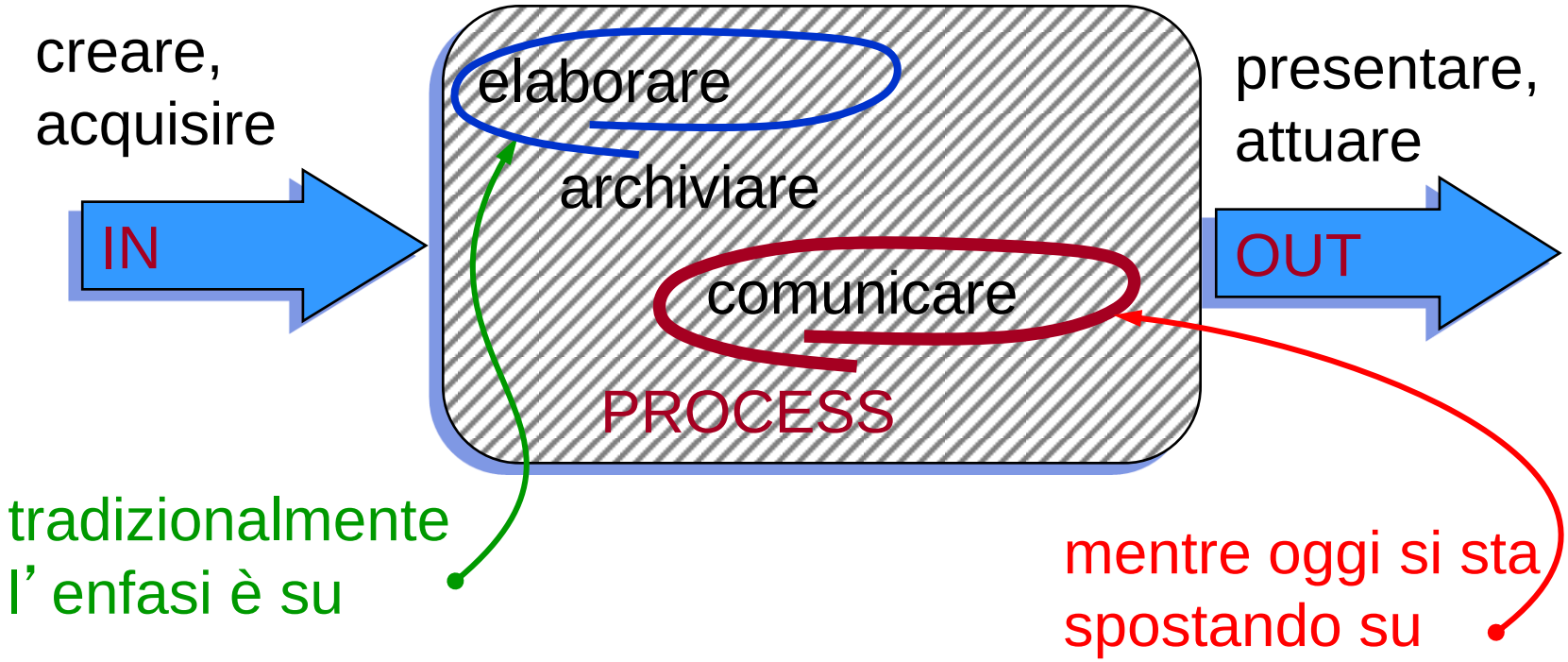
Comunicazione di Rete

Reti di comunicazione



Perche la rete?

- Condividere risorse
  - utilizzo razionale di risorse HW (magari costose)
  - Condivisione di software (programmi e dati da parte di utenti)
  - affidabilità e disponibilità delle risorse

- Comunicare tra utenti
  - scambio informazioni
  - collaborazione a distanza

Cos’è una rete?

- Una rete informatica è un insieme di dispositivi collegati tra loro tramite sistemi di interconnessione (cablaggio o wireless).
  - Consente di comunicare e condividere informazioni e risorse.
  - Sono classificate a seconda delle dimensioni.
  - È possibile ospitarle in una sede singola oppure dislocarle in vaste aree.

Rete di computer

- Ogni elaboratore collegato a una rete viene detto ***nodo*** o host.
- I dati trasmessi vengono raggruppati in ***pacchetti*** per essere trasmessi e ricevuti da un host all'altro.
- Il pacchetto (frame) rappresenta una quantità di dati di dimensione standardizzata, che può variare secondo il ***protocollo di comunicazione*** utilizzato.

I protocolli di comunicazione

- Per comunicare i calcolatori debbono seguire delle le ***regole***: i protocolli di comunicazione.
- I protocolli di comunicazione specificano:
  - i formati dei dati
  - la struttura dei pacchetti
  - la velocità di trasmissione
  - …
- Definire tutte queste proprietà tramite un unico protocollo è praticamente impossibile, per questo si definisce ***un insieme di protocolli:***
  - ogni protocollo gestisce univocamente una componente ben definita della comunicazione
  - ogni protocollo condivide con gli altri protocolli i dati di cui essi necessitano

Alcuni protocolli applicativi

- HTTP
  - Per navigare sul web
- HTTPS
  - Per acquistare su web in modo sicuro
- SMTP
  - Per spedire email
- POP
  - Per ricevere email e scaricarle sul proprio PC
    - Una volta scaricate sul PC le email non sono leggibili con altri dispositivi ma non serve più essere collegati a internet per consultarle
- IMAP
  - Per ricevere email senza scaricarle sul proprio PC
    - La mail può essere letta da qualunque dispositivo ma bisogna essere collegati a internet

TIPOLOGIE DI RETI

Architetture di rete: caratteristiche

- I mezzi di trasmissione sono costituiti da:
  - appositi cablaggi;
  - rete telefonica dati;
  - satelliti;
  - sistemi di comunicazione wireless.

Componenti di una rete

- Componenti di una rete sono:
  - ***nodi***: un nodo è un qualsiasi dispositivo hardware del sistema, in grado di comunicare con gli altri dispositivi che fanno parte della rete
  - ***collegamenti*** (links) tra i nodi

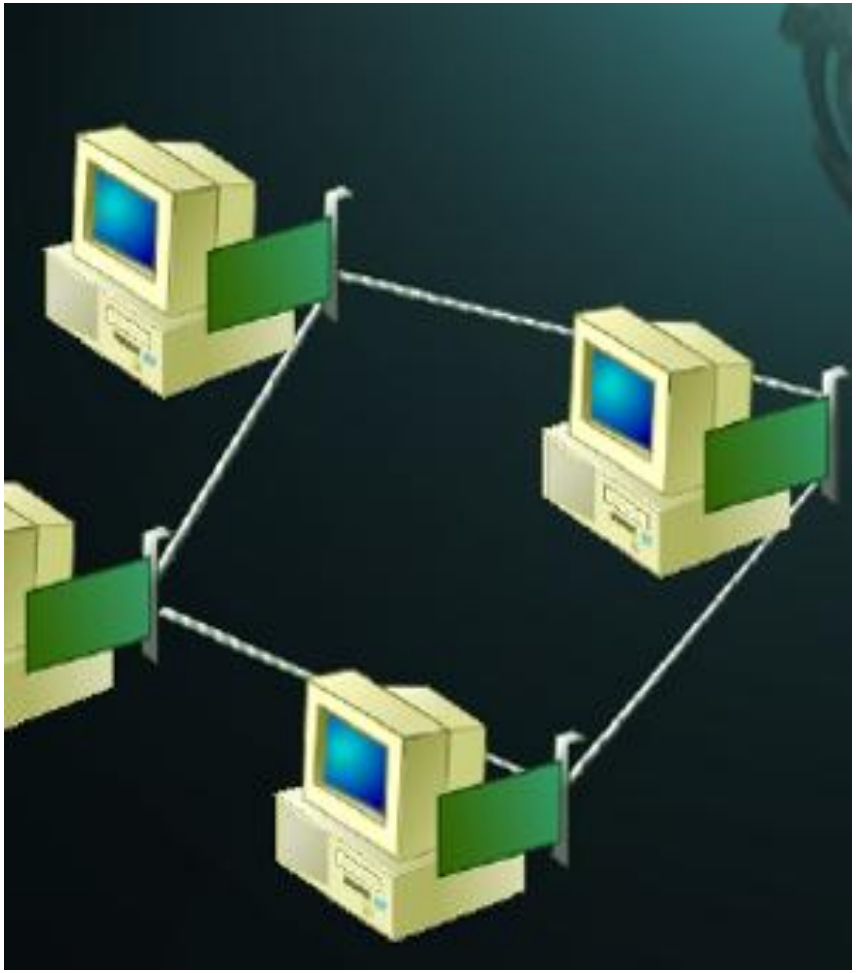
Tipologie di rete

- I tipi di rete che possiamo utilizzare coprono spazi diversi:
  - possiamo utilizzare una semplice rete, collegando un computer a un portatile;
  - collegarci via Internet per comunicare senza limiti di spazio.

Tassonomia delle reti

- Reti locali (Local Area Network, LAN)
  - di limitata estensione
  - collegano dispositivi collocati nello stesso edificio o in edifici adiacenti.
- Reti metropolitane (Metropolitan Area Network, MAN)
  - collegano di dispositivi collocati nella stessa area urbana.
- Reti geografiche (Wide Area Network, WAN)
  - collegano di dispositivi diffusi in un' ampia area geografica (nazione, continente, …);
- "Reti di reti" (Internetwork),
  - collegamento più reti differenti (in termini sia hardware che software) mediante opportuni elementi di interfaccia, che si possono estendere su tutto il pianeta (e.g. Internet).

LAN: Local Area Network



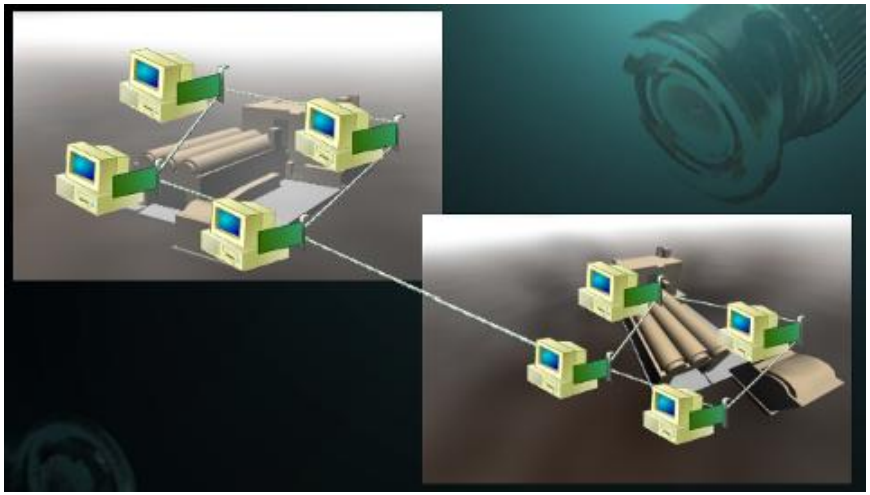
- Identifica una rete costituita da computer collegati tra loro (comprese le interconnessioni e le periferiche condivise) all'interno di un ***ambito fisico delimitato*** (ad esempio in una stanza o in un edificio, o anche in più edifici vicini tra di loro)

LAN: Local Area Network

- Sono reti private implementate per la condivisione di risorse.
- Le risorse possono essere:
  - elaboratori;
  - stampanti;
  - dati.

MAN: Metropolitan area network

- La MAN è una rete che si estende in un ***area metropolitana***; essa può comprendere diverse LAN al suo interno.
- La connessione di tutti gli elaboratori di una Università distribuita in diversi plessi è una rete MAN.

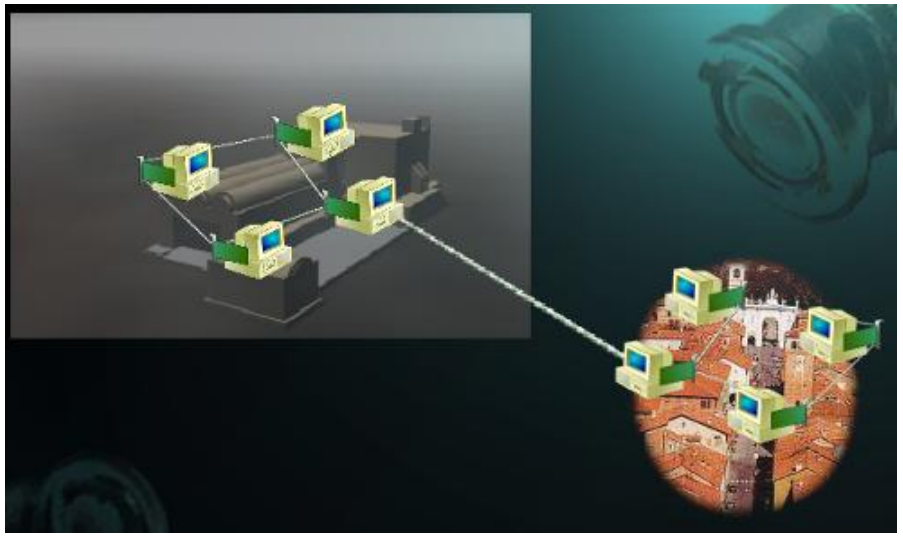


MAN: Metropolitan area network

- Una rete metropolitana è una versione ampliata di rete.
- Può coprire un gruppo di uffici, aziende, città.
- È pubblica ma anche privata.
- La comunicazione avviene su linee dedicate (analogico/digitale).

WAN: Wide Area Network

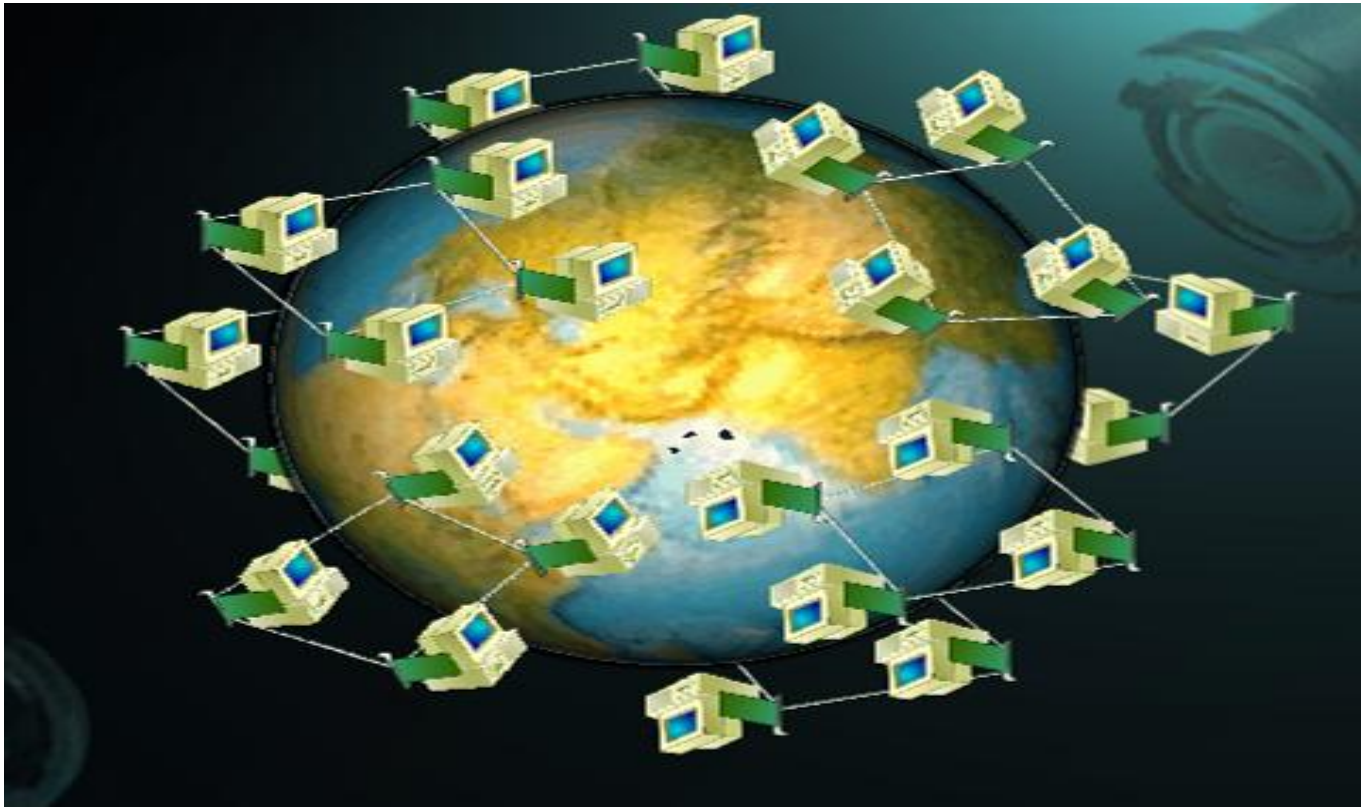
- Le WAN (Wide area network) sono usate per connettere ***più reti locali*** in modo che un utente di una rete possa comunicare con utenti di altra rete.
- Molte WAN sono costruite per una particolare organizzazione e sono private.



WAN: Wide Area Network

- Una WAN è una rete di reti.
- Esempi di WAN:
  - la rete GARR, che collega tutte le reti delle Università italiane;
  - la rete ARPANET rete americana per collegare centri di ricerca.

Internet è una WAN



Scala delle reti

- Un criterio per classificare le reti è legato alla loro scala in base alla distanza tra nodi.

10 m	stanza	Rete locale LAN
100 m	edificio	LAN
1 km	università	LAN
10 km	città	Rete metropolitana MAN
100 km	nazione	Rete geografica WAN
1000 km	continente	Internet
10000 km	pianeta	Internet

INFRASTRUTTURA DI RETE

Cavi Ethernet e schede di rete

- I cavi ethernet e le schede di rete sono componenti indispensabili per il corretto funzionamento di una rete informatica.

Modem

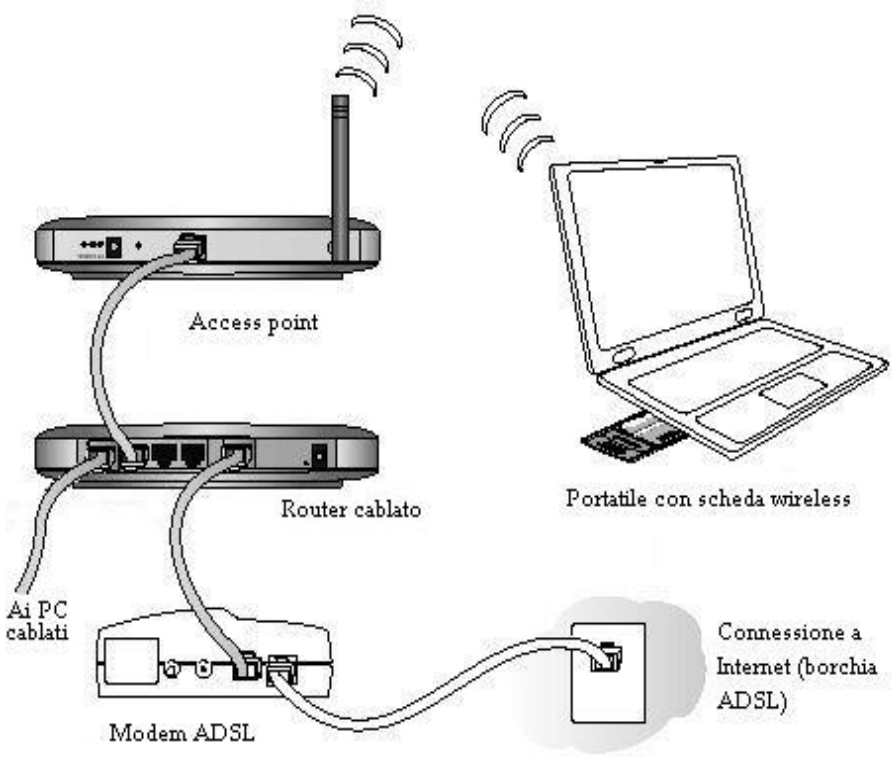
- Il modem deve convertire i dati digitali in segnali analogici e viceversa su linea telefonica.
- È indispensabile nelle connessioni Internet.

Router

- Connette due (o più) reti
- È in grado di trasferire pacchetti di un determinato tipo di protocollo di rete indipendentemente dal tipo di reti fisiche effettivamente connesse.

Devices per una rete wireless

- Nelle reti casalinghe, spesso, Modem, Router e Access Point sono contenuti in un unico apparato.



Scheda di rete wireless

- Funzionalità
  - Modulazione: traduzione del segnale dalla banda base a una forma analoga opportuna.
  - Amplificazione: aumento della potenza del segnale.
  - Controllo degli errori.

Access Point

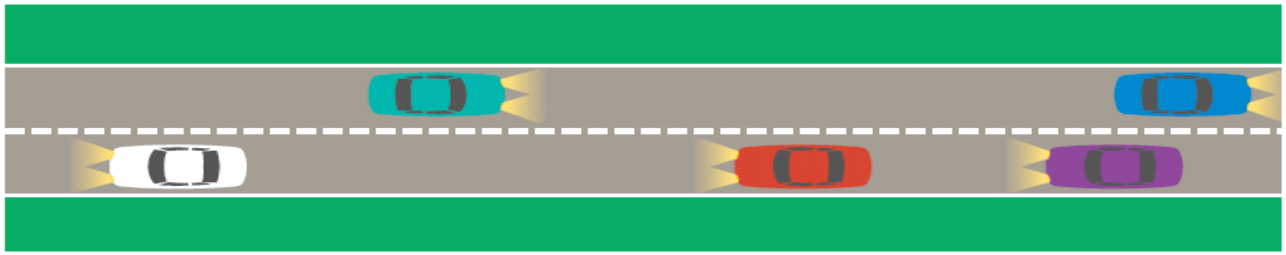
- È un dispositivo che permette all'utente mobile di collegarsi ad una rete wireless.
- L'access point, collegato fisicamente ad una rete cablata (oppure via radio ad un altro access point), riceve ed invia un segnale radio all'utente (per connessione).

PRESTAZIONE DELLA RETE

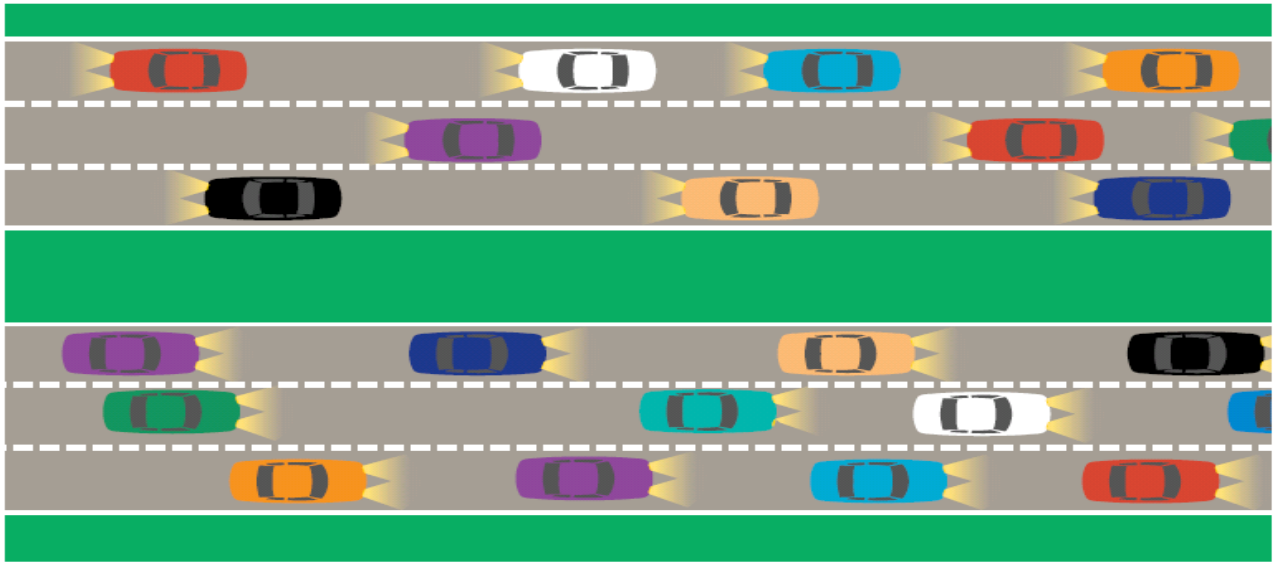
Prestazioni della rete

- La trasmissione avviene in base alla banda della rete (larghezza di banda- utilizzo di più canali)
- La velocità misurata in bit al secondo:
  - Kilobit/s (Kb/s)
  - Megabit/s (Mb/s)

La larghezza di banda



Una banda stretta è come una strada a due corsie



Una banda larga è come un'autostrada

La larghezza di banda

Perché la banda larga?

- Banda larga significa:
  - più servizi (TV, telefonia tradizionale, “on demand”, etc.) sulla stessa linea e senza cambiare il supporto fisico;
  - contenuti più “pesanti” (e interessanti).
- Ecco quanti dati si devono trasmettere per un video di qualità media:

Elemento	Quantità
Pixel dello schermo (640 × 480)	307 200
Bit per pixel	8
Totale bit dello schermo	2 457 600
Fotogrammi per secondo	30
Totale bit per secondo	73 728 000

Le cifre della trasmissione video

TIPOLOGIE DI COMUNICAZIONE

Comunicazioni fra individui

Nome utente | Nome dominio

dcurtin@interserve.com

Un indirizzo di posta elettronica

La posta elettronica (email) e l'instant messaging sono i principali mezzi di comunicazione individuale attraverso la rete.

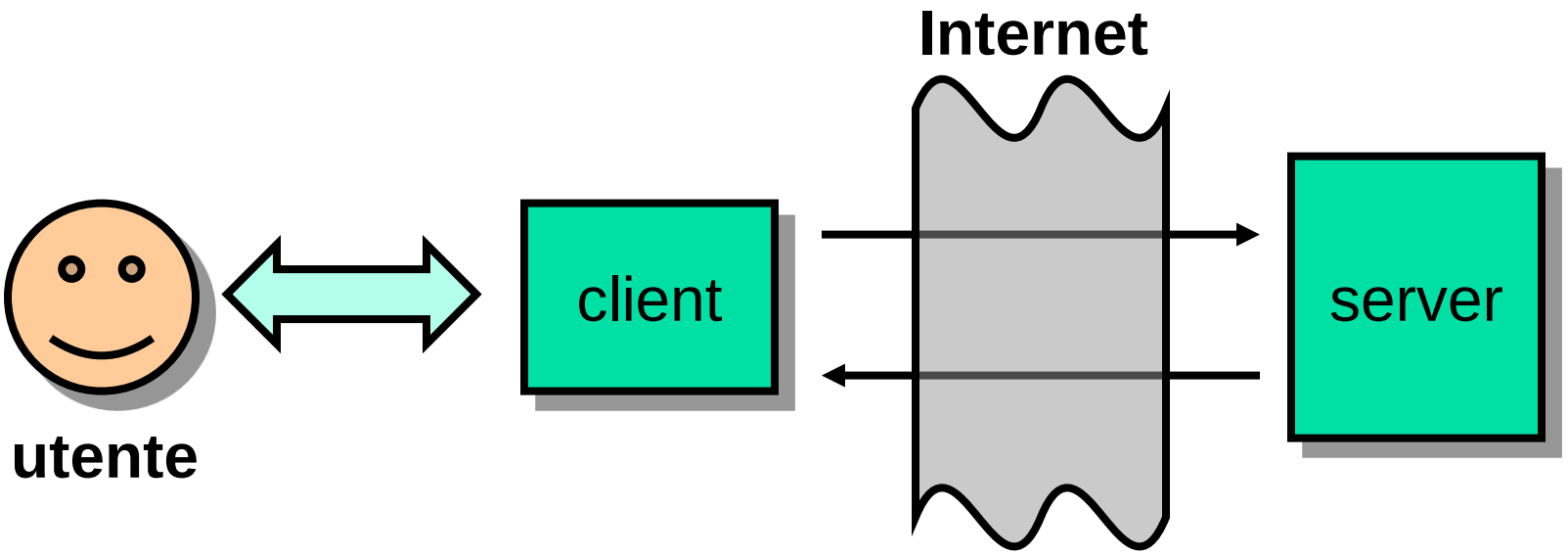
La tecnica detta store-and-forward permette alle email di raggiungere il destinatario con certezza e nel più breve tempo possibile.

La tecnica store-and-forward

Comunicazioni fra gruppi

- I newsgroup
  - Gli utenti affiggono in “bacheche elettroniche” dei messaggi/articoli che altri lettori possono commentare pubblicamente o privatamente. Le risposte sono gerarchicamente accodate in modo da poter ricostruire la discussione.
- Le mailing list
  - Notizie e interventi riguardo un argomento sono inviati per posta elettronica. Ci si iscrive e dimette dalle liste con un semplice messaggio.
- Internet Relay Chat
  - Le chat consentono di comunicare in tempo reale con gli altri utenti che abitano una particolare “stanza”.
- Giochi di rete
  - Dapprima testuali e ora graficamente elaborati, i giochi di rete permettono di divertirsi con utenti di qualunque parte del mondo.
- Videoconferenze
  - Una volta molto difficili da preparare, oggi un qualunque PC è sufficientemente attrezzato per far partecipare l'utente a una videoconferenza sfrutti tecnicamente a Internet.

Comunicazione client-server

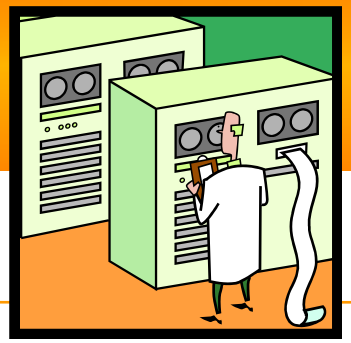


- L'utente comunica la sua richiesta al client
- Il client si collega al server e trasmette la richiesta
- Il server risponde al client
- Il client fornisce la risposta all'utente

Il client

- Si preoccupa di dialogare con l'utente
- Sfrutta tutte le possibilità fornite dal calcolatore su cui viene eseguito (audio, video, ...)
- Fornisce all'utente un'interfaccia intuitiva
- Elabora le richieste dell'utente e le risposte dei server
  - la comunicazione avviene secondo un formato standard (protocollo)

Il server

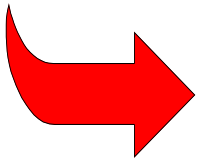


- Rende disponibili delle risorse
- Accetta richieste e risponde automaticamente
  - non bada alla provenienza della richiesta
  - il processo client può trovarsi in qualsiasi punto della rete
- Si può organizzare un insieme di server in modo che siano collegati tra loro
- Potrebbe essere eseguito dallo stesso calcolatore che esegue il processo client!

INTERNET E IL WORLD WIDE WEB

La storia di Internet

Inizi anni '60 - La ARPA (Min.Difesa USA) avvia un progetto che prevede la costruzione di una rete di computer.

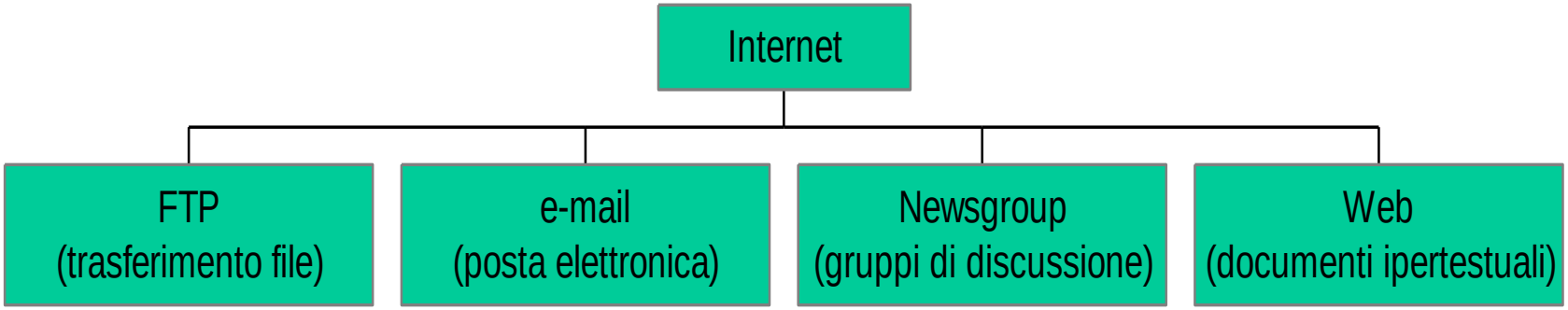


Novembre 1969: due computer di facoltà universitarie (UCLA e SRI) si collegano attraverso una rete BBN progenitrice dell'attuale Internet.

Oggi: né università né organi governativi gestiscono la rete, ma un'associazione volontaria, la

ISOC (*Internet Society*)

Internet e WWW
non sono la stessa cosa



i servizi di Internet, dal più remoto al più recente

Il World Wide Web

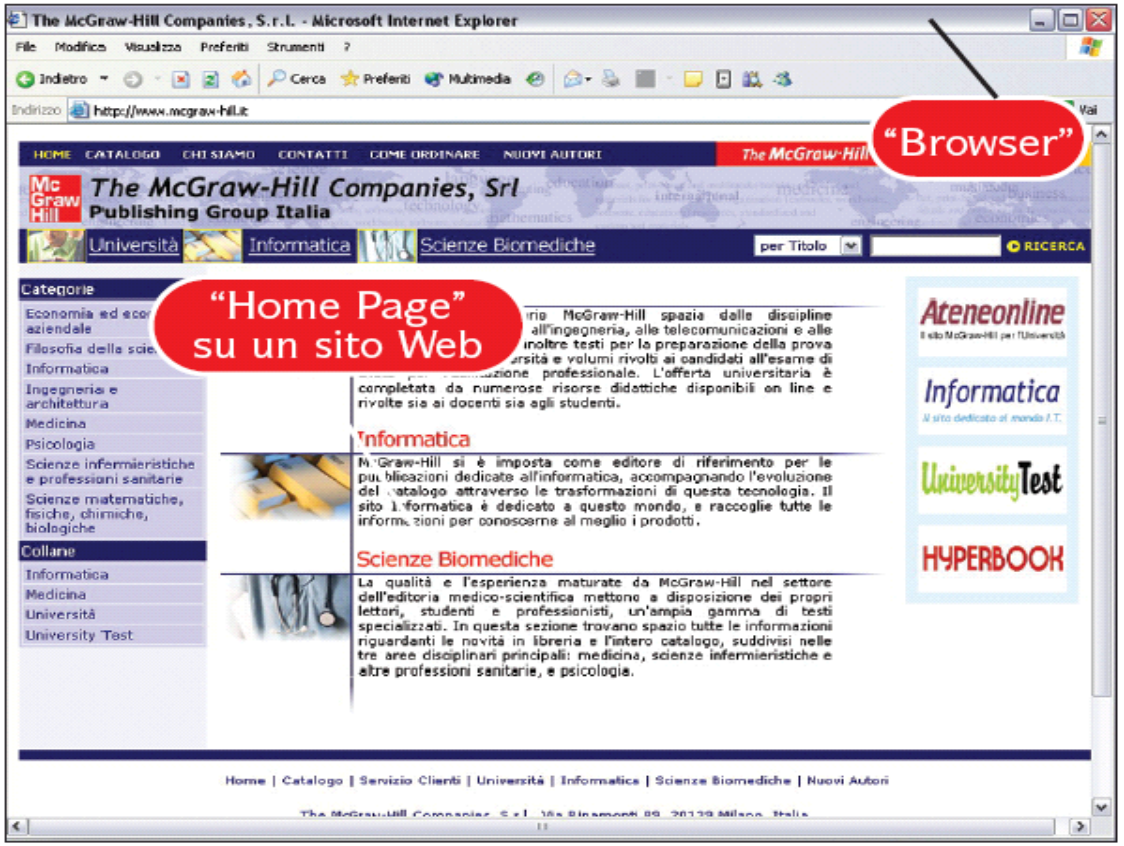
- Il servizio più recente di Internet
- Costituito da documenti che sono su computer diversi (anche a distanza) collegati tra loro
- I documenti sono consultabili per mezzo di programmi chiamati browser
  - Internet Explorer, Mozilla Firefox, Google Chrome, Opera, ecc.

La storia del Web

- Il Web è nato nel 1989
- Da un'idea di Tim Berners-Lee
  - Ricercatore del CERN di Ginevra
- Berners-Lee elaborò i pilastri del Web:
  - HTTP (HyperText Transfer Protocol)
    - Come comunicare
  - HTML (Hypertext Markup Language)
    - Come scrivere
  - URL (Uniform Resource Locator)
    - Dove trovare
- Nel 1998 nasce il World Wide Web Consortium (W3C)

Un pagina Web

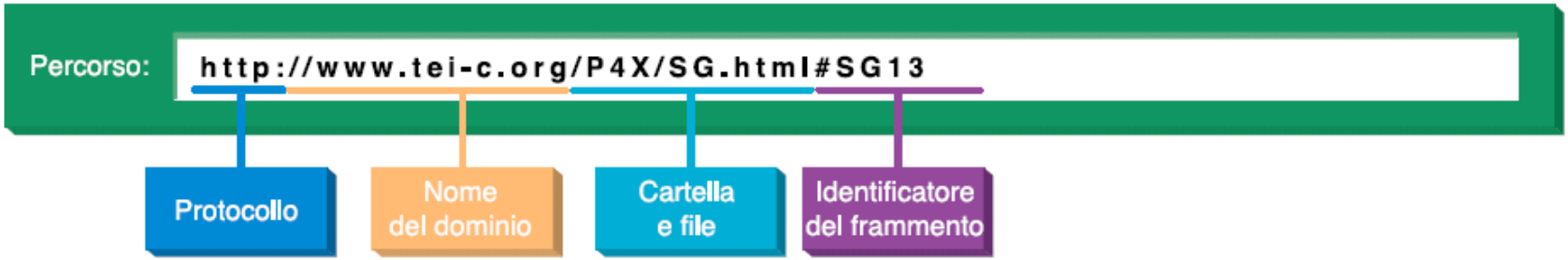
Ciò che appare all'utente sul suo schermo è l'unione di due elementi ben diversi: il ***browser***, l'applicazione che consente di navigare tra le pagine web, e il ***contenuto*** di una pagina presente su un sito.



Home page del sito della McGraw-Hill Italia
http://www.mcgraw-hill.it

Analisi di un indirizzo web (URL)

- Un indirizzo URL è l'unione del metodo (protocollo) per trovare un file in Internet e l'esatta locazione di un elemento all'interno di quel file disponibile su un server. Ogni parte dell'URL identifica, sempre più specificatamente, la posizione dell'elemento.



Indirizzo IP

- Un Indirizzo IP è un numero (a 32 bit) che identifica univocamente i dispositivi collegati con una rete informatica che utilizza lo standard IP (Internet Protocol)
  - Ciascun dispositivo (router, computer, server di rete, stampanti, alcuni tipi di telefoni, ...) ha il suo indirizzo.

Indirizzi IP e DNS

- L'IP ***non è di semplice comprensione*** da parte dell'utente, ed è quindi uso comune assegnare ad ogni IP un ***nome simbolico***
- Per fare questo si utilizza il ***Domain Name System (DNS)***, che associa uno o più nomi ad ogni IP, e gestisce la conversione tra le due codifiche.

SICUREZZA

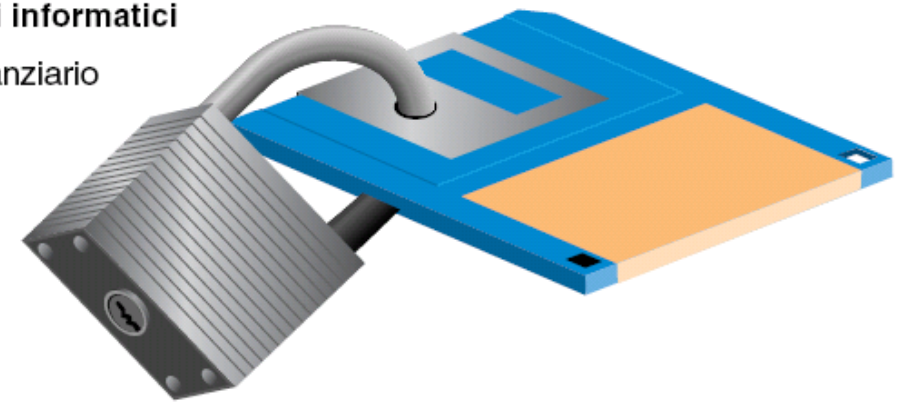
Cosa vuol dire sicurezza informatica

- Sicurezza “interna”
  - Accesso sicuro ai propri dati, alle proprie informazioni.
  - Copia delle informazioni importanti.
  - Gestione di login, nickname e password personali.
- Sicurezza “esterna”
  - Certezza sul trattamento dei dati sensibili.
  - Difesa dagli attacchi da virus e altro malware.
  - Non commettere reati inconsapevolmente.

Crimini e criminali informatici

Le motivazioni dei criminali informatici

- Tornaconto personale o finanziario
- Divertimento
- Vendetta
- Favore personale
- Sfida
- Incidente
- Vandalismo



Tipi di *crimine* informatico

- Furti e manipolazioni dei dati
- Accessi abusivi a informazioni
- Attacchi "Denial of Service"
- Violazioni del copyright

Tipi di *criminale* informatico

- Cracker
- Dipendenti delle aziende colpite
- Persone in genere non autorizzate a svolgere determinate operazioni

La sicurezza in rete

- Le quattro principali aree in ambito di sicurezza in rete sono:
  - *segretezza dei dati*:
    - garantire che utenti non autorizzati possano leggere o modificare dati privati (e.g. crittografia)
  - *autenticazione*:
    - accertamento dell'identità del proprio interlocutore in rete, per evitare di fornire informazioni riservate ad estranei
  - *firme elettroniche*:
    - accertamento dell'autenticità dell'autore di un determinato documento "firmato"
  - *controllo di integrità*:
    - accertamento che un messaggio ricevuto non sia stato modificato durante la trasmissione.

La crittografia

- La crittografia è l'arte di progettare algoritmi (o cifrari) per crittografare un messaggio rendendolo incomprensibile a tutti tranne al suo destinatario
- Il destinatario, con un algoritmo simile deve essere in grado di codificarlo, attraverso un parametro segreto detto chiave (usato in precedenza anche dal mittente per la cifratura)

Algoritmo di crittografia

- Un algoritmo di crittografia riceve un testo da codificare (detto testo in chiaro) e lo trasforma, attraverso la ***chiave***, in un testo cifrato apparentemente incomprensibile
- La sicurezza di un sistema di crittografia risiede solo ed esclusivamente nella segretezza della chiave e non dell'algoritmo che è opportuno far conoscere alla pubblica analisi, in modo che se ne possano scoprire eventuali punti deboli in tempo

I dati cifrati sono inviolabili?

- La crittografia risulta necessaria ovunque si voglia archiviare o trasmettere dati riservati, rendendo impossibile (o meglio molto difficile) l'accesso a chi non dispone della chiave
- ***"Molto difficile"*** risulta più corretto che "impossibile", in quanto la maggior parte dei sistemi di crittografia ritenuti sicuri sono stati violati (nel tempo)

La firma digitale

- La firma digitale viene da molti considerata uno dei migliori mezzi possibili per ridurre drasticamente i problemi di sicurezza relativi alla trasmissione di documenti per via telematica
- Tale sistema permette di semplificare sia i rapporti tra imprese e/o privati che quelli tra cittadini e pubblica amministrazione.

Che cos'è la firma digitale?

- La legge la definisce il ***risultato di una procedura informatica*** – validazione – che attraverso un procedimento crittografico a chiavi asimmetriche, permette di identificare il reale mittente di un documento informatico verificandone l'autenticità

Messaggi a firma digitale

- Come viene inviato un messaggio? Tre diversi modi:
  - il mittente in possesso della chiave pubblica del destinatario cifra con essa il messaggio; il destinatario attraverso la propria chiave privata può decifrarlo
  - è il mittente a rendere cifrato il messaggio con la propria chiave privata, in questo caso chiunque sia in possesso della chiave pubblica del mittente può decifrarlo (in questo modo viene assicurata la reale identità del mittente)
  - il mittente cifra il proprio messaggio con la chiave pubblica del destinatario e con la propria chiave privata; il ricevente dovrà decifrare il testo sia con la propria chiave privata che con quella pubblica del mittente. In questo modo oltre alla segretezza del messaggio dovrebbe essere garantita anche l'autenticità della provenienza

Il certificatore

- Ma come essere sicuri che la chiave pubblica non sia stata contraffatta e provenga effettivamente dall'utente-titolare?
  - Per garantire trasparenza e sicurezza la legge ha creato la figura del CERTIFICATORE:
    - "il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati"
      (D.P.R. 513/97, art.1).

Alcuni consigli

- Se NON uso la crittografia, tutti possono leggere i dati che transitano via Internet…
- Se uso la crittografia, NESSUNO può decifrare il mio messaggio. A meno che:
  - non si riesca a “rompere” la codifica
  - non debba cedere la chiave
  - non sia il destinatario voluto (es. codice carta di credito)
- La crittografia rallenta un po’ la comunicazione

Alcuni consigli

- Il ***commercio elettronico*** si effettua con il browser in modalità sicura (***https*** con lucchetto)
  - La carta di credito per il commercio elettronico si usa SOLO se si conosce bene l'azienda in Internet.
- L'accesso dall'esterno è possibile alle condizioni che noi autorizziamo (impostazioni firewall)

Password

- L'uso di ***password non va confuso con la crittografia***
- Le password (e i relativi nomi utente) servono per accedere ad "aree riservate" (in locale o in rete) non per cifrare i dati
- Non usare parole di senso compiuto come password perché sono facilmente identificabili
  - i9C_1!kdNd è una password sicura
  - Gianni121290 (nome e data di nascita del fidanzato) non è una password sicura

Malware (http://it.wikipedia.org/wiki/Malware)

- Virus
  - Si attaccano a un file e vengono eseguiti ogni volta che il file infetto viene aperto
- Worm
  - Non necessita di attaccarsi a un altro eseguibile per diffondersi
- Backdoor
  - programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione
- Cavallo di Troia
  - Inserito in un programma apparentemente utile contiene istruzioni dannose eseguite all'insaputa dell'utente
- Dialer
  - Accedono a internet modificando il numero telefonico con uno a tariffa speciale all'insaputa dell'utente. Nessun problema per chi usa ADS
- Spyware
  - Usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato
- Hoax
  - Sono bufale (catene di S. Antonio, richieste di aiuto per malattie, richieste di aiuto per trasferimento di denaro, …)

I Virus

- In informatica il virus è un ***frammento di codice*** inserito all'inizio di un normale programma con lo scopo di *alterare o distruggere dati, rallentare le prestazioni di sistemi o bloccarli del tutto*
- Lo sviluppo di Internet ha favorito ed aumentato la diffusione di migliaia di tipologie di virus
- Per ogni virus "progettato" viene immediatamente codificato un nuovo ***antivirus***:
  - programma che contiene grandi liste di virus regolarmente aggiornate e che ispeziona i file sospetti "riconoscendo" ed eliminando l'eventuale codice pericoloso.
- Essendo spesso causa di distruzione o manomissione di dati importanti, la generazione di virus è ritenuta un ***reato***

Virus: alcuni consigli

- Un virus è un programma scritto da programmatori!
- Gli antivirus possono bloccare alcuni dei virus riconosciuti (esistenti nel database dell'antivirus)
- Gli eseguibili allegati alle email vanno eseguiti SOLO se si è certi del contenuto (e di chi ha spedito la email)
- I virus possono essere eseguiti all'insaputa dell'utente
- I virus permettono lauti guadagni alle aziende che producono antivirus e s.o.
- Formattazione: cancella tutto il contenuto del disco, virus ma anche dati

Tecniche di attacco

- Sniffing
  - attività di intercettazione passiva dei dati che transitano in una rete telematica
- Spoofing
  - tipo di attacco informatico dove viene impiegata in qualche maniera la falsificazione dell'identità (es.: falsificazione dell’indirizzo IP)
- Phishing
  - truffa via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili

Lo Spam

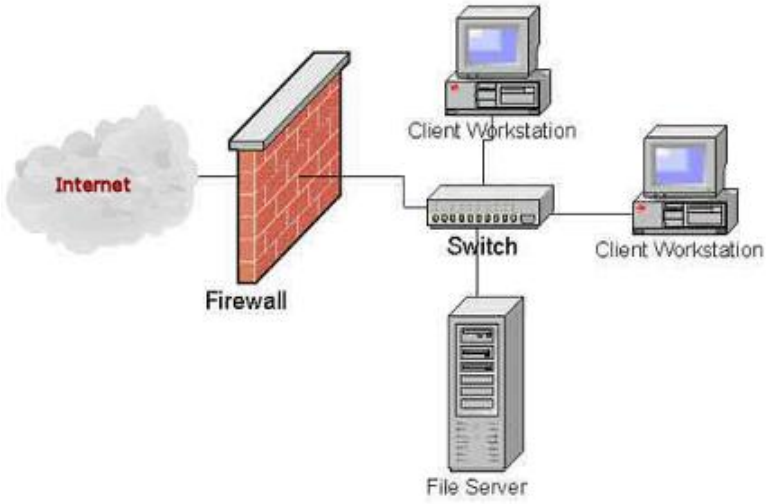
- La SPAM (Spiced Ham) era la carne in scatola fornita ai soldati dell'esercito americano, e si guadagnò una ***fama negativa***
- In Internet lo "Spamming" consiste nell'***invio di messaggi pubblicitari*** tramite posta elettronica in ***nessun modo sollecitati*** ("Junk Mail")
- Lo Spamming danneggia il ricevente facendogli ***perdere tempo e denaro*** per scaricare posta inutile, e danneggia il gestore del server di posta con uno smisurato aumento di "traffico" nelle sue linee.

Evitare lo spam

- Evitare messaggi di spam è molto difficile: alcuni metodi sono troppo blandi mentre altri troppo restrittivi (fermano anche posta “legittima”).
- Tuttavia esistono norme pratiche che consentono di ridurre questo problema:
  - evitare di comunicare pubblicamente il proprio indirizzo email attraverso siti, guestbook, chat, messenger, ICQ, ecc.
  - spesso gli spammers reperiscono automaticamente gli indirizzi, cercando stringhe della forma tizio@caio.ecc
  - quindi, se desideriamo comunicare la nostra email in un contesto pubblico è buona norma scriverla nella forma: tizioNOSPAM@caio.ecc
- Se ricevo mail di spam NON rispondo

Il Firewall

- Il Firewall è un Nodo configurato come una barriera per impedire l'attraversamento del traffico da un segmento all'altro, migliorando la sicurezza della rete.
- Può fungere da barriera tra reti pubbliche e private collegate tra loro.



Il Firewall

- Utilizzando un firewall è possibile:
  - impedire gli accessi indesiderati;
  - monitorare le sedi alle quali si accede più di frequente;
  - analizzare la quantità di larghezza di banda che la connessione Internet sta utilizzando.
- Distinguiamo tra FW hardware e FW software

Firewall Hardware

- Un firewall può essere realizzato con un normale computer
- Può essere una funzione inclusa in un router
- Può essere un apparato specializzato.

Firewall Software

- Un FW software effettua un controllo di tutti i programmi che tentano di accedere a Internet presenti sul computer
- L'utente può impostare delle regole tali da concedere o negare l'access ad Internet

Firewall Hardware e Software

- Il firewall Software risulta più economico di quello Hardware ma anche più vulnerabile.
- Nel FW Hardware le regole che definiscono i flussi di traffico permessi vengono impostate in base all'indirizzo IP sorgente, quello di destinazione e la porta attraverso la quale viene erogato il servizio.
- Nel FW software è sufficiente che l'utente esprima il consenso affinché una determinata applicazione possa interagire con il mondo esterno attraverso il protocollo IP.
- Per poter entrare in un sistema protetto da FW SW, è sufficente mandare in crash il programma.
- Mentre per entrare in un sistema con FW HW è necessario manomettere FISICAMENTE il dispositivo.

CONSIGLI FINALI

Come aggiornarsi?

- Internet è la più ampia fonte di informazioni su se stesso
- I gruppi d'utenza ***(user group)*** sono libere organizzazioni di utenti, e ne esistono per qualunque hardware o software prodotto
- Le organizzazioni professionali hanno servizi esclusivi per i loro soci, ma sono in genere aperte alla consultazione pubblica e offrono informazioni preziose. Nel settore informatico:
  - Educom
  - Infoworld
  - Computerworld

Prepararsi per tempo ai cambiamenti tecnologici

- E’ importante ricordare che:
  - maggiori conoscenze informatiche si hanno, più facile sarà adattarsi ai cambiamenti che inevitabilmente subiranno gli strumenti che usiamo
  - va bene tenersi al corrente dei prossimi arrivi sul mercato informatico, ma non serve correre freneticamente dietro alla tecnologia
  - il futuro del proprio lavoro va immaginato, e non subito

Ergonomia

- L’ergonomia è la scienza che studia l'interazione tra uomo e macchina
- Alcuni consigli per lavorare davanti al PC:
  - ***Illuminare*** l'ambiente meno rispetto alla luminosità dello schermo
  - Attenzione ai ***riflessi***, alla posizione delle fonti di luce e agli oggetti o vestiti chiari.
  - I ***caratteri*** devono essere ben nitidi rispetto allo sfondo.
  - ***Sedia*** regolabile in altezza.
  - Documenti da consultare vanno tenuti alla stessa distanza dagli occhi che ha lo schermo
  - Una pausa raccomandata:
    - se il meno del 60% del tempo si fissa lo schermo = ¼ d'ora ogni due ore;
    - se oltre il 60% del tempo si fissa lo schermo = ¼ d'ora ogni ora.