _ error);
}

//$stringa= "select cognome, nome from utente where idutente = (select
idutente from utente where idutente not in (select idutente from visua-
lizzazioni));";
//$stringa="select cognome,nome from utente u, (select idutente as novis
from utente where idutente";
//$stringa= $stringa . "not in (select idutente from visualizzazioni)) t1
where u.idutente =novis;";
 $stringa = "select cognome,nome\n"
```

```
    . "from utente u, (select idutente as novis\n"
    . "                          from utente \n"
    . "                          where idutente not in (\n"
    . "                                       select idutente \n"
    . "                                       from visualizzazioni) \n"
    . "                                                  ) t1\n"
    . "where u.idutente =novis order by cognome, nome";

$result = $conn->query($stringa);

if ($result->num_rows > 0) {
     $riga = $result->fetch_assoc();

     echo "<table border = 1>";
     echo "<tr> <th> cognome </th> <th> nome </th> </tr>";
   echo "<tr> <td>". $riga['cognome']." </td> <td>". $riga['nome']." </td>
</tr>";
    while($riga = $result->fetch_assoc()) {
     echo "<tr> <td>". $riga['cognome']." </td> <td>". $riga['nome']."  </tr>";
    }
     echo "</table>";
} else {
    echo "0 results";
}
$conn->close();


?>
</body>
</html>
```

Quesito II *In relazione al tema proposto nella prima parte, si consideri che* EasyTrain *per motivi di sicurezza è tenuta a mantenere un registro dei siti visitati dai viaggiatori attraverso la connettività WiFi a loro riservata. Si discutano le possibili soluzioni, anche tenendo conto degli aspetti legati alla privacy.*

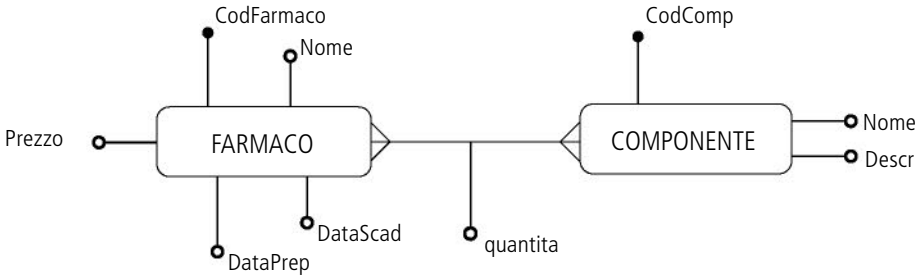
Sarebbe preferibile non eseguire l'autenticazione degli utenti associando a essi un MAC address (che, di fatto, identifica il dispositivo utilizzato ma non l'utente ed è facilmente modificabile), ma è consigliabile un'autenticazione più sicura su base SIM e numero di cellulare, associata al passeggero.
Le informazioni relative ai siti visitati (soggetti a una possibile limitazione da parte del firewall presente sul treno) possono essere spediti al server in Cloud e qui memorizzati per successivi controlli e statistiche.
In realtà a norma di legge (98/2013) gli utenti possono accedere al servizio WiFi senza essere identificati personalmente anche se, in molti casi, l'autenticazione può essere utile per applicare una serie di regole al servizio, come per esempio la durata delle sessioni o per monitorare gli accessi ed evitare alla compagnia di trasporto di essere ritenuta corresponsabile di eventuali violazioni commesse dai passeggeri.

Quesito III *Dato il seguente schema logico*

FARMACO (COD_F,NOME_F,DATA_PREPARAZIONE,DATA_SCADENZA,PREZZO)
COMPONENTE (COD_C,NOME_C,DESCRIZIONE)
CONTIENE (ID_FARMACO,ID_COMPONENTE,QUANTITA_C)
si chiede di:

a) disegnare il diagramma del modello concettuale corrispondente;
b) definire in linguaggio SQL il modello fisico corrispondente tenendo conto dei vincoli di integrità referenziali e/o vincoli di dominio;
c) esporre il significato delle varie tipologie di vincoli che si possono riscontrare nella progettazione delle basi di dati e dei riflessi che essi hanno sulle operazioni di inserimento, aggiornamento e cancellazione.

Il modello concettuale



Di seguito è riportato il modello fisico corrispondente in inguaggio SQL:

```
CREATE TABLE farmaci (
    CodFarmaco int NOT NULL,
    Nome varchar (25) NOT NULL,
    Prezzo  float not null,
    DataPreparazione  date,
    DataScadenza date,
    PRIMARY KEY (CodFarm)
);

CREATE TABLE componenti (
    Codcomp int NOT NULL,
    Nome varchar (25) NOT NULL,
    Descr  varchar (100),
    PRIMARY KEY (Codcomp)
);

CREATE TABLE Contiene (
    CodFarmaco int NOT NULL,
    CodComp int NOT NULL,
    Quantita int NOT NULL,
    PRIMARY KEY (CodFArmaco,CodComp),
    FOREIGN KEY (CodFArmaco) REFERENCES farmaci(CodFarmaco)
    ON DELETE CASCADE
    ON UPDATE CASCADE,
    FOREIGN KEY (CodComp) REFERENCES Componenti(CodComp)
    ON DELETE CASCADE
    ON UPDATE CASCADE
);
```

```
CREATE TABLE dosi (
    IdDose int not null,
    IdPrepar int NOT NULL,
    idComp int not null,
    quantita int not null,
    PRIMARY KEY (IdDose),
    FOREIGN KEY (IdComp) REFERENCES Prepareazione(IdPrepar)
    ON DELETE CASCADE
    ON UPDATE CASCADE,
    FOREIGN KEY (IdPrepar) REFERENCES Prepareazione(IdPrepar)
    ON DELETE CASCADE
    ON UPDATE CASCADE
);
```

I vincoli di integrità si applicano ai diversi elementi.

- Integrità sull'entità: nessun elemento della chiave primaria può avere valore null imposto con "not null" nella create. Anche se non si mette è implicito che la PK non può avere valore null.
- Integrità sugli attributi: sono vincoli che devono essere rispettati dai valori degli attributi.
  Per esempio se un attributo è obbligatorio occorre crearlo con "not null". È possibile in fase di creazione tabella utilizzare l'opzione "check" per imporre dei vincoli sui valori dei campi.
- Integrità sulle associazioni (integrità referenziale):
  per garantire l'integrità dei dati il valore di una chiave esterna o è null, oppure deve avere un valore presente come PK nella tabella associata.
  I problemi si potrebbero verificare in caso di:
  INSERIMENTO: non è possibile inserire una riga con FK non presente come PK;
  MODIFICA: non è possibile modificare una PK se ci sono FK associate;
  CANCELLAZIONE: non è possibile cancellare una PK se ci sono FK associate.

In caso di modifica o cancellazione è possibile in fase di create table specificare il comportamento.
In caso di modifica:

- **cascade**: il nuovo valore dell'attributo della tabella principale viene riportato su tutte le corrispondenti righe della tabella secondaria (a cascata);
- **set null**: alla chiave esterna della tabella secondaria viene assegnato il valore nullo al posto del valore modificato nella tabella principale;
- **set default**: alla chiave esterna della tabella secondaria viene assegnato il corrispondente valore di default al posto del valore modificato nella tabella principale;
- **no action**: nessuna azione viene intrapresa e viene generato un errore.

In caso di cancellazione:

- **cascade**: le corrispondenti righe della tabella secondaria vengono cancellate (in cascata);
- **set null**: alla chiave esterna della tabella secondaria viene assegnato il valore nullo al posto del valore cancellato nella tabella principale;
- **set default**: alla chiave esterna della tabella secondaria viene assegnato il corrispondente valore di default al posto del valore cancellato nella tabella principale;
- **no action**: nessuna azione viene intrapresa e viene generato un errore.

Quesito IV *In una azienda dotata di diversi uffici, alcuni dipendenti collegano impropriamente via cavo i laptop personali ai "punti di rete" della Lan aziendale, allo scopo di attivare, negli stessi laptop,* hot spot *WiFi "open" (senza protezioni) con cui fornire connessione per altri dispositivi, o propri o di eventuali ospiti non autorizzati. Il candidato tratti le conseguenze negative che una simile pratica può comportare per l'azienda e proponga soluzioni tecniche ed organizzative che potrebbero essere adottate per prevenire tali abusi.*

Di principio i *laptop personali* non dovrebbero poter accedere alla rete aziendale e fornire servizi hot spot WiFi. Per questo andrebbero autorizzati preventivamente e controllati al momento del collegamento. La cosa più semplice (ma non consigliata, per motivi di sicurezza) è il controllo dell'indirizzo MAC. Meglio è la presenza di un certificato caricato sul laptop a cura dell'azienda o la possibilità di disporre di un token USB, una chiavetta elettronica che, protetta dalla crittografia, permette di accedere a servizi garantendo l'identità del proprietario. Inoltre si rimanda alla possibilità di autenticarsi e ottenere le autorizzazioni tramite il protocollo Kerberos (RFC 4120).

In realtà a norma di legge (98/2013) gli utenti possono accedere al servizio WiFi senza essere identificati personalmente anche se, in molti casi, l'autenticazione può essere utile per applicare una serie di regole al servizio, come per esempio la durata delle sessioni o per monitorare gli accessi ed evitare alla compagnia di trasporto di essere ritenuta corresponsabile di eventuali violazioni commesse dai passeggeri.

SIMULAZIONE MINISTERIALE FEBBRAIO 2019

Indirizzo: ITIA – INFORMATICA E TELECOMUNICAZIONI Articolazione: INFORMATICA
Tema di: INFORMATICA e SISTEMI E RETI – FEBBRAIO 2019

Parte prima

Il Comune di una città europea di medie dimensioni vuole implementare, per sostenere politiche di mobilità sostenibile, un servizio di noleggio di biciclette attraverso stazioni di "noleggio e riconsegna" dislocate in diversi punti della città. Al fine di addebitare il costo del servizio di noleggio, si vuole conoscere in ogni momento chi ha preso in uso una determinata bicicletta. Il servizio è fruibile previa registrazione online dei dati dell'utente, incluso un numero di carta di credito valida. A seguito della registrazione, il Comune provvederà alla consegna di una tessera elettronica (smart card) al domicilio dell'utente o presso appositi uffici, che conterrà il codice identificativo dell'utente leggibile in modalità senza contatto (contactless). Ogni stazione di noleggio e riconsegna è dotata di cinquanta slot, ciascuno dei quali può ospitare una bicicletta ed è dotato di un sistema di blocco meccanico della bicicletta stessa, mediante un lucchetto controllato elettronicamente. Per noleggiare una bicicletta, l'utente dovrà avvicinare la propria tessera elettronica a un apposito lettore, unico per la stazione: di conseguenza verrà sbloccata una delle biciclette inserite negli slot. Ogni bicicletta è dotata di un proprio tag a radiofrequenza (RFID) che ne riporta il codice univoco: questo tag viene letto da un apposito dispositivo su ogni slot (RFID reader) sia in ingresso che in uscita della bicicletta. L'utente potrà successivamente riconsegnare la bicicletta presso una qualsiasi stazione cittadina (quella di noleggio o un'altra) che abbia slot liberi. In questo modo, per ogni stazione è sempre possibile sapere quali biciclette sono bloccate negli slot e disponibili per il noleggio, quali sono state noleggiate e quali vengono riconsegnate. L'operazione di noleggio o di riconsegna di una bicicletta comporta la registrazione dei seguenti dati:

- identificativo della bicicletta noleggiata o riconsegnata;
- identificativo dell'utente;
- data e ora dell'operazione;
- identificativo della stazione di noleggio o di riconsegna.

La registrazione dei dati delle due operazioni è finalizzata anche alla loro trasmissione in tempo reale a un sistema centrale per il monitoraggio, controllo e tariffazione del servizio. Per mezzo di una mappa, visualizzabile su Web o su App per telefono cellulare, si può conoscere per ogni stazione cittadina quante biciclette sono disponibili per il noleggio e quanti slot sono liberi per la riconsegna di una bicicletta noleggiata.

Il candidato analizzi la realtà di riferimento e, fatte le opportune ipotesi aggiuntive, individui una soluzione che a suo motivato giudizio sia la più idonea per sviluppare i seguenti punti:

Punto 1 il progetto, anche mediante rappresentazioni grafiche, dell'infrastruttura tecnologica e informatica necessaria a gestire il servizio nel suo complesso, dettagliando:

a) l'infrastruttura di comunicazione, in termini di caratteristiche dei canali, degli apparati e dei protocolli, che permette di trasmettere le informazioni di ciascuna stazione al sistema centrale;
b) le caratteristiche generali dei componenti hardware e software del sistema sia a livello centrale che nelle stazioni;
c) le misure e gli apparati per assicurare la continuità del servizio;

Punto 2 il progetto della base di dati per la gestione delle informazioni relative agli utenti, alle operazioni di noleggio e riconsegna delle biciclette, e alla situazione di occupazione delle stazioni: in particolare si richiede il modello concettuale e il corrispondente modello logico;

Punto 3 il progetto delle pagine web che permettono le seguenti funzioni, codificandone una con i linguaggi ritenuti più idonei:

a) a partire da una mappa delle stazioni, verificare se una stazione ha bici disponibili per il noleggio;
b) consentire al gestore del sistema di visualizzare le bici attualmente in uso, da quali utenti e presso quale stazione sono state prelevate.

Parte seconda

Quesito I *In relazione al tema proposto, si integri il progetto con le pagine che consentono la produzione di un report contenente le bici noleggiate da un utente, le stazioni in cui sono state prelevate e restituite, la durata del noleggio e i relativi costi. Si discuta la problematica riguardante l'invio periodico e automatico del suddetto report sulla base di una temporizzazione impostata dall'utente nel suo profilo, e si proponga una soluzione motivandola adeguatamente.*

Quesito II *In relazione al tema proposto nella prima parte, si sviluppino in linguaggio SQL le query che consentono di soddisfare le seguenti richieste: a) dato il codice di una bicicletta elencare gli utenti che l'hanno utilizzata nel mese corrente; b) mostrare la stazione presso la quale è stato effettuato il maggior numero di noleggi in un dato periodo.*

Quesito III *Considerata la relazione QUADRO (Cod_Quadro, Cod_Museo, Titolo_Quadro, Nome_Museo, Citta_Museo, Prezzo, DataInizioEsposizione, DataFineEsposizione) si verifichino le proprietà di normalizzazione e si proponga, eventualmente, uno schema equivalente che rispetti la terza forma normale, motivando le scelte effettuate.*

Quesito IV *Alla luce delle problematiche relative alla sicurezza e integrità delle informazioni archiviate nei sistemi informatici e della loro riservatezza, si discutano vantaggi e svantaggi delle principali tecniche per l'autenticazione degli utenti di un sistema informatico di rete, discutendo sistemi e protocolli utilizzati in tale contesto.*

SVOLGIMENTO DELLA PROVA

Parte prima – Soluzione

La soluzione della Parte prima si articola in due passi fondamentali:

A. la lettura del testo e l'individuazione delle parole chiave;

B. lo sviluppo dei 3 punti assegnati dal tema ministeriale.

A. LA LETTURA DEL TESTO E L'INDIVIDUAZIONE DELLE PAROLE CHIAVE

- Città europea di medie dimensioni.
- Noleggio di biciclette attraverso stazioni dislocate in diversi punti della città.
- **Registrazione online** dei dati dell'utente, pagamento con carta di credito:
  - **portale web** con protocollo https;
  - **smart card contactless**, con il codice identificativo dell'utente (ID_UTENTE).
- Stazione di noleggio:
  - 50 slot;
  - smart card per noleggio e sblocco su lettore della stazione.
- Ogni bicicletta è dotata di un proprio **tag a radiofrequenza** (**RFID**) con codice univoco (ID_BICI).
- Per ogni stazione è sempre possibile sapere quali biciclette **sono bloccate negli slot e disponibili**:
  - sistema centrale online per il monitoraggio, controllo e tariffazione del servizio.
- Mappa su Web o su App con biciclette disponibili per il noleggio e indicazione di quanti sono gli slot liberi per la riconsegna di una bicicletta noleggiata.

B. SVILUPPO DEI 3 PUNTI ASSEGNATI DAL TEMA MINISTERIALE

Punto 1

Nel **Punto 1.a** occorre progettare l'**infrastruttura di comunicazione**, che permette di trasmettere le informazioni di ciascuna stazione al sistema centrale.

La Figura 1 schematizza la catena di rilevazione ed elaborazione dei dati (comune a molti casi).

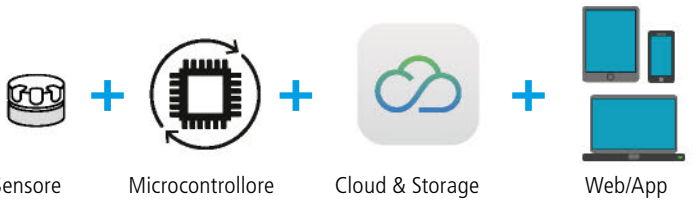


Fig. 1 La logica per la rilevazione e l'elaborazione dei dati prevede sensori (ed eventuali attuatori) per la rilevazione dei parametri fisici; la loro elaborazione locale per una gestione più efficiente (*fog computing*); l'invio a una piattaforma remota per lo sviluppo di applicazioni cloud-based; l'interazione con gli utenti.

Nel **Punto 1.b** occorre definire le **caratteristiche generali dei componenti hardware e software** del sistema sia a livello centrale che nelle stazioni. Il risultato a cui giungeremo è illustrato nella Figura 2.

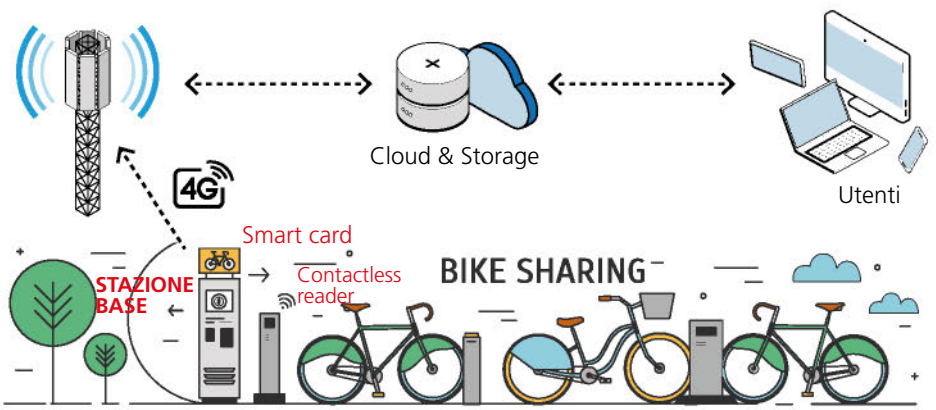


Fig. 2 Lo schema generale di funzionamento dell'intero sistema: i lettori RFID negli slot con il meccanismo di sblocco delle bici; la stazione base che contiene il microcontrollore e il lettore di smart card; il collegamento in 4G tramite APN; la piattaforma remota per lo sviluppo di applicazioni cloud-based che comprende anche lo storage; il collegamento con utenti/amministratori.

Esaminiamo i componenti hardware e software.

Stazione

- Microcontrollore (per esempio Raspberry Pi).
- Lettore/scrittore "SMARTCARD CONTACTLESS RFID NFC": collegamento tramite interfaccia USB al microcontrollore. I dati pervengono al microcontrollore da interfaccia USB come se fossero prelevati da tastiera.
- Sensori/attuatori.
- Un sensore RFID (*RadioFrequency IDentification*) utilizza radiofrequenze allo scopo di identificare e tracciare i tag attaccati agli oggetti. Il sensore può disporre di un'antenna incorporata per il collegamento radio con il microcontrollore (Figura 3).
  Nota: in alternativa, ma in modo meno efficiente, si potrebbero utilizzare anche sensori associati a una scheda intelligente, per esempio Arduino o Raspberry, dotata di indirizzo IP e collegata alla stazione via seriale (o con schede Ethernet o WiFi), oppure sensori intelligenti.



Fig. 3 ID-12LA (ID Innovations) è un lettore RFID molto semplice da usare con un'antenna incorporata.

- Un attuatore con un relè, gestito da microcontrollore, che pilota il sistema elettromeccanico per l'aggancio/sgancio della bici nello slot.
- 4G (con APN) per collegamento protetto microcontrollore-server (eventualmente tramite VPN).
  Nota: APN (Access Point Name) fa da gateway tra la rete mobile 4G e la rete Internet su cui risiede il server. Il dispositivo mobile che effettua una connessione dati deve essere configurato con un APN per poter ottenere dal fornitore di servizi l'indirizzo IP, il tipo di servizio e gli altri parametri necessari alla connessione.

Sistema centrale

- Piattaforma remota per lo sviluppo di applicazioni cloud-based per l'interazione con l'utente e lo storage dei dati. Il server remoto espone i propri servizi web (Web Service) nella modalità RESTful. Le API web specificano il modo con cui i componenti software devono interagire tra loro, utilizzando il protocollo HTTP come intermediario. Il client utilizza i classici comandi HTTPO ("verbi") per interagire con il servizio:
  - POST per creare una risorsa;
  - GET per restituire una rappresentazione della risorsa;
  - PUT per aggiornare lo stato di una risorsa;
  - DELETE per eliminare una risorsa.

Considerazione sulla trasmissione e sui protocolli

- Un portale web in HTTPS per gli utenti.
- Collegamento delle stazioni base al server centrale tramite "Virtual Private Network (VPN)". La stazione base è dotata di un client VPN che non solo fornisce l'accesso sicuro (SSL), ma dispone di firewall e antivirus.

Nel **Punto 1.c** possiamo analizzare che la piattaforma cloud offre i servizi completi per tutti gli aspetti legati a fault tolerance e business continuity. Di solito il fornitore di servizi mette a disposizione un "**Business Continuity Plan**" che contiene le procedure di riposta, recupero e ripristino delle attività a seguito di un'interruzione.

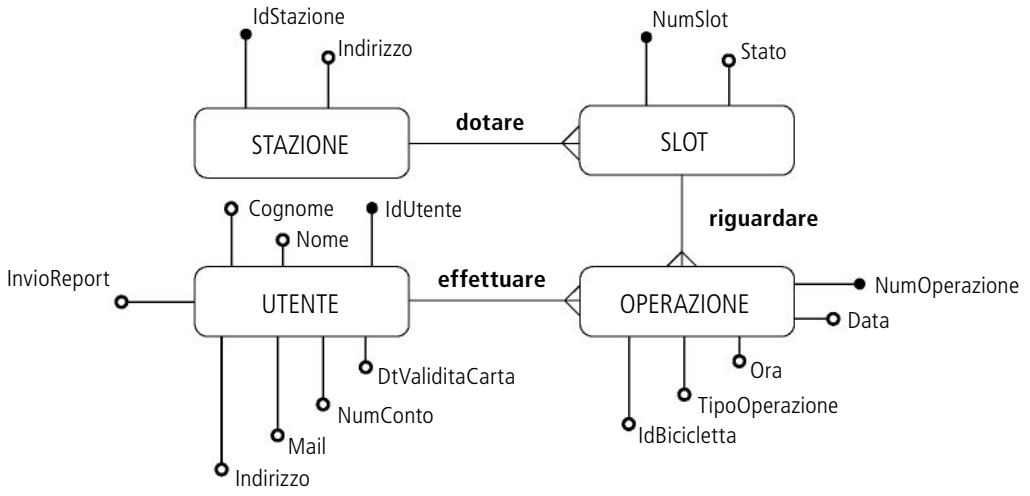
- **Fault tolerance**: è l'insieme dei dispositivi hardware necessari per evitare interruzioni nei servizi erogati a fronte di guasti tecnici. Sostanzialmente si tratta di disporre di hardware specializzati per rilevare guasti hardware (processori, memorie, dispositivi di rete, alimentatori ecc.) e transitare immediatamente a hardware ridondanti:
  - RAID (*Redundant Array of Independent Disks*);
  - mirroring con duplicazioni di memorie di massa;
  - duplicazioni di server e apparati di rete.
- **Business continuity**: è la capacità per una organizzazione di garantire l'erogazione dei propri servizi anche in caso di eventi avversi.
  Di fatto si tratta di valutare non solo la disponibilità e la replica dei componenti fisici, ma di far cooperare le risorse hardware e software per ripristinare rapidamente i servizi essenziali e ridurre al minimo i tempi di fermo macchina.
  ISO 22301 e successive normative internazionali forniscono le linee guida da seguire in caso di incidenti che potrebbero causare l'interruzione delle attività e portare, in casi estremi, a mettere a rischio la sopravvivenza aziendale. Queste raccomandazioni non si riferiscono solo ad apparati e risorse fisiche e logiche, ma anche a persone e fornitori esterni.

Punto 2

Progettazione della base di dati necessaria per gestire le informazioni

Occorre progettare la base di dati per la gestione delle informazioni relative agli utenti, alle operazioni di noleggio e riconsegna delle biciclette e alla situazione di occupazione delle stazioni. Allo scopo, occorre redigere il modello concettuale e il corrispondente modello logico.

Modello concettuale



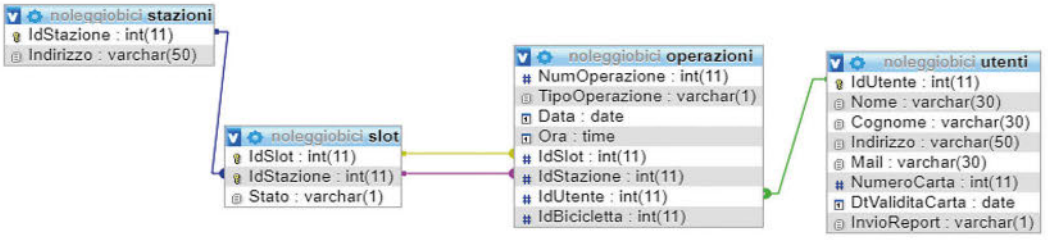
Descrizione delle entità

Stazione: luogo fisico in cui è possibile noleggiare o restituire una bicicletta.
Slot: punto in cui è "agganciata" una bicicletta.
Utente: persona fisica che è registrata al servizio di noleggio biciclette.
Operazione: noleggio (N) o restituzione (R) di una bicicletta.

Regole di lettura

Stazione/Slot: una stazione è dotata di più slot, uno slot è in dotazione a una stazione.
Slot/Operazione: uno slot riguarda una o più operazioni, un'operazione riguarda uno slot.
Operazione/Utente: un utente effettua una o più operazioni, un'operazione è effettuata da un utente.

Modello logico



Osservazioni

- Nella tabella Slot il campo Stato può assumere valore L (*libero*, la bici non è disponibile), O (*occupato*, la bici è disponibile).
- Tale stato è aggiornato quando viene effettuata un'operazione. A fronte di un noleggio viene posto a L, a fronte di un reso viene posto a O. Si suppone che il servizio sia attivo fino alle ore 2.00. Dalle ore 2.00 alle ore 6.00 degli addetti del Comune riorganizzeranno le biciclette rifornendo le stazioni in tutti i loro slot. Ogni mattina alle ore 6.00 tutti gli slot saranno in stato O.
- La chiave primaria della tabella Slot è una chiave composta da IdSlot (un numero compreso tra 1 e 5) e IdStazione (che è chiave esterna).
- La tabella Slot è popolata inizialmente con 5 righe per ogni stazione, inizializzata con stato='L'.
- L'attributo "InvioReport" della tabella Utenti indica la frequenza scelta dall'utente per invio report (vedere seconda parte, questito I). Può assumere i seguenti valori:
  A=Annuale, M=Mensile, S=Settimanale, T=Trimestrale

- Non è stata definita l'entità bicicletta perché oltre all'id non ci sono altri attributi utili al problema.
- Quando è effettuato un noleggio, è inserita una riga nella tabella operazioni con IdStazione, Ora, Data, IdUtente, IdBicicletta, TipoOperazione ='N', NumOperazione progressivo. È anche subito inserita la riga per la restituzione con uguale numero di operazione, TipoOperazione ="R", data='0000-00-00', ora ='00:00:00', IdBicicletta, IdUtente (gli stessi dell'operazione N), IdStazione e IdsSlot *null*. Data, Ora, IdStazione, IdSlot saranno valorizzati al momento della restituzione. Per ogni N, quindi, c'è sempre una corrispondente riga R.
- Si assume che un utente possa noleggiare una bicicletta alla volta.

Punto 3

Dopo aver progettato le pagine web secondo le indicazioni ai punti a) e b), occorre codificarne una con i linguaggi ritenuti più idonei.
Di seguito forniamo il codice essenziale per la realizzazione delle pagine web. Potrebbe essere correlato di apposita interfaccia utente e layout adeguato.

A partire da una mappa delle stazioni, verificare se una certa stazione ha biciclette disponibili per il noleggio.

QUERY SQL Conto gli slot occupati di una stazione data.

```
select count(*) as liberi from slot where idstazione = $idstazione and
stato = 'O'
<!DOCTYPE html>
<html>
<head>
<title> bici disponibili </title>
</head>
<body>

<?php
//verificare se una certa stazione ha biciclette disponibili per il no-
leggio;
//assegnare i valori in base al progetto
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "noleggiobici";

// Crea connessione al database
$conn = new mysqli($servername, $username, $password, $dbname);

// controlla connessione
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
// idstazione può essere scelta dall'utente tramite mappa
$idstazione=$_GET ['idstazione'];

$stringa= "select count(*) as liberi from slot where idstazione = $idsta-
zione and stato = 'O'";
}

$result = $conn->query($stringa);
```

```
if ($result->num _ rows > 0) {
      $riga = $result->fetch _ assoc();
      echo "BICICLETTE DISPONIBILI ALLA STAZIONE " . $idstazione. " : "
.$riga["liberi"].  "<p>";

} else {
    echo "0 results";
}
$conn->close();
?>
</body>
</html>
```

Consentire al gestore del sistema di visualizzare le bici attualmente in uso, da quali utenti e presso quale stazione sono state prelevate.

QUERY SQL

```
select IdBicicletta, IdStazione, IdUtente
from operazioni o,   (select NumOperazione as no
                     from operazioni
                     where TipoOperazione = 'R' and data = '0000-00-00') as t1
where o.numoperazione=no and tipooperazione ='N';
<!DOCTYPE html>
<html>
<head>
<title> letturadati </title>
</head>
<body>

<?php
//consentire al gestore del sistema di visualizzare le bici attualmente in
uso, da quali utenti e presso quale stazione sono state prelevate.
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "noleggiobici";

// Crea connessione al database
$conn = new mysqli($servername, $username, $password, $dbname);

// controlla connessione
if ($conn->connect _ error) {
    die("Connection failed: " . $conn->connect _ error);
}

$stringa= "select IdBicicletta, IdStazione, IdUtente from operazioni o,";
$stringa=$stringa . " (select NumOperazione as no from operazioni where
TipoOperazione = 'R' and data = '0000-00-00') as t1 ";
$stringa=$stringa . " where o.numoperazione=no and tipooperazione ='N' ";
$result = $conn->query($stringa);
```

```
if ($result->num _ rows > 0) {
      $riga = $result->fetch _ assoc();
      //echo "IdBicicletta : " .$riga["IdBicicletta"].  "<p>";
      echo "<table border = 1>";
      echo "<tr> <th> bicicletta </th> <th> stazione </th> <th> utente </
th></tr>";
  echo "<tr> <td>". $riga['IdBicicletta']." </td> <td>". $riga['IdStazione']."
</td> <td>". $riga['IdUtente']." </td> </tr>";
    while($riga = $result->fetch _ assoc()) {
      echo"<tr><td>". $riga['IdBicicletta']."</td><td>". $riga['IdStazione']."
</td> <td>". $riga['IdUtente']." </td> </tr>";
    }
      echo "</table>";
} else {
    echo "0 results";
}
$conn->close();

?>
</body>
</html>
```

Parte seconda – Risposte ai quesiti

Quesito I *In relazione al tema proposto, si integri il progetto con le pagine che consentono la produzione di un report contenente le bici noleggiate da un utente, le stazioni in cui sono state prelevate e restituite, la durata del noleggio e i relativi costi. Si discuta la problematica riguardante l'invio periodico e automatico del suddetto report sulla base di una temporizzazione impostata dall'utente nel suo profilo, e si proponga una soluzione motivandola adeguatamente.*

Discussione
In generale la gestione degli utenti (clienti) può essere fatta utilizzando un CRM e impostando l'invio del report dell'uso sel servizio in base a quanto scelto dall'utente.
L'invio può quindi essere effettuato automaticamente dal sistema via mail. Il CRM può raccogliere dati per poi indagare in merito alle abitudini degli utenti al fine di migliorare il servizio (**DataMining**, **BigData**). I **dati analizzati** possono essere dei clienti, ma anche provenienti dagli oggetti (biciclette, slot)
Di seguito il codice SQL per ottenere i dati per il report per un determinato cliente.

- Creo la tabella Noleggi con tutti i noleggi dell'utente numero 1.

```
Select NumOperazione, IdStazione, Data, Ora as Ora1, IdBicicletta INTO
Noleggi
From Operazioni
Where TipoOperazione='N'  and IdUtente=1
```

- Creo la tabella Resi con tutti i resi dell'utente numero 1 (data e bicicletta sono le stesse della corrispondente riga Noleggi).

```
Select NumOperazione, IdStazione,  Ora as Ora2,  INTO Resi
From Operazioni
Where TipoOperazione='R'  and IdUtente=1
```

- Creo report per utente 1 con IdBicicletta, data, durata del noleggio, costo. Si assume che il costo è di 0,50 euro al minuto.

```
Select IdBicicletta, Data, Ora1, Ora2, timediff (Ora2,Ora1) as Durata,
Minute(Timediff(Ora2,Ora1)) * 0,50
From Noleggio,Resi
Where Noleggi.NumOperazione=Resi.NumOperazione
```

Quesito II *In relazione al tema proposto nella prima parte, si sviluppino in linguaggio SQL le query che consentono di soddisfare le seguenti richieste: a) dato il codice di una bicicletta elencare gli utenti che l'hanno utilizzata nel mese corrente; b) mostrare la stazione presso la quale è stato effettuato il maggior numero di noleggi in un dato periodo.*

a) Dato il codice di una bicicletta, elencare gli utenti che l'hanno utilizzata nel mese corrente.

```
Select distinct IdUtente
From Operazioni
Where Month(Data) = Month (Now())
```

b) Mostrare la stazione presso la quale è stato effettuato il maggior numero di noleggi in un dato periodo.

```
select idstazione,max(tot)
from
          (select idstazione, count(*) as tot
            from operazioni
            where tipooperazione='N'
            group by idstazione) a
```

Quesito III *Considerata la relazione QUADRO (Cod_Quadro, Cod_Museo, Titolo_Quadro, Nome_Museo, Citta_Museo, Prezzo, DataInizioEsposizione, DataFineEsposizione) si verifichino le proprietà di normalizzazione e si proponga, eventualmente, uno schema equivalente che rispetti la terza forma normale, motivando le scelte effettuate.*

La relazione non è in 3FN, perché i dati del Museo e dell'esposizione non dipendono dal Codice Museo. Questo fatto implica un problema di ridondanza.

Normalizzo fino alla 3FN:

```
Quadri (CodQuadro, TitoloQuadro)
Museo (CodMuseo, NomeMuseo, CodCity)
City (CodCity, NomeCity)
Esposizione (CodMuseo, CodQuadro, DataInizioEsposizione, DataFineEsposizione)
```

Quesito IV *Alla luce delle problematiche relative alla sicurezza e integrità delle informazioni archiviate nei sistemi informatici e della loro riservatezza, si discutano vantaggi e svantaggi delle principali tecniche per l'autenticazione degli utenti di un sistema informatico di rete, discutendo sistemi e protocolli utilizzati in tale contesto.*

Il controllo logico degli accessi impone soluzioni hardware e software per impedire accessi non autorizzati a risorse, sistemi e reti. Queste soluzioni si basano su tecniche e protocolli che garantiscono l'identificazione, l'autenticazione e l'autorizzazione degli utenti.

L'**autenticazione** è la capacità di verificare con certezza l'identità di un utente e di applicare le regole che lo autorizzano a usufruire di una risorsa. Un identificatore univoco permette l'associazione tra un soggetto e un'attività o una risorsa. Il nome dell'utente è il mezzo più comune utilizzato per identificarlo. Può consistere in un PIN o in un codice alfanumerico, un indirizzo e-mail, una smart card personale, l'impronta digitale, il riconoscimento del proprio volto o della voce. Il vantaggio è un sistema semplice da implementare e comodo da utilizzare, anche se debole. Per ridurre il rischio di accessi non consentiti e frodi è spesso utilizzata una "autenticazione forte" che prevede la combinazione di almeno due fattori indipendenti tra loro come, per esempio, il codice PIN (qualcosa che solo l'utente conosce), il suo smartphone (qualcosa che solo l'utente possiede) e l'impronta digitale (qualcosa che caratterizza l'utente). In ogni caso le tecnologie di autenticazione non sono infallibili e sono soggette a diversi tipi di attacchi. Eccone alcuni esempi:

- si può risalire alla password con un attacco di forza bruta o tramite un dizionario;
- si può entrare in possesso di chiavi hardware e duplicarle;
- nel caso di sistemi biometrici, i più difficili da forzare, si può ricorrere a tecniche per replicare l'identità degli utenti;
- l'attaccante può penetrare nei sistemi di controllo e iniettare processi trojan che possano estrarre informazioni e credenziali e far accedere al sistema da remoto.

La protezione dei dati durante la loro trasmissione avviene applicando le tecniche crittografiche a chiave asimmetrica e certificati digitali con l'utilizzo di protocolli che, come SSL, garantiscono gli standard di sicurezza e si basano sul fatto che il tempo necessario a decifrare i pacchetti catturati potrebbe essere molto elevato e non conveniente.

Di seguito proponiamo una simulazione che può essere svolta in preparazione all'esame. Lo svolgimento è disponibile online.

PROPOSTA DI SIMULAZIONE

Indirizzo: INFORMATICA E TELECOMUNICAZIONI – Articolazione: INFORMATICA
Tema di: SISTEMI E RETI

Il candidato svolga la prima parte della prova e risponda a due tra i quesiti proposti nella seconda parte. Il candidato potrà eventualmente avvalersi delle conoscenze e competenze maturate attraverso esperienze di alternanza scuola-lavoro, stage o formazione in azienda.

Parte prima

Coltivazioni indoor: un mondo in cui la natura e la tecnologia si fondono

Negli ultimi anni le metodologie di coltivazione indoor hanno rivoluzionato il settore agricolo, migliorando la qualità delle piante e riducendo l'impatto ambientale. I diversi sistemi di coltivazione (idroponica, aeroponica e acquaponica) hanno dato vita a numerose vertical farm. In particolare, la coltura idroponica non richiede l'uso del terreno; le radici crescono e si sviluppano in acqua, alla quale si aggiungono sostanze nutritive per garantire lo sviluppo completo delle piante.
La società IdraFarm, situata alle porte di una grande città italiana, è un centro di ricerca dedicato alla coltivazione idroponica. All'interno della serra sperimentale, grande quanto un campo di calcio, vengono testate le condizioni ambientali ottimali per la crescita di ortaggi ed erbe aromatiche. I dati raccolti dai test di coltura forniscono preziose informazioni per ottimizzare il processo di crescita delle piante.
La struttura del centro di ricerca comprende un corpo centrale con la serra sperimentale e una palazzina adiacente suddivisa in due aree. Una di queste è dedicata agli uffici per il controllo dei sensori e la sorveglianza dell'intera struttura, mentre l'altra è riservata al pubblico, ospitando incontri e convegni. Il centro di ricerca è collegato alla sede centrale presente in città.

All'interno della serra, sono installati sensori per il rilevamento dei dati ambientali, tra cui intensità luminosa, umidità, temperatura e pH dell'acqua. Questi sensori sono collegati a un sistema microcontroller che fa parte della rete dedicata al monitoraggio. Il microcontrollore elabora i dati e li invia periodicamente (ogni 5 minuti) alla sede centrale di IdraFarm, dove vengono analizzati per ottenere risultati scientifici significativi. La Sede Centrale di IdraFarm, oltre agli uffici di rappresentanza, ospita un'area di elaborazione con un server dedicato all'analisi dei dati. Qui, esperti e ricercatori lavorano per estrarre informazioni preziose dalle rilevazioni effettuate nella serra sperimentale.
IdraFarm fornisce inoltre, sul suo sito, una serie di servizi online a clienti esterni (aziende o privati), relativi a corsi, consulenza tecnica, eventi. Per usufruire di questi servizi, gli utenti devono registrarsi alla piattaforma web di IdraFarm e prenotare i servizi desiderati. Inoltre, è possibile accedere ai servizi anche tramite un'app scaricabile da uno store mobile.
Per lo svolgimento della prova è necessario tenere presente i seguenti vincoli.

- La rete che presiede alla sorveglianza della serra va tenuta separata da quella degli ospiti, al fine di evitare promiscuità.
- La sede centrale di IdraFarm è collegata con il centro di ricerca in modo sicuro. Gli accessi alla sede sono protetti da apparati di sicurezza per evitare intrusioni esterne. I dati sono soggetti a backup periodico e le linee di collegamento a Internet adottano tecniche di ridondanza.
- I servizi web e di posta elettronica aziendali sono delegati a server in cloud.

Il candidato, fatte le opportune ipotesi aggiuntive e tenendo presente i vincoli indicati:

Punto 1 schematizzi il progetto dell'infrastruttura informatica generale. Corredi il progetto specificando i dispositivi utilizzati, i mezzi fisici, i protocolli e gli standard;

Punto 2 proponga un'analisi delle reti coinvolte nel progetto, specificando quali sono i dispositivi coinvolti in ciascuna rete, quali misure di sicurezza sono utilizzate all'interno di ogni rete e come le reti sono collegate tra loro;

Punto 3 proponga una soluzione per la sicurezza perimetrale delle reti;

Punto 4 discuta il vantaggio di avere sistemi di ridondanza e backup;

Punto 5 confronti la soluzione di server in cloud rispetto alla DMZ;

Punto 6 elenchi i requisiti fondamentali di un sistema abilitato per il lavoro in smart working.

Parte seconda

Il candidato risponda a due quesiti a scelta tra quelli sotto riportati.

Quesito I *In relazione al tema proposto, si vuole permettere a un cliente di conoscere i corsi offerti e di iscriversi a un corso di suo interesse. Il candidato progetti lo schema concettuale e il modello logico della porzione di base di dati necessaria. Progetti poi le pagine web che consentono di ottenere le informazioni sui corsi: nome del corso, contenuto, durata, orario, giorni, modalità (in presenza oppure online) e numero massimo di iscritti, scrivendo in un linguaggio a scelta il codice di una parte significativa.*

Quesito II *IdraFarm offre ai suoi collaboratori la possibilità di lavorare da remoto. Il candidato discuta le problematiche relative allo smart working con particolare riferimento alle tecniche e ai protocolli di sicurezza da utilizzare per garantire un collegamento sicuro con la sede aziendale.*

Quesito III *In relazione al tema proposto, il candidato sviluppi con un linguaggio a scelta (o con una pseudocodifica) un frammento di codice per inviare al server i dati relativi alle grandezze fisiche rilevate dai sensori.*

Quesito IV *Il candidato dopo aver discusso sui benefici e rischi della tecnologia che cambierà le nostre vite, analizzi come l'elevata quantità di dati scambiati aumenti la possibilità di compromissione dei sistemi e della privacy con impatto significativo sia a livello economico sia sui diritti e sulla libertà degli individui.*



Svolgimento simulazione

Indice analitico

3DES (Triple DES) **162**
3GPP **293**
5G **293**

A

ACL (Access Control List) **206**
Estesa **206**
Standard **206**
Advanced Encryption Standard (AES) **279**
Adware **126**
AES (Advanced Encryption Standard) **162**
affiliati RaaS **141**
AfriNIC **45**
Authentication Header (AH) **246**
algoritmi
a chiave asimmetrica **161**
algoritmi a chiave simmetrica **161**
RSA **163**
a trasposizione **160**
di Rijndael **162**
analisi post-incidente **134**
ANSI/TIA-942 **332**
Application **284**
Application Server **289**
applicazione multilayer **7**
AppSKey (Application Session Key) **289**
APS (Application Object) **287**
APT (Advanced Persistent Threats) **117, 143**
archiviazione **320**
archiviazione a blocchi **323**
ARIN **45**
armamento (Weaponization) **128**
attacco informatico **116**
attacco KRACK **295**
autenticazione **166**
a due fattori **168**
a tre fattori **168**
debole **168**
passwordless **169**
forte **168**
Autenticazione, Autorizzazione e Contabilità (AAA) **201**
Authoritative Name Server **49**
autorizzazione **166**
availability (disponibilità) **116**
Azioni sull'obiettivo (Actions on Objectives) **129**

B

backdoor **72, 139, 144**
backup **336**
bastion host **216**
beamforming **293**
black hat **127**
Bluetooth **284**
body **55**
Botnet **118**
Broad network access **349**
Broker **291**
business continuity **332, 333**

C

cache **49**
Calcolo **320**
carico utile (payload) **123**
ccTLD **44**
CERT **134**
CERT-AGID **136**
Certification Authority (CA) **175**
CERT-PA **136**
chain of trust **71**
chiave di sessione **163**
privata **162**
pubblica **162**
Incident Response Life Cycle (ciclo di vita della risposta) **132**
cifrari monoalfabetici **179**
cifratura
a blocco **161**
a flusso **161**
del messaggio **164**
client **6**
di posta **54**
DNS **47**
Client/Server **8**
clonazione **336**
Cloud **373**
Cloud Computing **348**
cluster di server **334**
codifica Code 64 **146**
Comando e Controllo (Command and Control) **129**
Common Vulnerability Scoring System (CVSS) **121**
Common Weakness Enumeration (CWE) **121**
Common Vulnerabilities and Exposures (CVE) **121**
Community Cloud **355**
Computer Emergency Response Team (CERT) **135**
Computer Security Incident Response Team (CSIRT) **136**
comunicazione asincrona **53**
confidentiality (riservatezza) **116, 160**
container **352**
Container as a Service (CaaS) **351**
contenimento (Containment) **134**
continuità del servizio **72, 332**
controller **284**
cookie **18, 19**
crittografia **160, 180**
asimmetrica **162**
quantistica **184**
CSF 2.0 **132**
CVE **121, 123**
CVE-ID **121**
cyber **115**
Cyber Kill Chain **128**
cybersecurity **115**
cyber warfare **138**

D

dark web **144**
data center **318**
fisico **329**
in cloud off-premise **331**
in colocation **330**
on-premise **330**
tipi di **330**
virtuale **329**
Data Encryption Standard (DES) **162**
DDoS (Distributed Denial of Service) **118, 124, 138**
debolezza (weakness) **119**
decifratura del messaggio **164**
DELETE **11, 23**
DeMilitarized Zone (DMZ) **218**
desktop virtuale **328**
digest **177**
DIKW (Data, Information, Knowledge, Wisdom) **115**
disaster recovery **333, 336**
distribuzione (delivery) **129**
DNS **42, 43, 56**
cache poisoning **71**
dinamico **52**
spoofing **71**
zone file **47**
Docker **353**
Domain Name System **42**
dominio **44, 45**
di primo livello **44, 45**
nomi di **43**
downtime **335**

E

ecosistema **372**
edge computing **379**
e-mail (posta elettronica) **53**
Emotet **124, 142**
Encapsulating Security Payload (ESP) **246**
envelope **55**
eradicazione (eradication) **134**
EternalBlue e DoublePulsar (CVE-2017-0145) **139**
Extranet **238**

F

Fault Tolerance **333**
Fibre Channel over Ethernet **324**
Fireball **126**
firewall **200, 202**
Firma Digitale **172**
firma elettronica **172**
fog computing **379**
FTP (File Transfer Protocol) **65**
modalità attiva **66**
modalità passiva **66**
Functions as a Service (FaaS) **351**
funzione sigmoide **380**
funzioni di hash **177**

G

gateway **289, 373**
Gateway LoRaWAN **290**
gerarchia di distributori **47**
gerarchia di dominio **43**
GET, metodo **11, 16, 18, 23**
governo (govern) **132**
grey hat **128**
gTLD **44**

H

hacker **127**
state sponsored **128**
hacking, tecniche di **168**
hacktivist **128**
header **55**
high availability **333**
honeypot **130**
Host **284**
HTTP
headers **13**
metodi **9, 11**
protocollo **8**
request **9**
response **10**
stateless **18**
HTTPS **248, 252**
Hybrid Cloud **355**
hypervisor **326**

I

IANA **45**
ICANN **44, 45, 47**
identificazione (Identify) **133, 166**
IDNA **44**
Identity Provider (IdP) **170**
IEEE 802.15.4 **285**
integrità (Integrity) **116**
IKE (Internet Key Exchange) **248**
ILOVEYOU (virus) **124**
IMAP **54, 56**
incidente di sicurezza **119**
Incident Response Life Cycle **132**
indicatori di compromissione **134**
indirizzi IP dinamici **51**
Infrastructure as a Service (IaaS) **350**
installazione (Installation) **129**
Intelligenza Artificiale **136, 221, 372, 379**
Intranet **238**
Intrusion Prevention System (IPS) **200, 204**
IoT (Internet of Things) **372**
sicurezza dei sistemi **377**
IPsec **238, 241, 244, 245**
ISAKMP (Internet Security Association and Key Management Protocol) **240, 248**

J

JavaScript **147**

K

Kerberos **244**
Keylogger **126**
kill chain **128**
Kubernetes **353**

L

LACNIC **45**
Local Name Server **48**
LockBit **124**
LockBit 2.0 **141**
LockBitRansomware.exe **141**
LoRa (Long Range) **289**
LoRaWAN (Long Range Wide Area Network) **289**

M

macchina virtuale **326**
mail box **56**
Mail Transfer Agent **54**
Mail User Agent **54**
malware **116, 121**
manifest **353**
Man in the Middle **118**
MD5 **177**
Measured Service **349**
Message Integrity Code (MIC) **285**
Messaggi di testamento (Will) **292**
MFA (Multi-Factor Authentication) **168**
Microservizi **352**
Migrazione **335**
MIME **57**
minacce persistenti avanzate (APT) **128**
minaccia (threat) **116**
Mirai **121, 124**
MITRE ATT&CK **145**
Morris Worm **124**
MPLS **237, 243**
MQTT (Message Queuing Telemetry Transport) **290**
MTA **54**
MUA **54**
multi tenancy **349**

N

NAS (Network Access Server) **296, 323, 327**
National Institute of Standards and Technology (NIST) **132**
National Security Agency (NSA) **140**
netiquette **74**
Network Server **289**
Network slicing **293**
NGFW (Next Generation Firewall) **204**
NIC **46**
NIST **132, 348**
NIST SP 800-61 Revisione 3 **133**
NS dinamico **51**
NwkSKey (Network Session Key) **289**

O

on-demand self-service **349**
OpenVPN **242, 244, 322**
OWASP (Open Worldwide Application Security Project) **134**

P

packet filtering – stateless, firewall **203**
pagina web **14**
pagina web statica **14**
Passwordless Authentication **169**
PATCH **11**
pattern malevoli **153**
Pegasus **124**
persistenza dei messaggi **292**
PGP (Pretty Good Privacy) **244, 256**
phishing **145**
  e-mail **124**
Python, script **146**
Platform as a Service (PaaS) **349**
PMF (Protected Management Frames) **282**
POP **42**
POP3 **54**
port-forwarding **219**
POST **11, 16, 23**
Preparazione **132**
principianti (script kiddie) **128**
Private Cloud **355**
prompt **380**
protezione delle e-mail e delle applicazioni Web **201**
protezione (Protect) **133**
protocolli
  IMAP **64**
  MPLS **242**
  POP3 **62, 84, 89**
  RADIUS **295**
  RTCP **69**
  RTP **69**
  SMTP **59**
provider di identità **170**
proxy server (o forward proxy) **214**
public cloud **355**
publisher **290**
PUT, metodo **11, 23**

Q

Qualità del servizio (QoS) **292**
QUERY_STRING **17**

R

RAID **323, 334**
ransomware **114, 124, 139**
Ransomware-as-a-Service (RaaS) **141**
rapid elasticity **349**
record delle risorse **49**
recupero (Recovery) **134**
Regional Internet Registry **45**
Resource pooling **349**
rete aperta **279**
reverse proxy **217**
ricognizione (reconnaissance) **128**
rilevamento (detect) **133**
RIPE **45**
riservatezza **160**
risposta (respond) **134**
Rootkit **124**
Root Name Server **48**
root server **45, 50**
router **290**
RTP **68**

S

SAML, protocollo **171**
SAN **323, 327**
SA (Security Association) **247**
Secure Access Service Edge **239**
Secure VPN **236**
Security Association Database (SAD) **247**
server **6, 320**
  DNS **47**
  HTTP **6**
  MX **56**
  proxy pubblico **216, 217**
  session **18, 19**
serverless **319, 320**
Server Message Block versione 1 (SMBv1) **139**
sfruttamento (exploitation) **129**
SHA **177**
SIEM (Security Information and Event Management) **129, 133, 134, 135**
Simultaneous Authentication of Equals (SAE) **279**
Single Point of Failure Dependency **329**
small cells **293**
Smart City **376**
SMTP **54, 56**
  comandi **59**
snapshot **335**
SOAR (Security Orchestration, Automation, and Response) **136**
SOC **134**
social engineering **116**
social networking analysis **143**
SOC (Security Operations Center) **135**
Software as a Service (SaaS) **349**
SPAM **54**
SPD (Security Policy Database) **248**
spear phishing **143**
SPI **247**
Spoofing IP **118**
SP (Security Policy) **248**
Spyware **124**
SRTP **68**
Stateful Packet Inspection (Circuit-Level Gateway), firewall **204**
steganografia **180**
sTLD **44**
storage **323**
Stuxnet **114, 124**
submission **53**
subscriber **290**
SYN Flood **118**

T

TCP/IP, stack **118**
Teardrop **118**
tecnologia NFC (Near Field Communication, Comunicazione di prossimità) **283**
template **336**
thin client **328**
TLD **44, 45**
TLS **244**
Topic **291**
Transport Layer Security **248**
Transport Mode **245**
triage ospedaliero **137**
Trojan / Backdoor **124**
Tunnel Mode **245**
tunnel virtuali **236**

U

URI **8, 10**
URL **43**
userid **167**
uTLD **44**
UTM (Unified Threat Management, Gestione unificata delle minacce) **205**

V

VDI **328**
vettore **123**
videoconferenza **68**
virtual data center manager **327**
virtualizzazione **324, 329, 329**
  dei server **327**
  della rete **327**
  delle applicazioni **328**
  dello storage **327**
Virtual Machine **326**
Virtual Machine Monitor **326**
Virus **124**
  biologico **126**
  informatico **126**
Visual Basic for Applications (VBA) **147**
VPN **234**
  personali **236, 241**
  Remote Access **236, 239**
  Site-to-Site **235, 238**
  SSL **241**
  Trusted **236, 242**
vulnerabilità (vulnerability) **119, 120**
  intrinseche **120**
  tecnologiche **121**
  umane **121**

W

WannaCry **114, 123, 124, 139**
watering hole **128**
Web **13**
Web Application Firewall (WAF) **201**
Webmail **54**
WEP **279**
white hat **127**
WHOIS **46**
Wi-Fi **278**
WiMAX (Worldwide Interoperability for Microwave Access) **288**
Worm **124**
WPA **279**
WPA2
  modalità Enterprise **279, 280**
  modalità Personal **279**
  modalità PSK **280**
  Wi-Fi Protected Access II - IEEE 802.11i **279**
WPA3 **279, 281**

Z

Zenmap **148**
zero day **144**
zero downtime **333**
ZigBee **285**
ZigBee Device Object (ZDO) **287**