



Elementi di reti di calcolatori

Politecnico di Milano
Facoltà del Design – Bovisa

Prof. Gianpaolo Cugola
Dipartimento di Elettronica e Informazione

cugola@elet.polimi.it
<http://www.elet.polimi.it/upload/cugola>



Politecnico
di Milano

Testi consigliati

- Slide presentate a lezione
- James F. Kurose, Keith W. Ross “Internet e Reti di calcolatori 2/ed” - McGrawHill
- Gary Govanus “TCP/IP” - McGrawHill



Indice

- **Nozioni essenziali**
 - **Topologia di rete e supporti fisici**
 - **Segnalazione, modulazione e trasmissione**
 - **Indirizzamento e commutazione**
 - **Il concetto di protocollo**
- **Le reti locali**
 - Protocolli per reti cablate: Ethernet, ppp
 - Protocolli per reti wireless: 802.11, bluetooth
 - I dispositivi per reti locali
- **Le reti geografiche**
 - Internet e il protocollo TCP/IP
 - I protocolli applicativi: telnet, ssh, ftp, smtp, pop, mime
- **Cenni di sicurezza informatica**



Il concetto di rete di calcolatori

- Con il termine *rete di calcolatori* intendiamo riferirci a un sistema informatico costituito da due o più calcolatori collegati attraverso un sistema di comunicazione allo scopo di condividere risorse e informazioni
- Una *applicazione distribuita* è una applicazione composta da più elementi cooperanti posti in esecuzione su macchine diverse all'interno di una rete di calcolatori
 - Esempio, il web: il browser si collega ad un server remoto per chiedere una pagina che poi visualizza sul pc locale



Perché usare una rete?

- Per condividere periferiche costose, come le stampanti
 - In una rete, tutti i computer possono accedere alla stessa stampante
- Per scambiare dati tra PC
 - Trasferendo file attraverso la rete, non si perde tempo nel copiare i file su un dischetto (o su un CD)
 - Inoltre vi sono meno limitazioni sulle dimensioni del file che può essere trasferito attraverso una rete
- Per centralizzare programmi informatici essenziali
 - Come le periferiche, anche i software possono avere costi molto alti ed è spesso utile dividere tali costi (licenze) su più utenti
 - In altri casi si centralizza l'accesso al software perché lo si deve sfruttare assieme per realizzare un compito in collaborazione, come per gli applicativi finanziari e contabili
- Per comunicare mediante Internet con il resto del mondo
- ...



Tipi di rete

- Le reti possono avere dimensioni differenti ed è possibile ospitarle in una sede singola oppure dislocarle in tutto il mondo
- Una rete che è collegata su un'area limitata si chiama "Rete Locale" oppure *LAN (Local Area Network)*
- Per *WAN (Wide Area Network)* si intende un gruppo di dispositivi o di LAN collegate nell'ambito di una vasta area geografica, spesso mediante linea telefonica o altro tipo di cablaggio (ad es. linea dedicata, fibre ottiche, collegamento satellitare, ecc..). Uno dei più grandi esempi di WAN è l'Internet stessa
- All'estremo opposto stanno le *PAN (Personal Area Network)* che collegano tra loro, di norma attraverso connessioni radio, i dispositivi di un singolo utente



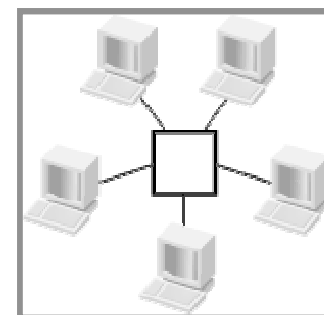
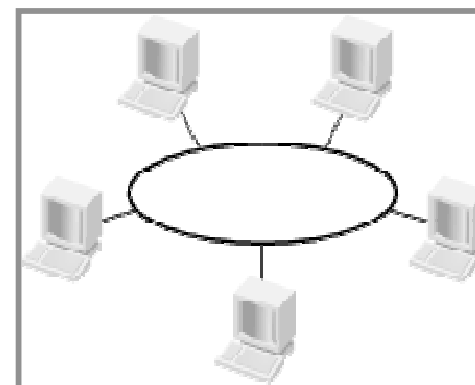
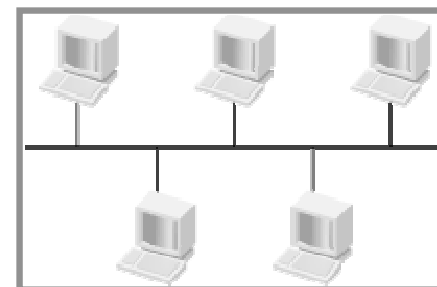
Topologia della rete

- Con il termine *topologia della rete* si indica la disposizione fisica dei componenti che realizzano la rete...
- ... la loro tipologia...
- ... e la modalità con la quale sono connessi



Topologia delle reti locali

- A **BUS**: è il metodo più semplice di connettere in rete dei computer. Consiste di un singolo cavo (chiamato dorsale o segmento) che connette in modo lineare tutti i computer. I dati sono inviati a tutti i computer come segnali elettronici e vengono accettati solo dal computer il cui indirizzo è contenuto nel segnale di origine.
- Ad **ANELLO**: i computer sono connessi tramite un unico cavo circolare privo di terminatori. I segnali sono inviati in senso orario lungo il circuito chiuso passando attraverso ciascun computer che funge da ripetitore e ritrasmette il segnale potenziato al computer successivo: si tratta quindi di una tipologia attiva, a differenza di quella a bus.
- A **STELLA**: i computer sono connessi ad un componente centrale chiamato Hub. I dati sono inviati dal computer trasmittente attraverso l'Hub a tutti i computer della rete.





Topologia elementare

- La più elementare topologia di rete prevede l'utilizzo di due soli PC (o altri dispositivi di rete) connessi direttamente tra di loro mediante *cavo di rete cross*
- Questa configurazione può essere utile ad esempio per scambiare dati tra portatile e PC oppure per connettere al PC una stampante di rete



Supporti fisici - 1

- Diversi *mezzi trasmissivi* possono essere adottati per costituire il supporto fisico sul quale viaggia la comunicazione in una rete di calcolatori
- I principali mezzi trasmissivi adottati sono:
 - Doppino ritorto (twisted pair):
 - Costituito da due fili di rame ricoperti da una guaina e ritorti
 - Tipicamente utilizzato per trasmissione telefonica
 - Consente velocità di trasmissione medio alte (100÷1000 Mbs su rete locale)
 - Su rete telefonica le velocità è più bassa (12 Mbps con ADSL)



Supporti fisici - 2

– Cavo coassiale:

- Costituito da un filo centrale in rame rivestito da una guaina in plastica a sua volta rivestita da una maglia in rame. Il tutto ricoperto da una guaina in plastica
- Permette velocità di trasmissione medio alte (100 Mbps)

– Fibra ottica:

- Costituito da una fibra di vetro ricoperta, capace di trasportare segnali luminosi
- La trasmissione avviene nel campo ottico sfruttando diodi fotoelettrici alle estremità del cavo
- Permette velocità di trasmissione molto elevate, dell'ordine delle decine di Gbps)



Supporti fisici - 3

- Onde elettromagnetiche:
 - Usate per trasmissioni radio e via satellite
 - Consentono trasmissioni su lunghissime distanze con degrado minimo del segnale
 - Permettono velocità di trasmissione medio alte e variabili a seconda della banda di frequenza utilizzata



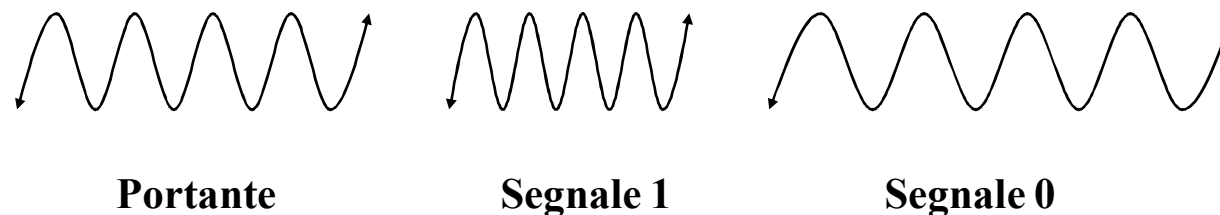
Segnalazione

- I dati binari scambiati da due calcolatori possono essere trasmessi direttamente sul canale o sfruttando la modulazione di un *segnale portante*
- Nel primo caso si parla di *segnalazione in banda base*
 - Esempio: il bit 1 viene trasmesso su un cavo come presenza di tensione, il bit 0 come assenza
- Nel secondo si parla di *segnalazione in modulazione*



Modulazione e demodulazione - 1

- Il principio della modulazione si basa sull'esistenza di un segnale portante che viene modulato per codificare i bit 1 e 0
- Modulazione in frequenza





Modulazione e demodulazione 2

- Modulazione di ampiezza



Portante



Segnale 1

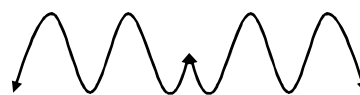


Segnale 0

- Modulazione di fase



Portante



Passaggio di fase



Trasmissione

- La trasmissione può essere
 - Simplex
 - Il senso di trasmissione è fisso (poco usata)
 - Half-duplex
 - La trasmissione è possibile, *alternativamente*, nei due sensi
 - Full-duplex
 - La trasmissione è possibile, *contemporaneamente*, nei due sensi



Indirizzamento e commutazione

- *Indirizzamento* è un servizio fornito da una rete di comunicazione che consente di indirizzare un messaggio ad un singolo destinatario
- *Commutazione* indica la modalità con la quale la rete opera per fornire il servizio di indirizzamento
 - Commutazione di circuito
 - Commutazione di pacchetto



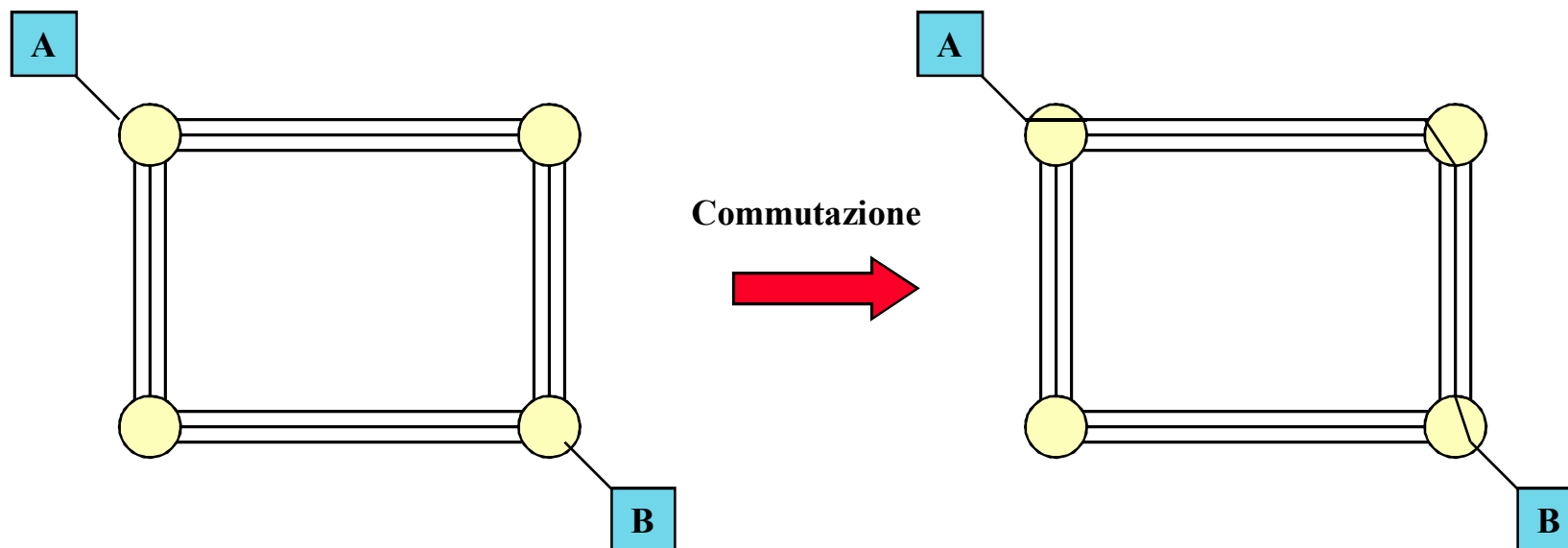
Commutazione

- In generale una rete non è completa
- Per collegare due nodi occorre stabilire un collegamento tra questi
- Nel caso di reti a commutazione di circuito il collegamento è realizzato in maniera fisica
- Nel caso di reti a commutazione di pacchetto il collegamento è “virtuale”



Commutazione di circuito

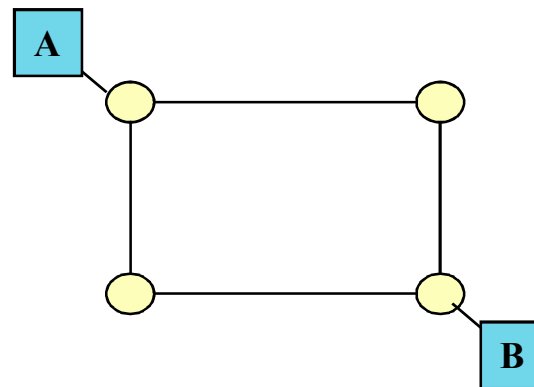
- Quando un nodo A chiede un collegamento con un nodo B viene creato un circuito fisico che collega A a B





Commutazione di pacchetto

- In fase di trasmissione la rete non forma alcun collegamento diretto tra due nodi...
- ... ma si limita a inviare i messaggi scambiati lungo i collegamenti della rete dal mittente al destinatario
 - Messaggi diversi possono prendere strade diverse





Reti a commutazione di pacchetto: servizi forniti

- Le reti a commutazione di pacchetto forniscono due tipi di servizi
 - Servizi a datagramma
 - Non viene creato alcun circuito tra mittente e destinatario
 - Il singolo messaggio viene gestito indipendentemente dai precedenti e dai successivi
 - Servizi a circuito virtuale
 - Viene stabilito un circuito virtuale tra mittente e destinatario
 - Viene mantenuto l'ordinamento tra messaggi diversi inviati lungo tale circuito virtuale
 - messaggi diversi inviati lungo lo stesso circuito virtuale possono comunque compiere strade diverse lungo la rete per raggiungere il destinatario



Protocollo di comunicazione

- Con il termine *protocollo di comunicazione* si indica l'insieme di regole di comunicazione che debbono essere seguite da due interlocutori affinché essi possano comprendersi
- Esempio: il protocollo alla base della comunicazione tra docente e allievi durante una lezione
 - il docente parla in una lingua comprensibile agli allievi
 - gli allievi ascoltano (si spera)
 - quando vogliono intervenire gli allievi alzano la mano ed attendono il permesso del docente per iniziare a parlare
 - durante l'intervento degli allievi il docente ascolta
 - al termine dell'intervento il docente risponde



Protocollo di comunicazione

- In una rete di calcolatori il protocollo di comunicazione stabilisce tutti gli aspetti della comunicazione
 - dagli *aspetti fisici*...
 - Esempio: supporto fisico, meccanismo di segnalazione)
 - ... agli *aspetti più eminentemente logici*
 - Esempio: meccanismo di commutazione, regole di codifica dell'informazione, ecc.



Organizzazione a pila dei protocolli

- Data la loro complessità i protocolli utilizzati dai calcolatori sono organizzati secondo una *gerarchia*
- Ogni protocollo si appoggia ai protocolli di più basso livello per fornire un servizio di qualità superiore
- Esempi
 - Un protocollo con correzione d'errore costruito sulla base di un protocollo di rete non affidabile
 - Il protocollo che stabilisce le regole di codifica dell'informazione si appoggia ad un protocollo di trasporto che stabilisce come debbano essere trasportati i dati

ISO/OSI

Application
Presentation
Session
Transport
Network
Data Link
Physical



Indice

- Nozioni essenziali
 - Topologia di rete e supporti fisici
 - Segnalazione, modulazione e trasmissione
 - Indirizzamento e commutazione
 - Il concetto di protocollo
- **Le reti locali**
 - **Protocolli per reti cablate: Ethernet, ppp**
 - **Protocolli per reti wireless: 802.11, bluetooth**
 - **I dispositivi per reti locali**
- Le reti geografiche
 - Internet e il protocollo TCP/IP
 - I protocolli applicativi: telnet, ssh, ftp, smtp, pop, mime
- Cenni di sicurezza informatica



Il protocollo Ethernet

- Ethernet è il protocollo più diffuso per la creazione di reti locali
- Copre i livelli 1 e 2 della pila OSI
- Sviluppato a metà degli anni '70 nei laboratori della Xerox ottiene la prima standardizzazione ad opera della IEEE nel 1980
- Nella forma attuale viene standardizzato nel 1983 (standard IEEE802.3)



Ethernet: caratteristiche - 1

- Il protocollo ethernet consente trasmissioni su rete locale alla velocità di 10Mbit/s
 - La versione FastEthernet oggi in uso nella maggior parte delle installazioni arriva a 100 Mbit/s
 - La versione GigaEthernet raggiunge i 1000 Mbit/s
- La connessione avviene secondo lo schema a bus
 - Ogni macchina è logicamente collegata ad un unico canale sul quale trasmette le informazioni e dal quale riceve le informazioni immesse da tutte le altre macchine
- I supporti adottati possono essere diversi:
 - Coassiale spesso (1 cm di diametro c.a.)
 - Coassiale sottile (5 mm di diametro c.a.)
 - Doppino ritorto
- A seconda del supporto adottato varia la lunghezza massima del cavo e la distanza minima tra le macchine



Ethernet: caratteristiche - 2

- La trasmissione avviene adottando una codifica in banda base
- L'accesso alla rete avviene secondo la politica CSMA/CD (Carrier Sense Multiple Access/Collision Detection)
 - Prima di iniziare a trasmettere si ascolta il canale per accertarsi che non sia già in uso
 - Appena il canale è libero si inizia a trasmettere
 - Durante la trasmissione si ascolta il canale per sincerarsi che non stiano avvenendo collisioni
 - In caso di collisioni:
 - si continua a trasmettere fino al raggiungimento della dimensione minima del pacchetto (64 byte)
 - si attende un tempo arbitrario e si ricomincia a trasmettere

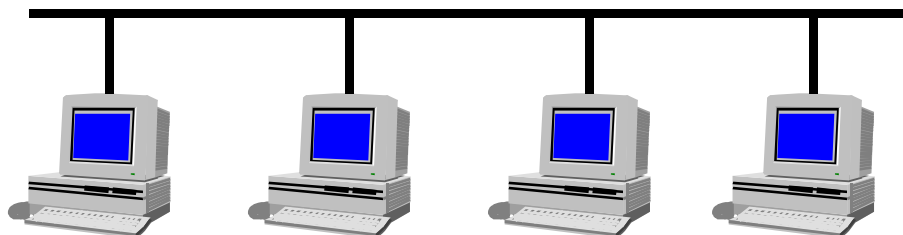


Ethernet: conseguenze dell'uso della politica CSMA/CD

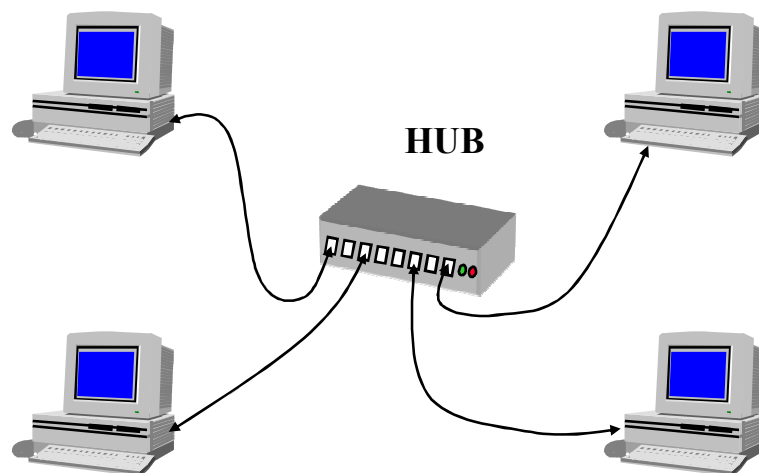
- La velocità di trasmissione effettiva dipende dal numero di collisioni...
- ... che a sua volta dipende dal numero di macchine in rete
 - In una situazione reale non si va oltre il 40%÷60% della banda disponibile
- La rete non è adatta alla trasmissione di traffico multimediale
 - Non è possibile assicurare una ben precisa qualità del servizio
- Più in generale la rete non è adatta allo sviluppo di applicazione real-time



Ethernet: topologia logica e fisica



**Topologia logica \equiv
topologia fisica usando coax**



**Topologia fisica
(usando doppino)**



Ethernet: caratteristiche del protocollo

- Connectionless
 - Non viene instaurato alcun tipo di connessione tra mittente e destinatario
- Assenza di supporto alla correzione d'errore
 - Il campo FCS permette solo di riconoscere eventuali errori ma non esiste supporto alla loro correzione
- Best-effort
 - Il sottosistema di rete non assicura la consegna ma fa solo “del proprio meglio” per consegnare il messaggio



Il protocollo PPP

- Usato per il collegamento diretto (punto a punto) tra due macchine
 - Tipicamente attraverso l'uso di un modem o di una connessione diretta via cavo
- Protocollo di livello 2
 - Si appoggia ad un protocollo di più basso livello quale V.90
- Può essere utilizzato per convogliare protocolli di livello 3 diversi quali IP, IPX/SPX, ecc.
- Protocollo con connessione e autenticazione



L'era del wireless

- Guglielmo Marconi ha inventato il telegrafo nel 1896
 - Nel 1901 la prima trasmissione attraverso l'oceano atlantico
- Da allora di strada ne abbiamo fatta...
 - La radio, prima, la televisione poi hanno portato le trasmissioni wireless in tutte le case
- Le comunicazioni satellitari sono iniziate negli anni '60
 - Oggi le reti satellitari trasportano 1/3 del traffico voce e il 100% delle trasmissioni televisive tra continenti
- Questi ultimi anni saranno ricordati come gli anni delle trasmissioni cellulari e wireless in generale
 - Nel 1990 i cellulari nel mondo erano c.a. 11 milioni
 - Nel 2004 hanno raggiunto il miliardo
 - Dal 1996 il numero di abbonamenti effettuati per reti cellulari ha superato quelli fatti per reti fisse
- Se le reti cellulari hanno iniziato la loro storia come reti voce oggi l'interesse è per il trasporto di dati
 - Servizi di messaggistica, accesso alla rete Internet, servizi “push”, servizi position-aware (anche attraverso la diffusione della tecnologia GPS)
- IEEE 802.11 e Bluetooth completano l'offerta delle reti dati in ambito wireless



Mobile computing

- A livello utente possiamo evidenziare diversi scenari di mobilità fisica
 - Nomadic computing
 - Base station mobility
 - Ad-hoc networking
- Non tutti prevedono l'uso di tecnologie wireless



Nomadic Computing

- Gli utenti si connettono alla rete da postazioni diverse,
- ... non sono connessi in maniera permanente, ...
- ... non sfruttano necessariamente reti wireless: eseguono la maggior parte delle operazioni legate alla rete da postazioni “fisse”





Base Station Mobility

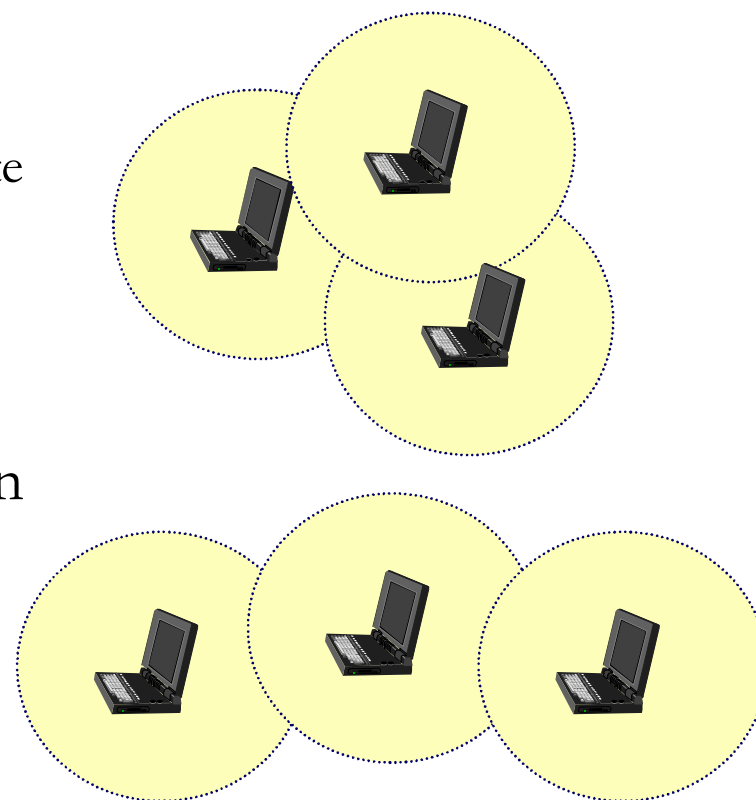
- Gli utenti si muovono da una postazione all'altra rimanendo connessi durante lo spostamento
- ... sfruttano link wireless per connettersi a una rete cablata...
- ...sulla quale viene eseguita la maggior parte della computazione (nonchè l'istradamento delle informazioni)
- I nodi mobili operano come “foglie” dell'architettura di rete





Ad-Hoc Networking

- E' lo scenario più estremo nel quale non è disponibile alcuna infrastruttura fissa
 - La comunicazione avviene interamente attraverso connessioni wireless
- In una “mobile ad-hoc network” (MANET), non sono necessari speciali meccanismi di routing se tutti i nodi sono reciprocamente “in range”
- Altrimenti ogni nodo deve esercitare funzionalità tipiche di un router tradizionale
- Esistono situazioni “miste” che uniscono MANET e reti fisse





IEEE 802.11

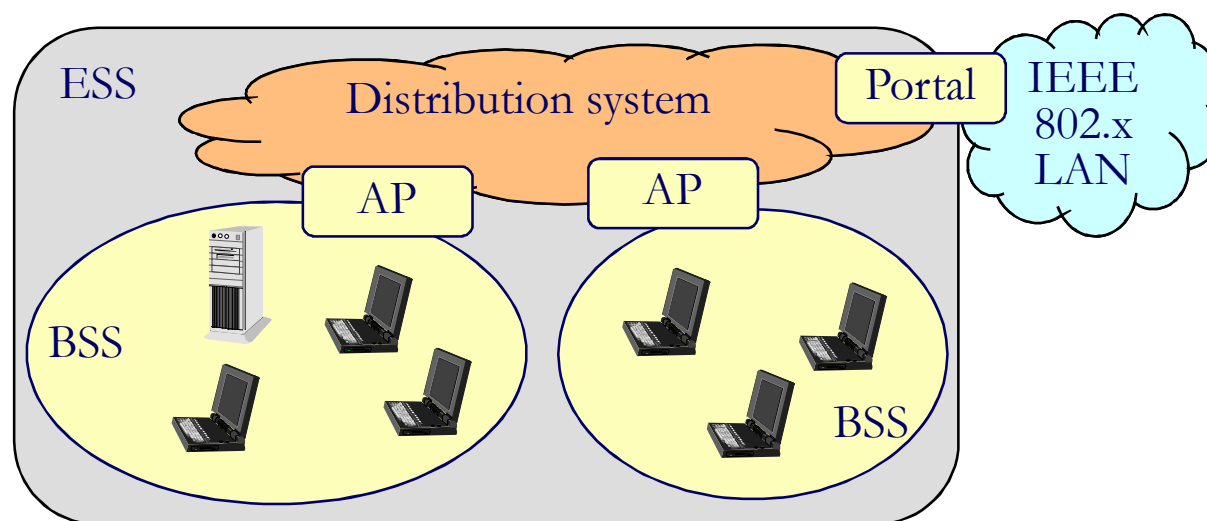
- Nel 1990 l'IEEE (Institute of Electrical and Electronic Engineers) fonda un gruppo avente l'obiettivo di produrre un insieme di specifiche per reti locali wireless sotto la nomenclatura di “standard 802.11”
- La prima versione dello standard, prodotta nel 1997, include la specifica per un livello MAC (livello 2 della pila OSI) e per tre livelli fisici (operanti a velocità comprese tra 1 e 2 Mbps):
 - Direct-sequence spread spectrum (DSSS)
 - Frequency-hopping spread spectrum (FHSS)
 - Infrared
- Di fatto l'opzione infrared non venne mai commercialmente adottata per le scarse prestazioni e per le intrinseche limitazioni (trasmissione solo “a vista”)

} operante nella banda libera
2.4GHz ISM (Industrial,
Scientific, and Medical)
} operante su lunghezze d'onda
tra 850 e 950nm



L'architettura di una rete 802.11

- Lo standard 802.11 sfrutta una architettura di rete di tipo cellulare nella quale ogni cella, nota come Basic Service Set (BSS) contiene un insieme di stazioni che adottano lo stesso protocollo MAC e competono per l'accesso al medium
- Ogni BSS tipicamente contiene una base station (nota anche come Access Point, AP) utilizzata per permettere la comunicazione tra le stazioni
- L'AP lega tra loro la BSS di competenza al sistema di distribuzione (una rete wireless o tradizionale) che connette diverse BSS
- L'intero sistema, chiamato External Service Set (ESS) è visto dai livelli superiori come un'unica rete LAN di tipo 802
- Una rete 802.11 può anche essere configurata in modalità "ad hoc", ovvero con un'unica BSS e senza AP





Il roaming su reti 802.11

- Con il termine “roaming” si intende, in ambito 802.11, il meccanismo che permette ad una stazione di muoversi da una cella (BSS) all'altra senza perdere la propria connettività
- In particolare, lo standard definisce tre forme di mobilità
 - *No transition*. In questo modello l'unica forma di mobilità è all'interno della stessa BSS
 - *BSS transition*. In questo modello una stazione può muoversi da una BSS all'altra all'interno dello stesso ESS
 - *ESS transition*. In questo modello una stazione può muoversi da una BSS all'altra anche se queste appartengono a ESS diverse
- La prima forma di mobilità è del tutto trasparente al sistema e non richiede alcun meccanismo particolare per essere supportata
 - Non si esce dal range trasmissivo dell'AP di competenza
- Per la seconda forma di mobilità non viene definito un meccanismo completo ma sono definiti una serie di servizi, in particolare per l'associazione, deassociazione e riassociazione di una stazione ad un AP
 - Alcuni produttori, sulla base di tali servizi, forniscono dei meccanismi di roaming per questo tipo di mobilità
- Per la terza forma di mobilità non è previsto alcun supporto



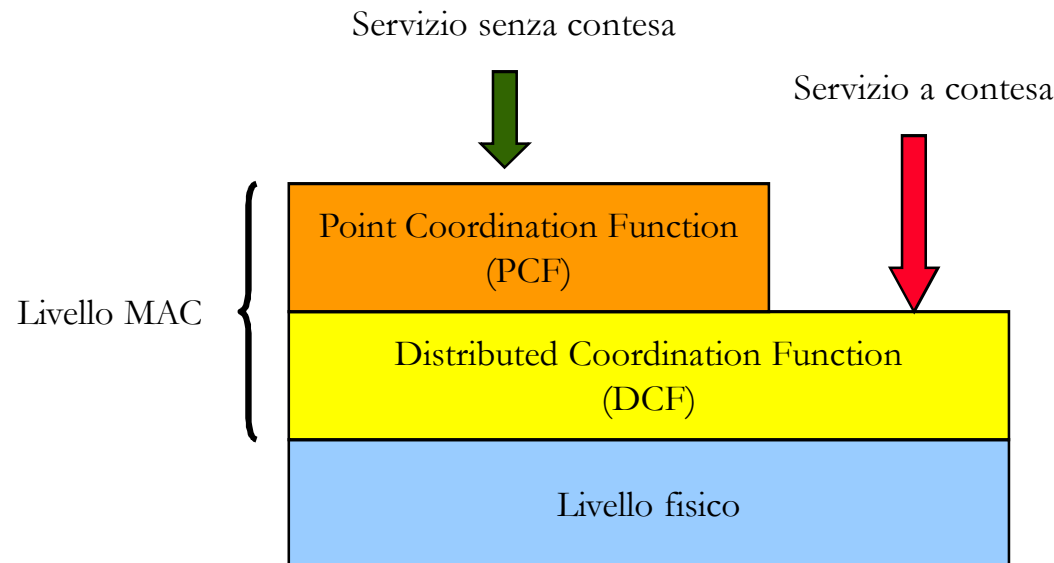
MAC 802.11 - Medium Access Control

- Compito principale del livello MAC è gestire l'accesso al canale
- Il gruppo 802.11 ha considerato due tipi di politiche di accesso
 - Protocolli di accesso distribuiti, i quali, come il CSMA/CD, distribuiscono la decisione di trasmettere a tutti i nodi tramite un meccanismo di “ascolto” della portante (carrier-sense)
 - Protocolli di questo tipo sono utili in reti ad-hoc oppure in presenza di traffico fortemente bursty
 - Protocolli di accesso centralizzati, che implicano la regolazione delle trasmissioni da parte di un decisore centralizzato
 - Si tratta di protocolli maggiormente utili quando parte dei dati è sensibile a ritardo di trasmissione o richiede particolari tipologie di qualità del servizio
- In ambito radio non è possibile adottare la politica CSMA/CD tipica delle reti ethernet
 - Determinare bassi livelli di segnale e distinguere tra segnale e rumore non è possibile in fase di trasmissione (la potenza del segnale trasmesso non permette una accurata lettura)
 - Non è detto che tutte le stazioni sentano tutte le altre (problema della stazione nascosta)



DFWMAC - Distributed Foundation Wireless MAC

- Il risultato dell'802.11 è stato un algoritmo denominato DFWMAC che consente un accesso di tipo distribuito con un meccanismo di controllo centralizzato costruito al di sopra di esso





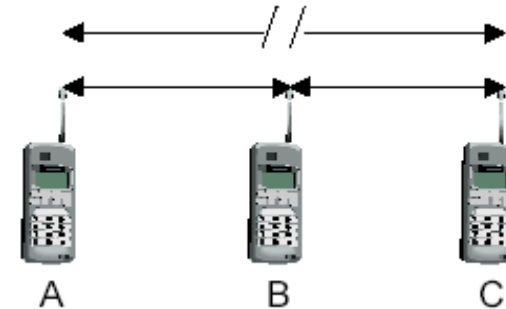
DCF: Approccio generale

- La funzione di coordinamento distribuita costituisce la base del meccanismo e deve essere sempre disponibile
- Si basa su un meccanismo CSMA/CA con ritrasmissione e acknowledge



DCF: La stazione nascosta

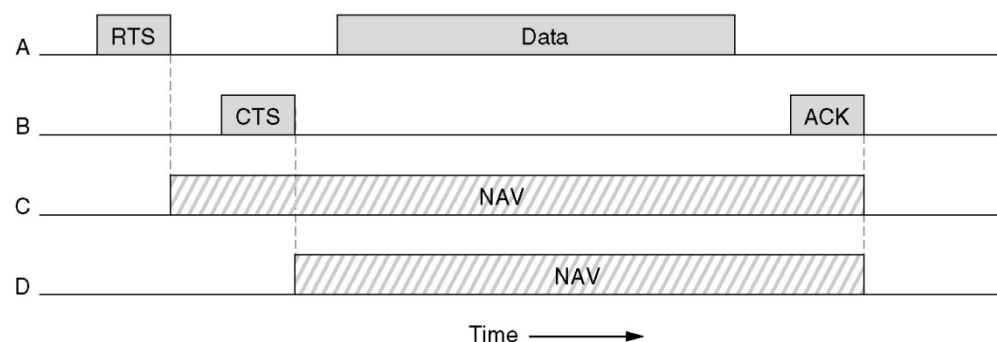
- A differenza di una rete cablata, in una rete wireless non tutte le stazioni sentono tutte le altre
- Si può verificare il fenomeno della “stazione nascosta”
 - A trasmette a B
 - C è fuori dal range trasmissivo di A e sente il canale libero
 - C inizia a trasmettere
 - In B si verifica una collisione
 - A era “nascosto” per C





DCF: RTS/CTS

- Il problema della stazione nascosta è alleviato in 802.11 adottando un meccanismo di RTS/CTS (opzionale)
- La stazione che vuole trasmettere invia un pacchetto di *Request To Send* che include il tempo necessario alla trasmissione
- La stazione ricevente risponde con un pacchetto di *Clear To Send* che include anch'esso il tempo necessario alla trasmissione
- Le altre stazioni non occupano il canale per un tempo detto Network Allocation Vector (NAV) che viene inizializzato al tempo indicato nei pacchetti di RTS e CTS





PCF: Approccio generale

- Si tratta di un meccanismo (opzionale per 802.11) di accesso al canale regolato da un controllore centrale utile per traffico a qualità del servizio garantita
- Il controllore (di norma l'AP) coordina l'accesso al canale interrogando le stazioni tramite appositi pacchetti per sapere se intendano trasmettere
- Il coordinatore ha la possibilità di controllare il canale e bloccare il traffico asincrono quando invia le interrogazioni e si pone in attesa delle risposte
- Per evitare che la stazione di coordinamento blocchi tutto il traffico asincrono emettendo ripetute interrogazioni viene introdotto un intervallo temporale denominato *supertrama*
 - Nella prima parte di tale intervallo la stazione di coordinamento emette interrogazioni in modo sequenziale, lasciando libero il resto dell'intervallo e permettendo la procedura di contesa per l'accesso asincrono



Livello fisico

- Lo standard 802.11 originale (1997) include la specifica per tre livelli fisici diversi
- Due di questi usano la banda tra 2.4 e 2.5GHz detta ISM (Industrial Scientific and Medical), lasciata libera dall'attuale regolamentazione
 - Due possibili velocità: 1 e 2 Mbps
- La terza usa l'infrarosso (lunghezze d'onda tra 850 e 950nm)
 - Di fatto l'opzione infrarosso non venne mai commercialmente adottata per le scarse prestazioni e per le intrinseche limitazioni (trasmissione solo "a vista")
- La potenza trasmissiva varia tra 1W (states) e 100 mW (europa)
- Il range trasmissivo conseguente varia tra i 40 metri (indoor) e i 200 metri (outdoor)
 - Dipende fortemente dal tipo di antenna adottata



802.11a, 802.11b e 802.11g

- Nel 1999, l'IEEE aggiunge due nuovi standard per il livello fisico:
 - 802.11a opera a 5GHz, con velocità fino a 54Mbps
 - La banda usata non è libera in Europa (solo negli states)
 - 802.11b opera a 2.4GHz, con velocità di 5.5 e 11Mbps
 - Alcuni produttori (e.g., USRobotics) forniscono una versione a 22Mbps, backward compatibile con lo standard
- Alla fine del 2001 viene introdotto un nuovo standard, 802.11g che consente velocità fino a 54Mbps nella banda 2.4Ghz
- Tutte le versioni 802.11x sono backward compatibili con l'originale 802.11
 - 802.11b and 802.11g sono compatibili tra loro ma non con lo standard 802.11a



Sicurezza su reti 802.11

- In una rete cablata, almeno fino ad un certo punto, possiamo supporre che sia delegare tutti gli aspetti di sicurezza al controllo dell'accesso fisico al canale
 - Se solo gli utenti abilitati possono fisicamente connettersi al canale, parte dei problemi di sicurezza spariscono
- Su reti wireless non esiste un canale “cablato”, chiunque può intercettare la comunicazione radio e/o occupare il canale
 - Occorrono meccanismi per gestire tanto l'autenticazione quanto la confidenzialità e l'integrità della comunicazione
- Per la confidenzialità (privatezza) dei dati trasmessi, lo standard prevede l'uso di connessioni criptate secondo il protocollo WEP



WEP: Wired Equivalent Privacy

- Il WEP è un algoritmo di cifratura che usa una chiave segreta K a 40 bit condivisa dai due partner
- Trasmissione
 - La stazione trasmittente genera un vettore di inizializzazione IV (24 bit)
 - L' IV viene concatenato alla chiave K per ottenere il seme da utilizzare per inizializzare un generatore pseudocasuale di numeri PRNG
 - Il PRNG viene utilizzato per generare una sequenza di bit S di lunghezza pari al pacchetto da crittografare (CRC incluso)
 - Il pacchetto viene crittografato tramite XOR bit a bit tra S e il pacchetto stesso
 - Al risultato viene attaccato l' IV e il tutto viene inviato
- Ricezione
 - Il ricevente appende l' IV letto alla chiave K a lui nota e inizializza il proprio PRNG, generando la medesima sequenza S del trasmittente
 - Il pacchetto (CRC incluso) viene decrittato tramite XOR bit a bit tra S e il pacchetto ricevuto
 - Si sfrutta la proprietà dello XOR per cui: $A \oplus B \oplus B = A$



Limiti della sicurezza in 802.11

- La chiave di 40 bit è troppo piccola
- Il meccanismo dell'IV tenta di far sì che la chiave effettivamente utilizzata cambi spesso
 - D'altra parte, l'IV può anche cambiare per ogni pacchetto ma 24 bit sono pochi
 - Collisioni (stesso IV) sono frequenti
- Questo, accoppiato con l'intrinseca debolezza dello schema basato su XOR rende relativamente facile individuare la chiave
- Per questo sono stati introdotti meccanismi alternativi
 - WEP a 128 bit
 - EAP – Extensible Authentication Protocol (MD5 o TSL)
 - Leap e Peap (proprietarie Cisco)



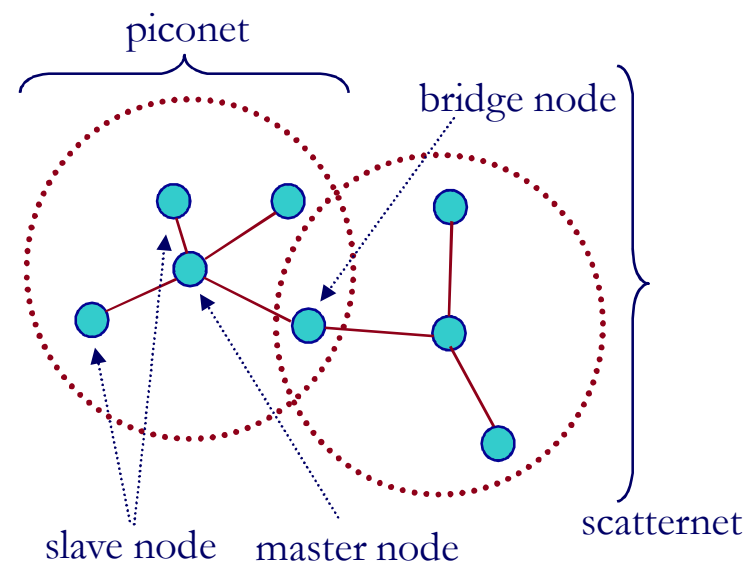
Bluetooth

- Nel 1998 viene istituito il consorzio Bluetooth (soprannome di un re danese del X secolo) con Ericsson, Nokia, IBM, Toshiba, Intel
 - Obiettivo del consorzio è sviluppare una tecnologia di trasmissione radio standard per permettere la comunicazione “plug & play” di periferiche “personali” diverse (PDA, notebook, cellulari, auricolari, ...) con bassi costi (soluzione “single chip”) e bassi consumi
- Nel 1999 viene definita la prima specifica su Bluetooth, per interconnessione di periferiche diverse in “ambito utente”
 - La versione attuale, Bluetooth 1.1, è del febbraio 2001
- Viene superato il problema del “Line of Sight” dei canali IrDA
- Supporta anche comunicazioni punto-multipunto



Piconet e scatternet

- Una *piconet* rappresenta un insieme di device che occupano lo stesso canale (vedi dopo)
- L'accesso al canale è regolato da un master (di norma il primo nodo a presentarsi)
 - Slave diversi sono identificati da un id a 3 bit
 - Considerando un indirizzo di broadcast sono possibili fino a 7 slave
- Piconet diverse possono avere range che si sovrappongono
- Due o più piconet interfacciate tramite un nodo “bridge” costituiscono una *scatternet*





Bluetooth: Livello fisico

- Opera nella banda 2.4 GHz ISM
- Usa una codifica tramite modulazione di frequenza che ogni $625\mu\text{s}$ cambia portante ciò per ridurre interferenze con WLAN, etc
- Sono possibili fino a 12 piconet che non interferiscono nella stessa area
- Supporta tanto canali dati quanto canali voce:
 - 721 Kbps per i dati + 3 canali voce
 - Il throughput effettivo può essere molto minore per l'overhead delle informazioni di controllo e perchè i canali voce hanno priorità su quelli dati
- La potenza varia tra 1mW e 100mW e viene regolata al minimo possibile sotto il controllo del master della piconet
 - Il range trasmissivo è intorno ai 10m



Bluetooth: Altri dettagli

- Il livello trasmissivo prevede l'uso di diversi meccanismi per la gestione dell'errore
 - Un codice di forward error correction
 - Un meccanismo a ritrasmissione con acknowledge e negative acknowledge
- Lo stack Bluetooth prevede canali PPP, IP (TCP/UDP) e voce (modulazione PCM)
- Sono definiti dallo standard meccanismi di autenticazione e crittografia



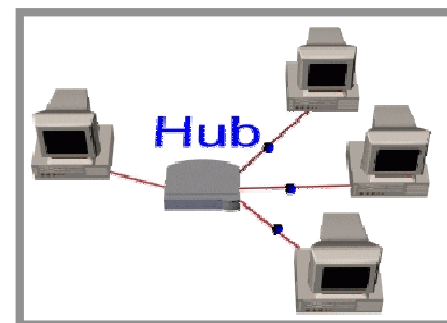
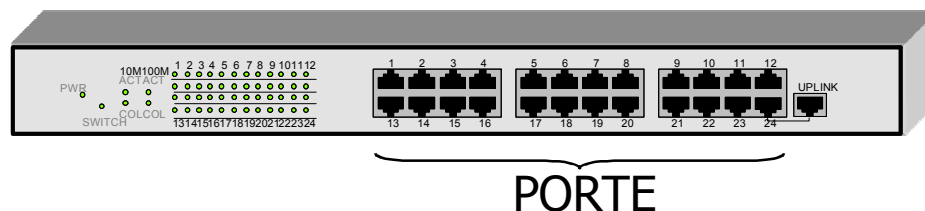
I dispositivi: la scheda di rete

- Tutti i PC, per essere connessi ad una rete, devono essere dotati di *schede di rete*
 - Possono essere schede separate o integrate nella scheda madre
- Nello scegliere una scheda di rete, è necessario considerare:
 - Il protocollo supportato: Ethernet, Fast Ethernet, GigaEthernet, WiFi
 - Il tipo di collegamento necessario: RJ-45 per doppino, BNC per cavo coassiale



I dispositivi: l'hub

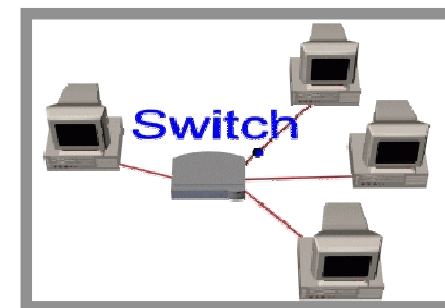
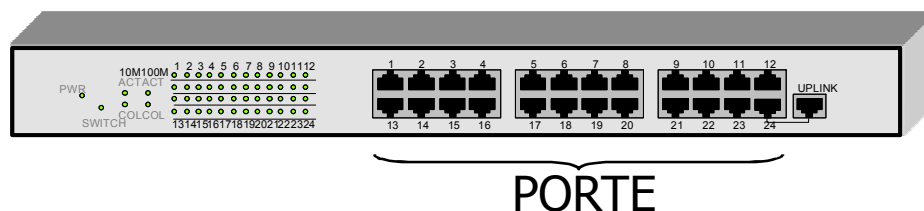
- Con il termine hub ci si riferisce ad un componente dell'apparecchiatura di rete che collega assieme i PC fungendo da ripetitore: ripete tutte le informazioni che riceve, a tutte le porte
 - Una rete logicamente a bus, come Ethernet, viene, per comodità, cablata secondo uno schema a stella usando un'hub
- Gli hub sono adatti alle piccole reti; per le reti con elevato livello di traffico si consiglia un'apparecchiatura supplementare come lo switch capace di suddividere la rete in più tronconi isolati





I dispositivi: lo switch

- Apparentemente simili agli hub, gli switch si avvalgono degli indirizzi di ciascun pacchetto per gestire il flusso del traffico di rete separando ogni troncone
 - Monitorando i pacchetti che riceve, uno switch "impara" a riconoscere l'indirizzo dei dispositivi che sono collegati alle proprie porte per poi inviare i pacchetti solamente alle porte pertinenti
 - Lo switch riduce la quantità di traffico non necessario, dato che le informazioni ricevute nella porta vengono trasmesse solo al dispositivo con il giusto indirizzo di destinazione e non, come negli hub, a tutte le porte
- Gli switch e gli hub vengono spesso utilizzati nella stessa rete. Gli hub ampliano la rete fornendo un numero maggiore di porte, mentre gli switch dividono la rete in sezioni più piccole e meno congestionate





I dispositivi: il router (o gateway)

- Anche i *router* sono ‘smistatori di traffico’ che ricevono dati e li inviano da qualche altra parte. Vengono generalmente utilizzati per collegare tra loro reti con tecnologia diversa
 - Gli switch collegano reti ethernet a reti ethernet, i router possono collegare reti diverse, ad esempio ethernet e wi-fi oppure ethernet e adsl
- I router sono particolarmente intelligenti:
 - Basandosi su una mappa di rete denominata “tabella di routing”, i router possono fare in modo che i pacchetti raggiungano le loro destinazioni attraverso i percorsi più efficaci
 - Se cade la connessione tra due router, per non bloccare il traffico, il router sorgente può definire un percorso alternativo
- Quando i router connettono la rete interna con la rete esterna, vengono anche chiamati gateway



I dispositivi: il modem

- Il modem è un dispositivo che va collegato direttamente al computer (es. via USB) e che si avvale della linea telefonica per effettuare una connessione di rete dial-up (ad es. verso un servizio online o un ISP)
- Il compito essenziale di un modem è di convertire i dati digitali necessari al computer in segnali analogici per la trasmissione attraverso la linea telefonica, e viceversa
- I modem tradizionali supportano velocità fino a 56Kbps
- Negli ultimi anni si sono diffusi i modem ADSL che supportano velocità molto più elevate (anche 12 Mbps)



Indice

- Nozioni essenziali
 - Topologia di rete e supporti fisici
 - Segnalazione, modulazione e trasmissione
 - Indirizzamento e commutazione
 - Il concetto di protocollo
- Le reti locali
 - Protocolli per reti cablate: Ethernet, ppp
 - Protocolli per reti wireless: 802.11, bluetooth
 - I dispositivi per reti locali
- **Le reti geografiche**
 - **Internet e il protocollo TCP/IP**
 - **I protocolli applicativi: telnet, ssh, ftp, smtp, pop, mime**
- Cenni di sicurezza informatica



Internet: "la rete delle reti"

- Internet: una rete *aperta*...
- ...*logicamente* formata da decine di milioni di calcolatori *direttamente* collegati tra loro...
- ... attraverso l'adozione di un unico insieme di protocolli per i livelli intermedi: il protocollo TCP/IP.
- I protocolli dei livelli più bassi possono essere diversi...
- ... e lo stesso vale per i protocolli dei livelli superiori, anche se si sono venuti a formare degli standard di fatto



Storia di Internet

- Fine anni '60:
 - la Advanced Research Project Agency (ARPA) sviluppa ARPANET con l'obiettivo di connettere laboratori di ricerca, università e enti governativi
- 1970
 - L'università delle Hawaii, su commessa dell'ARPA sviluppa ALOHAnet, la prima rete a commutazione di pacchetto
- 1971
 - ARPANET include 23 host
- 1973
 - ARPA diventa DARPA (Defence ...)
 - ARPANET collega per la prima volta un sito europeo (l'University College di Londra)
- Fine anni '70:
 - DARPA finanzia lo sviluppo di protocolli a commutazione di pacchetto
 - Nasce TCP/IP
 - Nel 1982 ARPANET si “converte” a TCP/IP

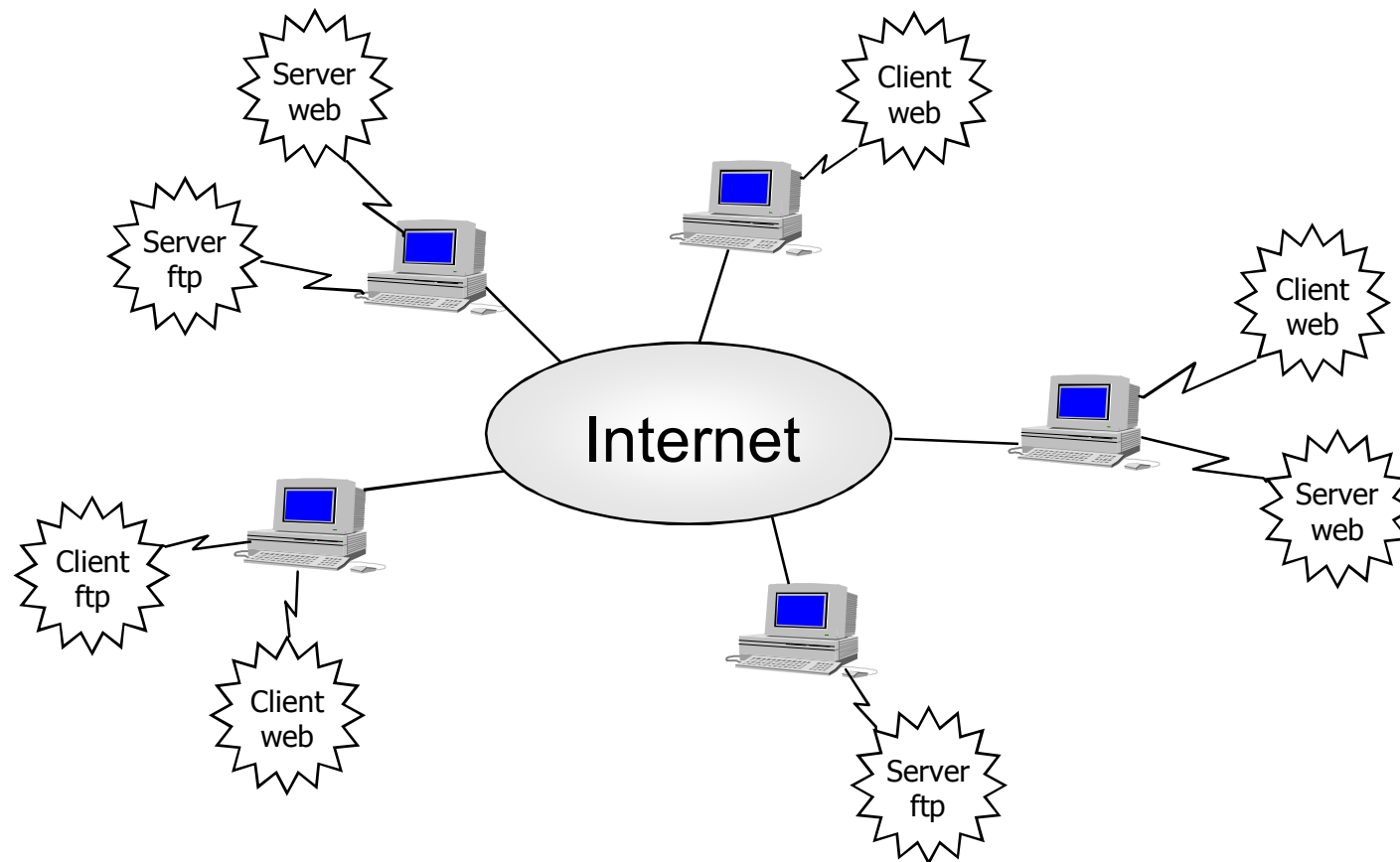


Storia di Internet

- Anni '80
 - Nel 1983 la conversione a TCP/IP è completa
 - MILNET (rete governativa e militare) si separa da ARPANET (1983)
 - Nel 1984 nasce il primo DNS
 - DARPA finanzia lo sviluppo di Berkeley UNIX (implementazione di TCP/IP che introduce l'astrazione dei socket)
 - ARPANET diventa un sottoinsieme di Internet
 - La National Science Foundation (NSF) realizza una rete di supercomputer (NSFNET) che agisce come backbone di Internet (1985)
 - Nel 1987 si stima che Internet connettesse oltre 10.000 computer
 - Due anni dopo (nel 1989) si stima che Internet connettesse oltre 100.000 computer
- Anni '90:
 - Il 28 Febbraio 1990 ARPANET viene definitivamente abbandonata (la rete è ormai “governata” dalla NSF)
 - Nel 1991 NSF decide di rimuovere i vincoli che impediscono attività commerciali su NSFNET
 - Nello stesso anno il CERN di Ginevra sviluppa il www (html, http e url)
 - Internet esplode e cresce con ritmi velocissimi (dimensioni e traffico)

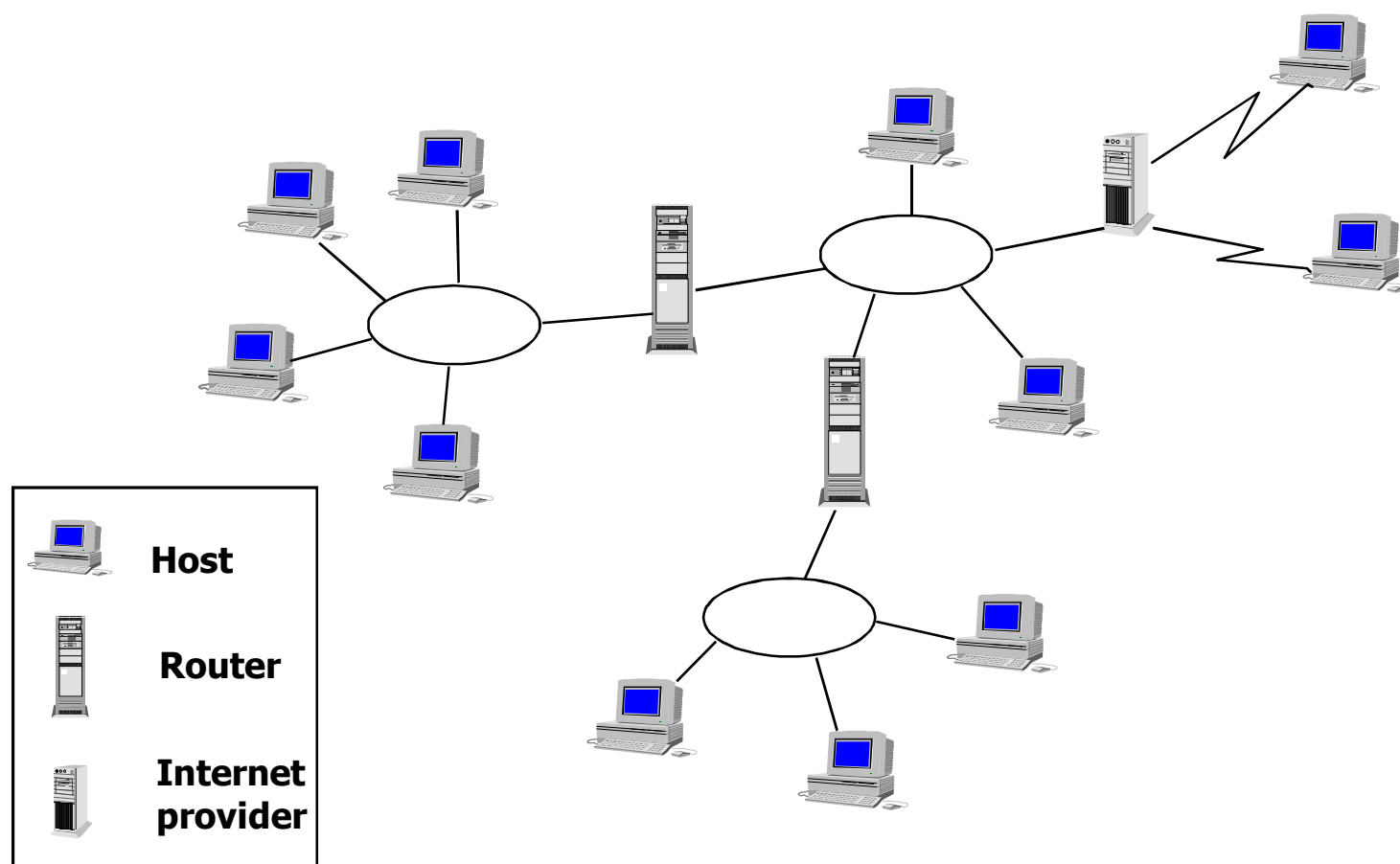


Internet: architettura logica





Internet: architettura fisica

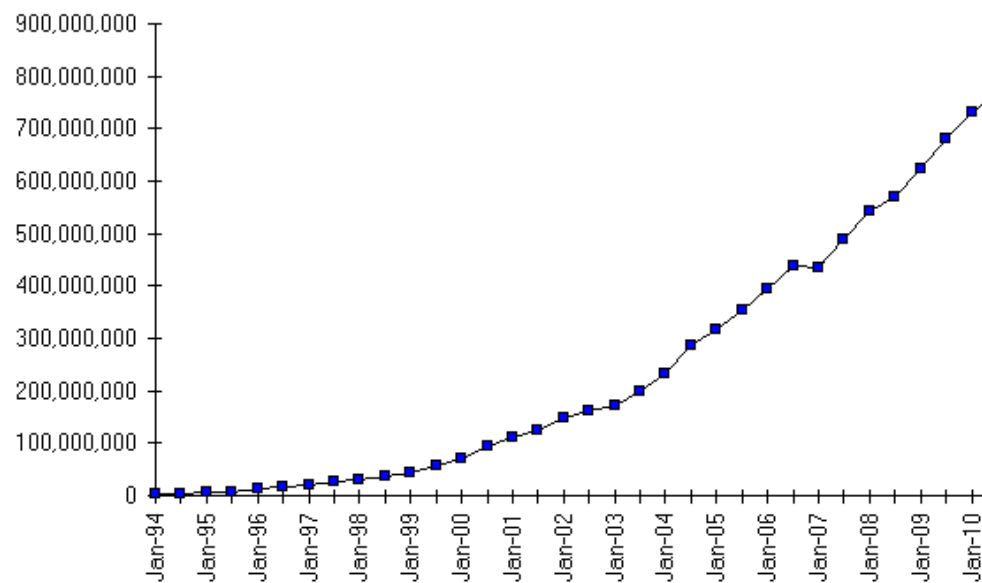




Internet: Hosts

Date	Hosts
Dec 1979	188
July 1989	130,000
July 1999	56,218,000
July 2001	125,888,197
July 2003	171,638,297
July 2005	353,284,187
July 2006	439,286,364
July 2007	489,774,269
July 2008	570,937,778
July 2009	681,064,561
July 2010	768,913,036

Internet Domain Survey Host Count



Source: Internet Systems Consortium (www.isc.org)

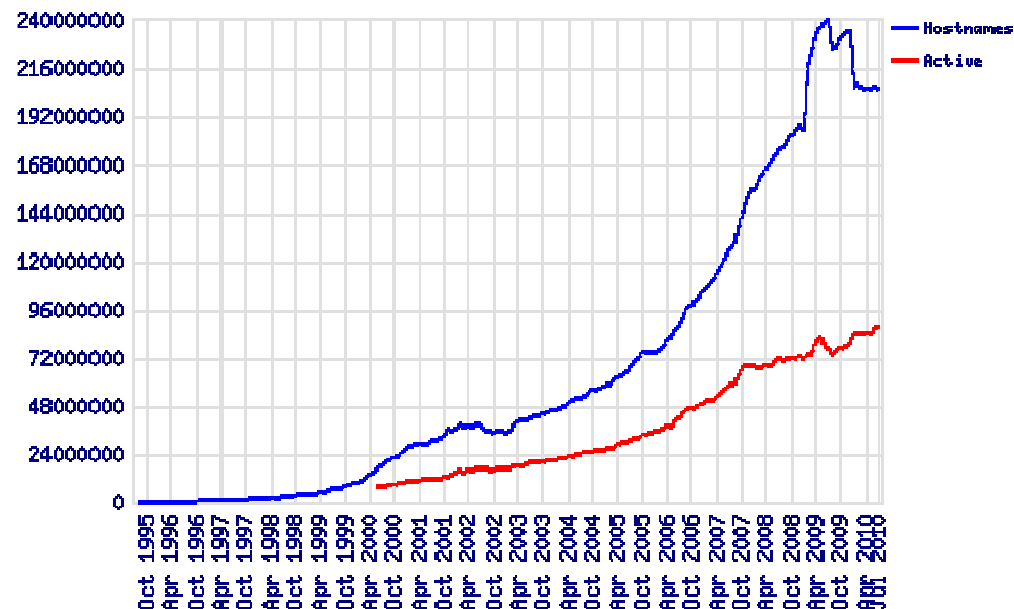
Source: Internet Systems Consortium



Politecnico
di Milano

Internet: Web servers

Date	Hosts	Web servers	%
July 1993	1,776,000	130	0.008
July 1995	6,642,000	23,500	0.4
July 1997	19,540,000	1,203,096	6
July 1999	56,218,000	6,598,697	12
July 2001	125,888,197	31,299,592	25
July 2003	212,570,000	42,298,371	20
July 2005	353,284,187	67,571,581	19
July 2006	439,286,364	88,166,395	20
July 2007	489,774,269	125,626,329	39
July 2008	570,937,778	175,480,931	33
July 2009	681,064,561	239,611,111	35
July 2010	768,913,036	205,714,253	27



Source: Netcraft web server survey

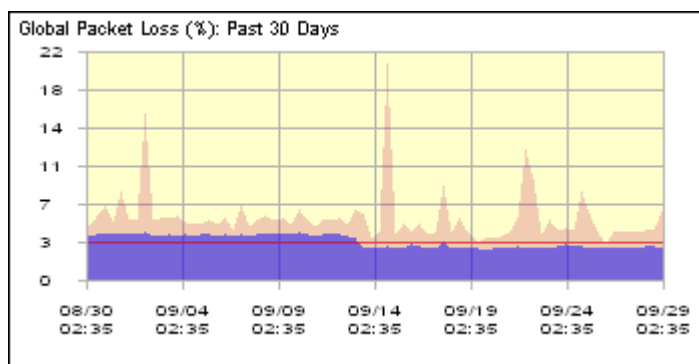
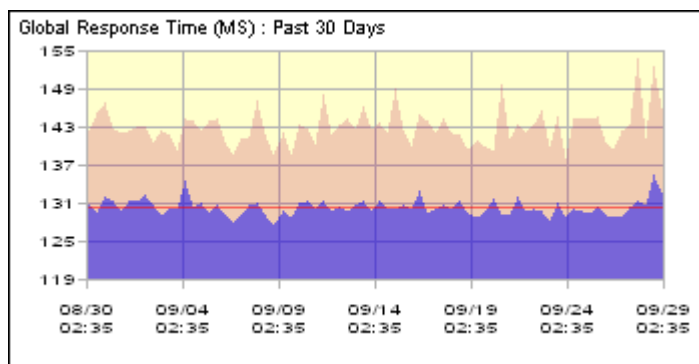
Elementi di Informatica e Reti di Calcolatori



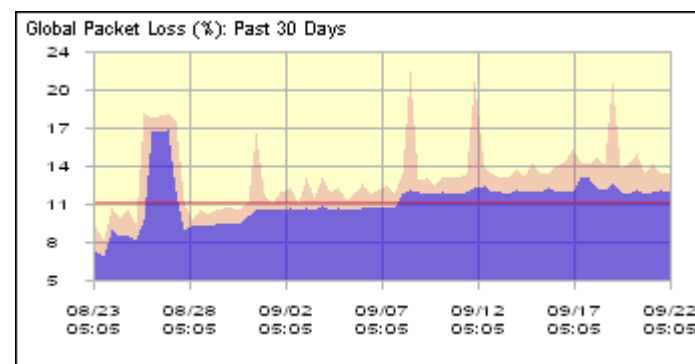
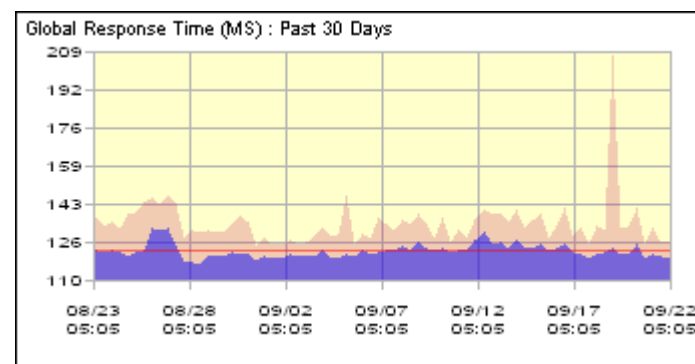
Politecnico
di Milano

Internet: Prestazioni

2010



2011



Legenda

red=max

purple=avg

Source: Internet Traffic Report



Siti top e traffico

Site	% of users visiting 22/9
google.com	44.61
facebook.com	36.19
youtube.com	23.65
yahoo.com	26.68
windows live (live.com)	14.96
wikipedia.org	13.74

Source: Alexa survey

Top 10 Global Web Parent Companies, Home & Work

August 2010

RANK	PARENT	UNIQUE AUDIENCE (000)	ACTIVE REACH %
1	GOOGLE	205,814,883	87.79%
2	MICROSOFT	180,098,857	76.82%
3	FACEBOOK	118,840,955	50.69%
4	YAHOO!	100,511,198	42.87%
5	EBAY	95,426,342	40.70%
6	WIKIMEDIA FOUNDATION	87,394,392	37.28%
7	AMAZON	54,444,795	23.22%
8	APPLE COMPUTER	49,831,728	21.26%
9	TELEFONICA/TERRA	45,830,250	19.55%
10	INTERACTIVECORP	43,291,706	18.47%

Source: Nielsen NetView

Top 10 U.S. Search Providers, Home & Work

August 2010

RANK	PROVIDER	SEARCHES (000)	SHARE OF SEARCHES
-	ALL SEARCH	9,199,567	100.0%
1	GOOGLE SEARCH	5,988,996	65.1%
2	MSN/WINDOWS LIVE/BING SEARCH	1,274,184	13.9%
3	YAHOO! SEARCH	1,208,774	13.1%
4	ASK.COM SEARCH	196,875	2.1%
5	AOL SEARCH	179,895	2.0%

Source: Nielsen MegaView Search



Internet vs. Intranet

- *Internet*: rete globale caratterizzata dall'uso dei protocolli TCP/IP
- *Intranet*: rete locale caratterizzata dall'uso dei medesimi protocolli di Internet
- Il boom di Internet ha favorito lo sviluppo di centinaia di applicazioni distribuite basate su TCP/IP
- Ciò ha reso conveniente l'uso dei protocolli TCP/IP anche in ambito locale
- Attualmente la maggior parte delle reti locali sfrutta TCP/IP come protocollo base



Internet Protocol Suite

ISO/OSI

Application
Presentation
Session
Transport
Network
Data Link
Physical

Internet Protocol Suite

Telnet	NFS
FTP	Web-NFS
SMTP	
HTTP	RPC
TCP e UDP	
IP e Protocolli di routing	
Non specificati (Ethernet, PPP, X.25, Frame Relay, ATM, ...)	



Il protocollo IP

- Caratteristiche:
 - protocollo connectionless
 - si occupa dell'instradamento e della rilevazione d'errore (nessuna correzione)
- Non si assicura:
 - la consegna,
 - l'integrità,
 - la non-duplicazione
 - l'ordine di consegna
- IP si può appoggiare ad una varietà di protocolli di più basso livello, quali Ethernet, PPP, X.25, Frame Relay, ATM, ...



Gli indirizzi IP

- Ogni host possiede un indirizzo IP *unico* per ogni interfaccia di rete
- Gli indirizzi IP sono formati da 32 bit, suddivisi in una parte che individua una sottorete ed in una porzione che identifica un nodo particolare della sottorete
- La divisione dipende dalla *classe* della sottorete, definita nei primi bit dell'indirizzo
 - *Classe A* (0): NetId = 7 bit (128 reti), HostId = 24 bit (16777216 host)
 - *Classe B* (10): NetId = 14 bit (16384 reti), HostId = 16 bit (65536 host)
 - *Classe C* (110): NetId = 21 bit (2097152 reti), HostId = 8 bit (256 host)
 - *Multicast* (1110): indirizzo multicast
- I router hanno due o più indirizzi IP diversi ed una tabella di instradamento



Gestione degli indirizzi

- L'uso di assegnare reti di classe A o B a compagnie che usano un ridotto sottoinsieme degli indirizzi rischia, oggi, di portare all'esaurimento degli indirizzi disponibili
- Sono state proposte diverse soluzioni ad hoc che consentono di “recuperare” parte degli indirizzi perduti...
- ... ma l'unica vera soluzione si avrà con il passaggio a IPv6 che userà 128 bit per gli indirizzi
 - $340.282.366.920.938.463.463.374.607.431.768.211.456 = 3,4 \times 10^{38}$ indirizzi distinti
 - Si calcola che saranno disponibili 1.564 indirizzi IP per ogni metro quadrato di superficie terrestre



Ancora sugli indirizzi IP (v4)

- Gli indirizzi IP si scrivono come quattro interi separati da punti
 - Esempio: 131.175.5.25
- L'indirizzo 127.0.0.1 rappresenta l'interfaccia di loopback
 - Indirizzo “fittizio” associato alla macchina corrente



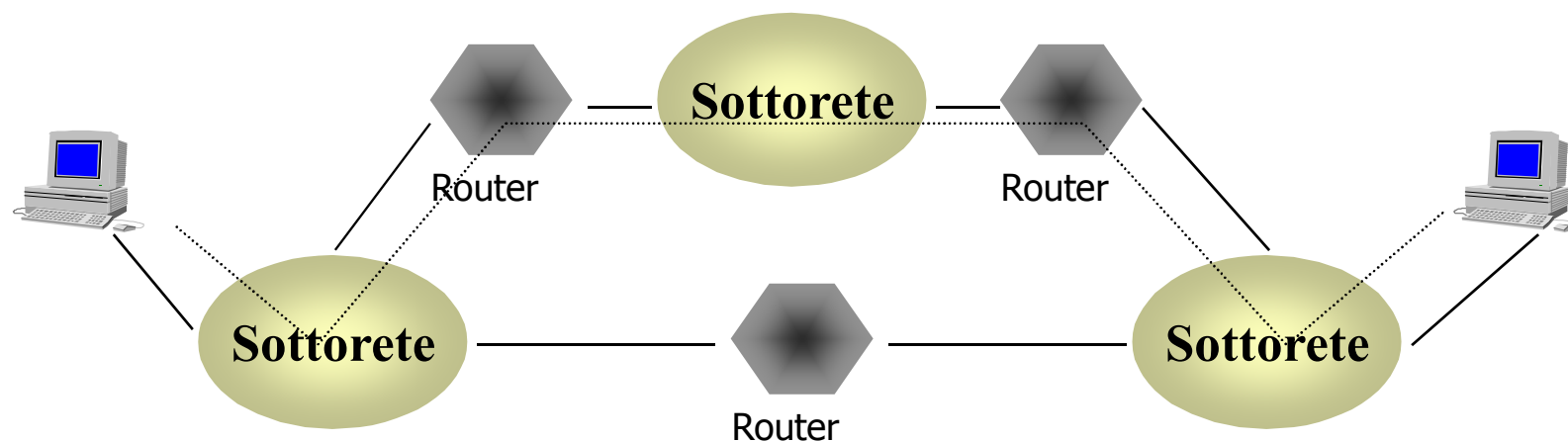
Indirizzi privati

- Gli indirizzi IP vengono gestiti dalla Internet Assigned Numbers Authority che collabora con strutture regionali (Europa, America, Asia)
- Alcune aziende non potendo/volendo chiedere un set di indirizzi IP scelgono indirizzi a caso
 - In questo caso tali indirizzi non dovranno essere visibili da reti esterne (si usa il meccanismo dell'*IP masquerading*)
- L'RFC 1597 definisce quali siano i set di indirizzi da usare in questo caso. Questi indirizzi non verranno mai assegnati a nessuna azienda o organizzazione



Instradamento - 1

- I datagrammi IP vengono trasportati dal nodo mittente al nodo destinatario attraverso molteplici nodi intermedi (*router*)





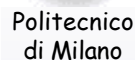
Instradamento - 2

- I nodi attraverso cui il pacchetto compie il suo percorso (*route*) vengono determinati usando le tabelle di routing
 - Le tabelle possono essere determinate staticamente
 - Le tabelle possono essere aggiornate dinamicamente dai protocolli di routing (ad es. RIP)
- Se lo host destinatario è direttamente collegato allo host mittente, il datagramma viene incapsulato in un pacchetto di più basso livello (es. ethernet) e consegnato direttamente
- Se lo host destinatario è localizzato in un'altra rete, il datagramma viene passato ad un router che si occuperà di consegnarlo, seguendo un processo analogo





Address Resolution Protocol

- ARP è il protocollo che permette di mappare indirizzi IP con indirizzi hardware delle interfacce (ad esempio, con gli indirizzi Ethernet)
- Quando uno host A vuole conoscere l'indirizzo hardware associato ad un indirizzo I_b esegue il broadcast di un messaggio speciale
- Lo host B che possiede l'indirizzo I_b risponde con un messaggio contenente il proprio indirizzo hardware
- La risposta viene mantenuta, da A , in una cache locale
- Per ottimizzare le prestazioni del protocollo, quando A esegue la richiesta, include anche il suo indirizzo IP



Gli indirizzi simbolici ed i DNS

- Un indirizzo simbolico può sostituire un indirizzo IP
- Un indirizzo simbolico è composto da un nome di dominio e da un nome di host
 - esempio:

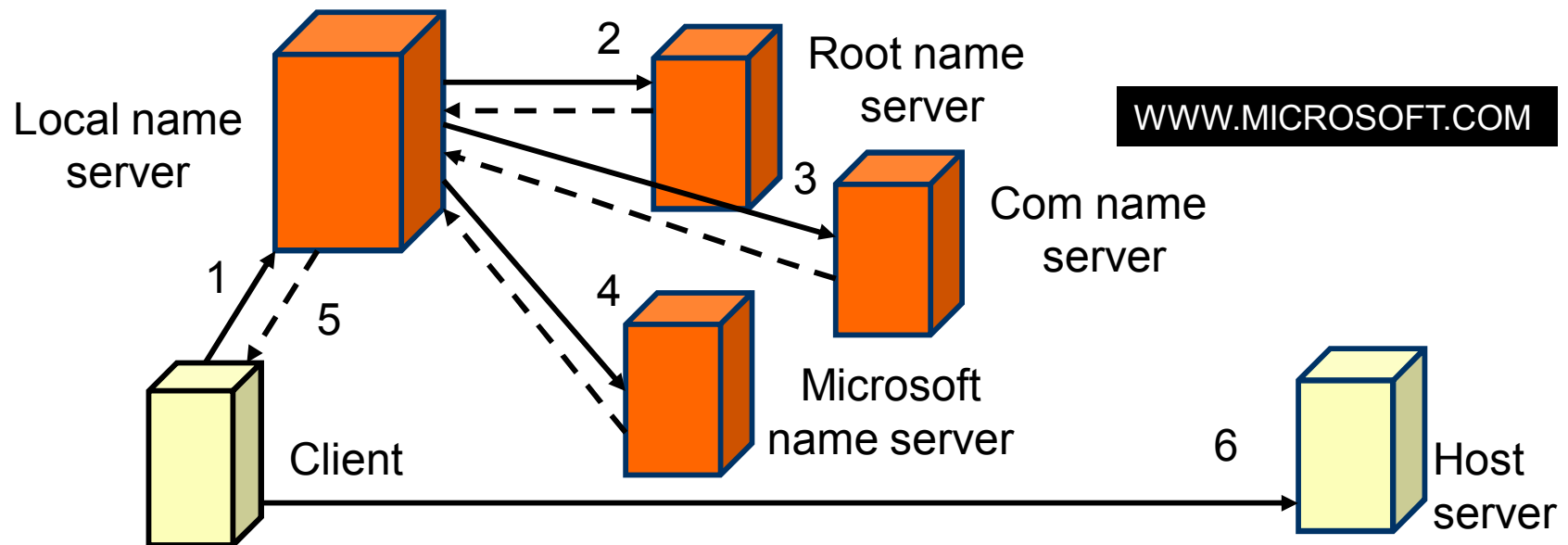
www	.polimi	.it	elet	.polimi	.it
					
host dominio			host dominio		
- I nomi di dominio vengono assegnati da un'autorità nazionale, chiamato Network Information Center (per l'Italia gestito dal CNR) che coopera con altre autorità simili
- **I Domain Name Servers (DNS):**
 - costituiscono un data base distribuito per i nomi simbolici
 - permettono l'associazione nome simbolico/indirizzo IP
 - esempio:

131.175.21.8	www.polimi.it
131.175.21.1	morgana.elet.polimi.it



Risoluzione dei nomi

- Si chiama risoluzione il processo che trasforma i nomi in indirizzi IP.
- Risoluzione diretta: il DNS utilizza il modello client/server per la risoluzione dei nomi.
- Per risolvere un nome il client fa una richiesta al name server locale; esso risolve il nome se è in grado altrimenti trasferisce la richiesta ad un altro name server.





Il protocollo UDP

- Caratteristiche:
 - Protocollo connectionless a datagrammi
 - Dimensione massima del messaggio 64kbyte
 - Si appoggia al protocollo IP aggiungendo il concetto di *porta*
 - Permette di distinguere tra applicazioni diverse che risiedono sulla stessa macchina
 - Fornisce un servizio di rilevazione d'errore basato su CRC
 - Non assicura la consegna nè, tantomeno, l'ordine di invio (unreliable, best-effort protocol)
- Utilizzato nelle applicazioni client-server di tipo richiesta/risposta
 - Esempio: il DNS



Il protocollo TCP

- Caratteristiche:
 - Protocollo connection-oriented (indirizzo IP - porta TCP)
 - Fornisce un servizio full-duplex, con acknowledge e correzione d'errore
- Due host connessi su Internet possono scambiarsi messaggi di lunghezza qualsiasi attraverso canali TCP
- TCP costituisce l'infrastruttura di comunicazione della maggior parte dei sistemi client-server su Internet



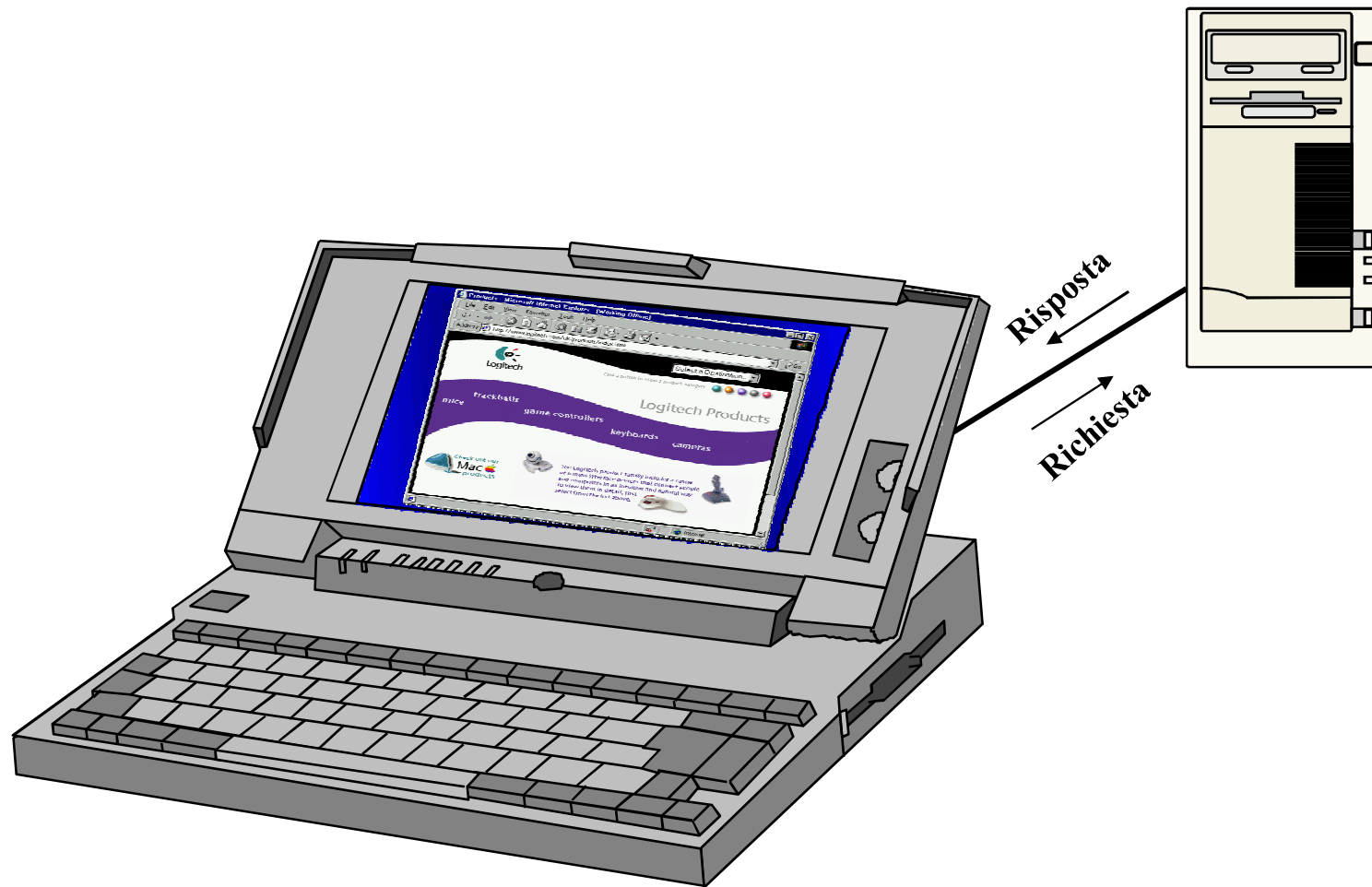
Architettura client/server

- La principale metodologia di utilizzo dei servizi TCP e UDP da parte dell'applicazione utente è detta *client/server*
 - Il server è un calcolatore connesso alla rete su cui gira continuamente un programma in ascolto su di una porta TCP o UDP
 - Uno o più calcolatori denominati client (anche contemporaneamente) possono contattare il server per ottenere servizi. Il dialogo tipico consiste nell'invio di una richiesta e nella attesa della risposta
- Esistono approcci diversi, ad esempio il Peer-to-Peer



Politecnico
di Milano

Il WWW come esempio di applicazione Client/Server





Telnet - SSH

- Permette ad un utente di collegarsi, attraverso il proprio elaboratore locale, come terminale remoto di un altro elaboratore connesso alla rete
- A connessione avvenuta tutti i caratteri battuti sulla tastiera locale vengono inviati all'elaboratore remoto e le risposte da questo generate sono mostrate sullo schermo locale
- Sfrutta una connessione TCP (porta 23) tra elaboratore locale e remoto
- Tutti i comandi digitati dal client (compresa la password per l'identificazione dell'utente) viaggiano "in chiaro" sulla rete, mettendo a repentaglio la sicurezza e la riservatezza
- Per superare questo problema si e' affermato in questi ultimi anni un nuovo programma per il login remoto in cui la comunicazione avviene in modo cifrato, denominato SSH (Secure SHell).
 - SSH utilizza la porta 22/TCP



FTP (File Transfer Protocol)

- Permette il trasferimento di file tra elaboratori diversi connessi in rete
- Vengono aperte due connessioni TCP per ogni sessione FTP:
 - Una connessione di controllo (porta 20)
 - Una connessione dati (porta 21)
- Il protocollo stabilisce il formato dei comandi e dei messaggi scambiati lungo la connessione di controllo
- FTP include un meccanismo di autenticazione basato su username e password passato dal client al server
 - la login anonymous



SMTP (Simple Mail Transfer Protocol)

- Gestisce l'invio di messaggi di posta elettronica attraverso la rete
- La connessione tra i diversi server di posta avviene attraverso una connessione TCP (porta 25)
- Ogni utente é identificato dall'indirizzo:
nomeutente@indirizzo_host
- Il processo di invio é batch

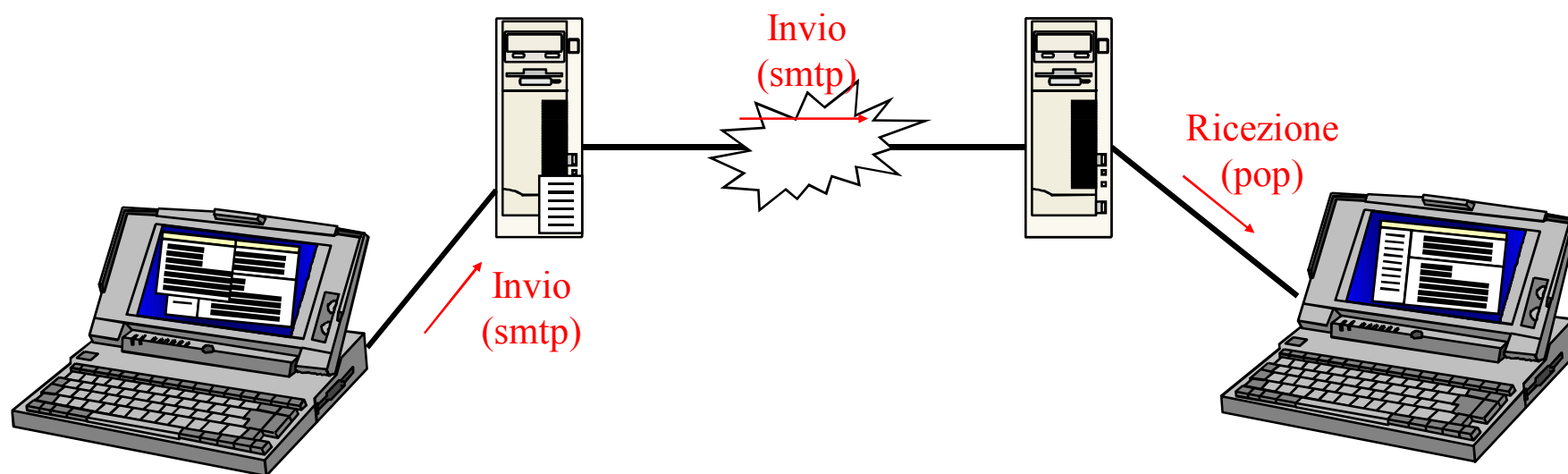


POP (Post Office Protocol)

- Protocollo per la lettura della propria posta da un mail server
- Sfrutta una connessione TCP sulla porta 110
- Fornisce comandi per avere la lista dei propri messaggi, scaricare un messaggio dal server al client, cancellare un messaggio dal server
- L'autenticazione è basata su una coppia “username-password” che viene scambiata in chiaro tra client e server



SMTP e POP: il funzionamento della posta su Internet





MIME

- Multi-purpose Internet Mail Extension
- Definizione di un formato per i messaggi multimediali
- Superamento della RFC 822 che definisce lo standard per i messaggi testuali su Internet (linee brevi di caratteri ASCII a 7 bit)
- Progettato per essere facilmente estendibile
- Versione corrente 1.0
 - RFC 1521-1522



Struttura di un messaggio MIME

- Header
 - `MIME-Version`: specifica la versione dello standard MIME (ad es. 1.0)
 - `Content-Type`: descrive il tipo dei dati contenuti nel body
 - `Content-Transfer-Encoding`: descrive il formato di codifica del messaggio
 - `Content-ID`: identifica univocamente il messaggio
 - `Content-Description`: descrive il contenuto in linguaggio naturale
- Body
- Header e Body sono separati da una linea vuota



Content-Type

- Type: specifica il tipo generale dei dati
- Subtype: specifica il tipo particolare
- Attributi: parametri espressi con coppie attributo=valore dipendenti dal particolare tipo/sottotipo
- È stato definito un insieme iniziale di tipi/sottotipi
- Estensioni a questo set devono essere richieste all'IANA (Internet Assigned Numbers Authority)
- Estensioni non-standard devono essere nominate con un prefisso "X-"



Tipi predefiniti

- `text`: testo
- Attributi:
 - `charset`: set di caratteri utilizzato
- Sottotipi:
 - `plain`: testo senza formattazione
 - `richtext`: testo con formattazione
 - `html`: testo HTML
- Esempio:
`Content-Type: text/plain; charset=us-ascii`



Tipi predefiniti

- message: messaggio incapsulato
- Sottotipi
 - rfc822: messaggio in formato RFC 822
 - partial: porzioni di messaggi RFC 822 (usato per frammentare messaggi lunghi). I messaggi vengono ricomposti grazie agli attributi id, number, total
 - external-body: riferimento ad una sorgente esterna di dati. Il modo di accesso è definito dall'attributo access-type (ftp, anon-ftp, tftp, afs, local-file, mail-server)

```
From: pippo
To: topolino
MIME-Version: 1.0
Content-Type: message/external-body
name="standard.ps"
site="ftp.waltdisney.com"
access-type=ANON-FTP
directory="pub"
mode="image"

Content-Type: application/postscript
Content-ID: <idd6673662882>
```




Tipi predefiniti

- `multipart`: oggetto costituito da diversi componenti (`body part`).
- Ogni componente possiede uno header e un body separati da una linea vuota, e può essere a sua volta di tipo `multipart`
- Attributi:
 - `boundary`: specifica la stringa usata per separare i diversi componenti
- Sottotipi:
 - `mixed`: diversi sottotipi indipendenti
 - `alternative`: lo stesso dato viene rappresentato in formati diversi
 - `parallel`: le diverse componenti devono essere visualizzate contemporaneamente
 - `digest`: ogni sottoparte è del tipo `message`



Tipi predefiniti

- `image`: immagini
 - Sottotipi
 - `jpeg`: immagini JPEG
 - `gif`: immagini GIF
 - `X-<formato>`: estensione
- `audio`: suoni
 - Sottotipi
 - `basic`
 - `X-<formato>`: estensione
- `video`: filmati
 - Sottotipi
 - `mpeg`: filmato MPEG
 - `X-<formato>`: estensione



Tipi predefiniti

- `application`: dati dipendenti dall'applicazione
- Sottotipi
 - `octet-stream`: dati binari
 - `postscript`: file PostScript
 - `X-<type>`: estensione
 - `application/X-java-applet`
 - `application/X-SafeTcl`



Content-Transfer-Encoding

- Formato di codifica dei messaggi
- 7bit
- quoted-printable
- base64
- 8bit
- binary
- x-<codifica>: estensione
- Esempio

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: base64



Content-ID e Content-Description

- Content-ID
 - Etichetta unica che identifica il messaggio
 - Usato nei messaggi message/external-body
 - Usato per il caching dei messaggi
- Content-Description
 - Testo in linguaggio naturale



Indice

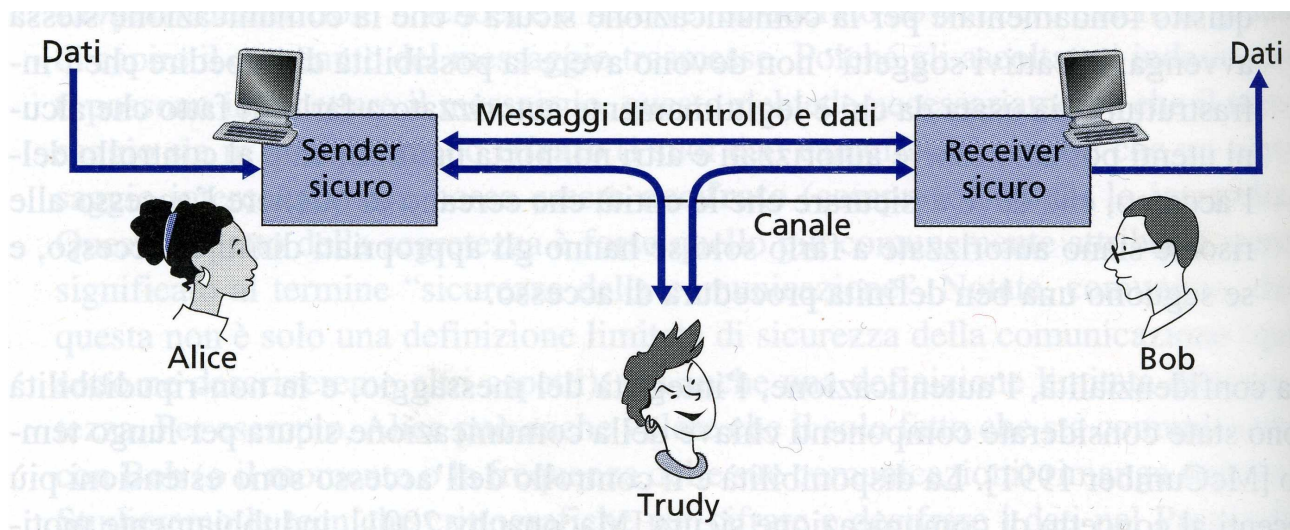
- Nozioni essenziali
 - Topologia di rete e supporti fisici
 - Segnalazione, modulazione e trasmissione
 - Indirizzamento e commutazione
 - Il concetto di protocollo
- Le reti locali
 - Protocolli per reti cablate: Ethernet, ppp
 - Protocolli per reti wireless: 802.11, bluetooth
 - I dispositivi per reti locali
- Le reti geografiche
 - Internet e il protocollo TCP/IP
 - I protocolli applicativi: telnet, ssh, ftp, smtp, pop, mime
- **Cenni di sicurezza informatica**



La sicurezza in rete: proprietà

Alice e Bob vogliono comunicare “in sicurezza”, questo significa che:

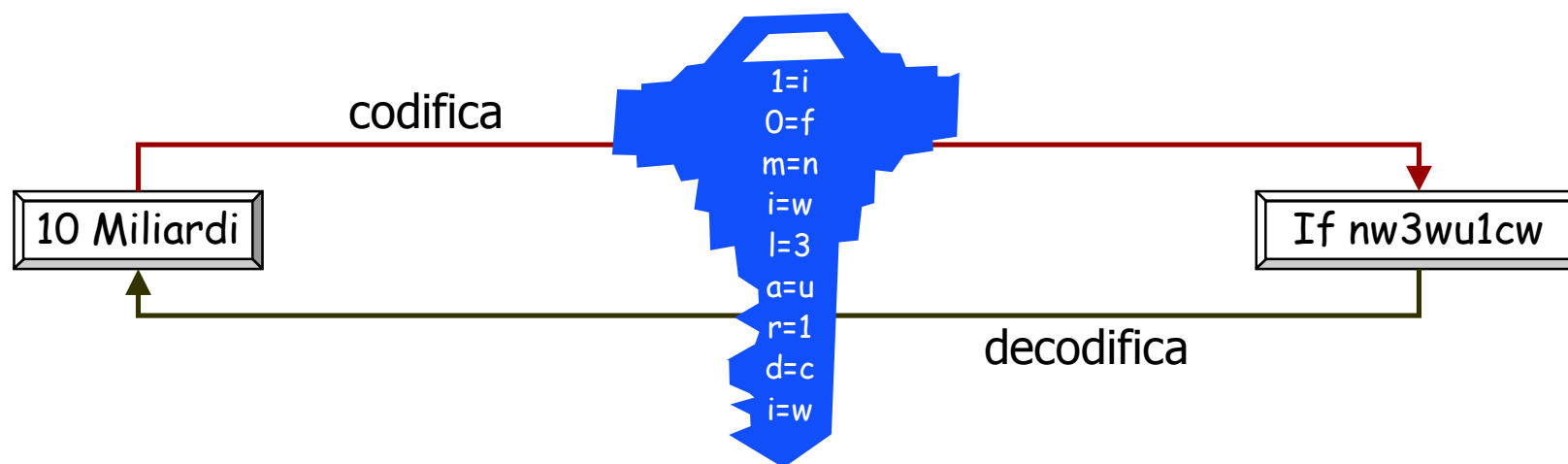
- Alice vuole che solo Bob sia in grado di capire un messaggio da lei spedito (**CONFIDENZIALITA'**), anche se essi comunicano su un mezzo “non sicuro” dove un intruso (Trudy) può intercettare qualunque cosa trasmessa attraverso questo canale
- Bob vuole essere sicuro che il messaggio che riceve da Alice sia davvero spedito da lei e viceversa (**AUTENTICAZIONE**)
- Alice e Bob vogliono essere sicuri che i contenuti del messaggio di Alice non siano alterati nel transito (**INTEGRITA' DEL MESSAGGIO**)





La crittografia: definizione

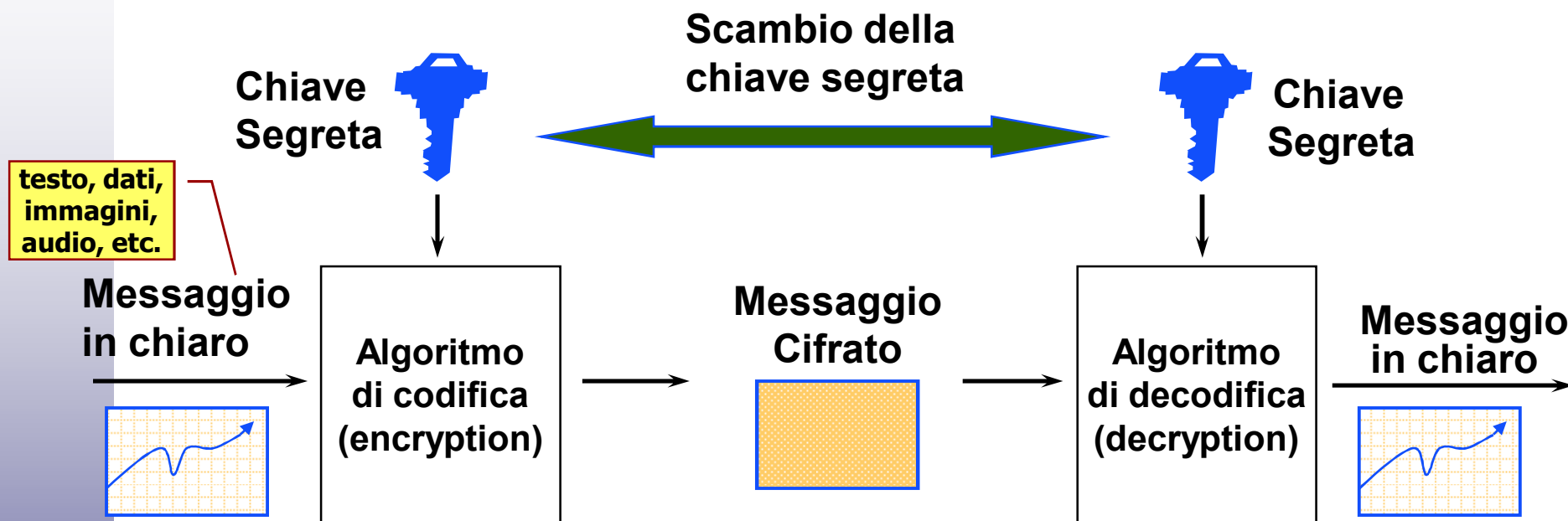
- Arte di proteggere il segreto di un testo mediante una scrittura convenzionale conosciuta solo da chi scrive e da chi legge.



- È costituita dalla combinazione di:
 - un algoritmo di crittografia (generalmente pubblico)
 - un'informazione segreta (chiave) in grado di personalizzare l'algoritmo



Crittografia simmetrica (a chiave segreta)



- Caratteristica peculiare degli algoritmi di crittografia simmetrica è che la codifica e la decodifica avvengono utilizzando la stessa chiave k :

$$D(k, E(k, m)) = m$$

- m = messaggio
- k = chiave
- E = algoritmo di codifica
- D = algoritmo di decodifica

Crittografia simmetrica

Esempio (banale): Codice di Cesare

- Algoritmo di sostituzione: ad ogni carattere si sostituisce un altro carattere, secondo una tabella di conversione.

– Esempio (Codice di Cesare):

Carattere cifrato = carattere in chiaro + shift (chiave)

Benvenuti al Politecnico

Chiave: +5



Gjsajszyn fq Utqnyjhsnht

a	b	c	d	e	f	g	h	..
<i>Shift = +5</i>								
f	g	h	i	j	k	l	m	..

- Noto l'algoritmo, è facilmente “crackabile”: sono sufficienti 26 tentativi

Crittografia simmetrica

Esempio (banale): Codice di Cesare

- Se non sono noti l'algoritmo e la chiave, il numero di sostituzioni possibili è pari a $26! = 4,03 \cdot 10^{26}$

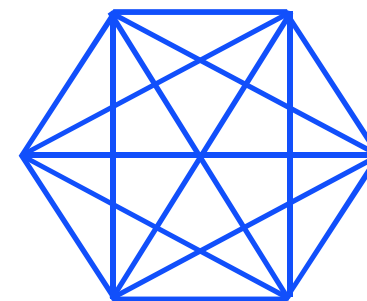
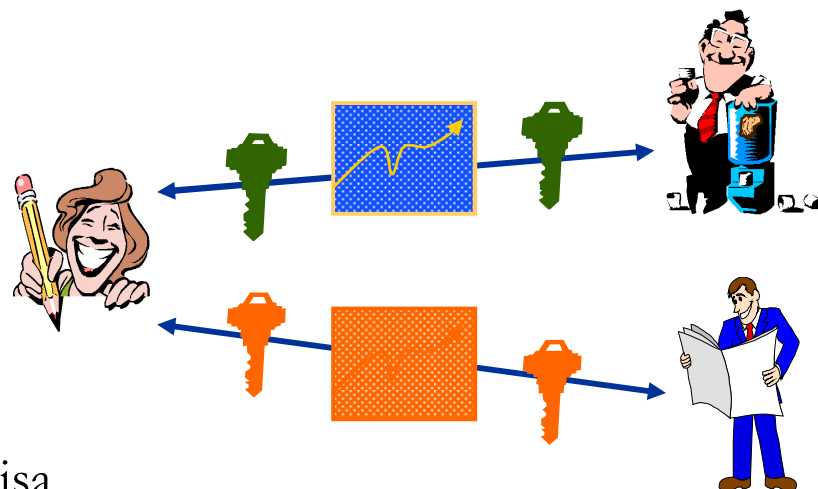
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
													↓												
U	W	G	R	P	N	Q	S	B	J	X	M	E	C	A	I	Z	O	Y	T	D	F	H	K	L	V

- Difficilmente crackabile con **metodi a forza bruta (brute force)**: con gli elaboratori più potenti richiederebbe comunque un tempo di alcuni secoli
- E' però facilmente crackabile con analisi statistica delle ricorrenze dei caratteri nel testo



Crittografia simmetrica: Vantaggi e svantaggi

- Vantaggi
 - semplicità e rapidità di esecuzione degli algoritmi crittografici
- Svantaggi:
 - scambio della chiave segreta: la comunicazione della chiave condivisa deve avvenire attraverso un canale sicuro;
 - è necessaria una chiave diversa per ogni coppia di interlocutori (per evitare che l'interlocutore C possa leggere i messaggi mandati a B).
 - per n coppie di interlocutori sono necessarie $n(n-1)/2$ chiavi simmetriche distinte



Crittografia asimmetrica (a chiave pubblica)

- Ogni utente ha una coppia di chiavi, distinte ma legate fra loro:



- la **chiave pubblica**, k_{pub} , divulgabile a tutti
- la **chiave privata**, k_{pri} , conosciuta e custodita dal solo proprietario

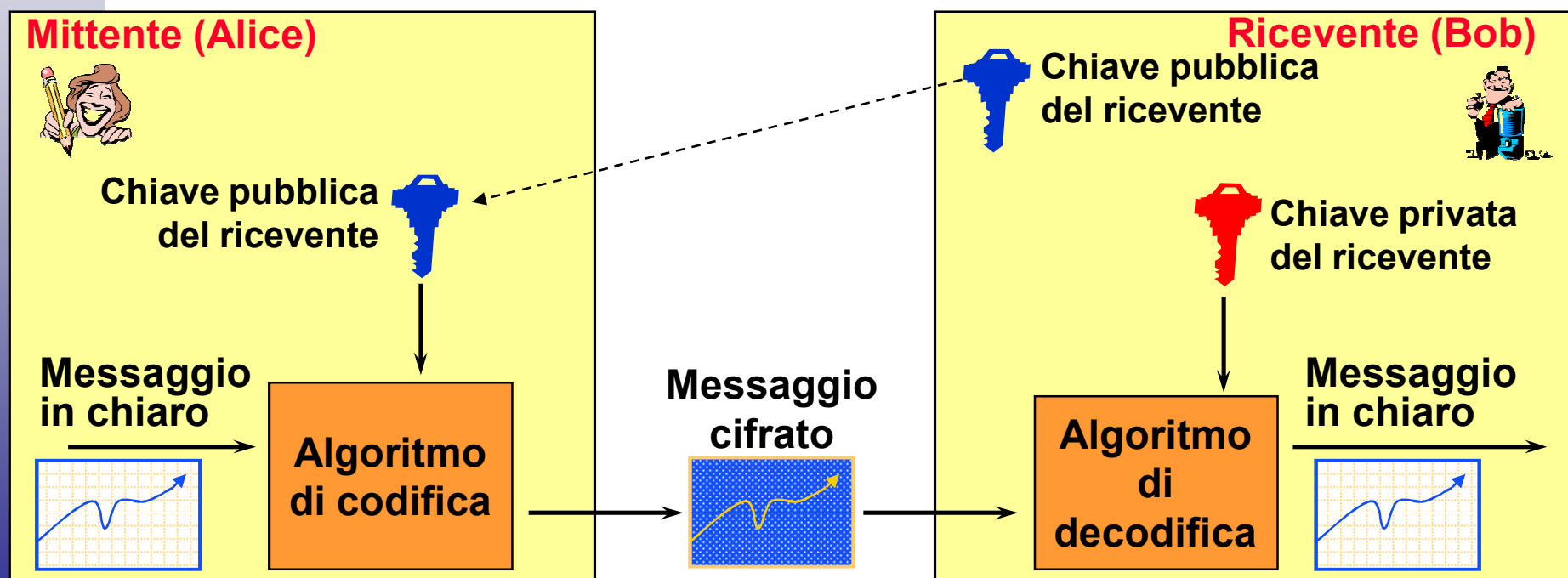
- Caratteristiche dell'algoritmo di cifratura:
 - Non è possibile risalire alla chiave privata conoscendo la chiave pubblica.
 - Un messaggio cifrato con la chiave pubblica K_{pub} è decifrabile solo con la corrispondente chiave privata K_{pri}
 - Viceversa, un messaggio cifrato con la chiave privata K_{pri} è decifrabile solo con la corrispondente chiave pubblica K_{pub}
 - Non esistono altre possibilità



Crittografia asimmetrica

1. Confidenzialità (=riservatezza)

- Bob divulga la propria chiave pubblica P e mantiene segreta la propria chiave privata S
- Alice cifra il messaggio con la chiave pubblica di Bob
- Bob decodifica il messaggio con la propria chiave privata; essendo l'unico in possesso di tale chiave privata, è l'unico a poter leggere il messaggio

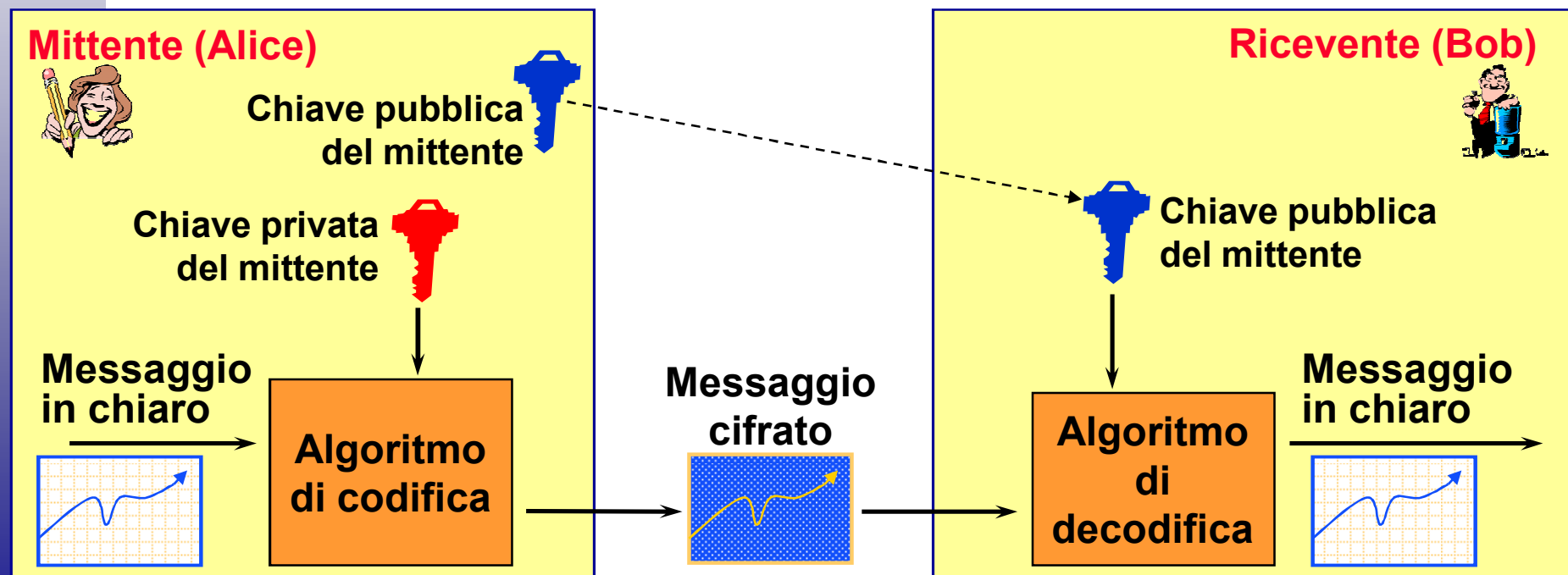




Crittografia asimmetrica

2. autenticazione e non ripudio

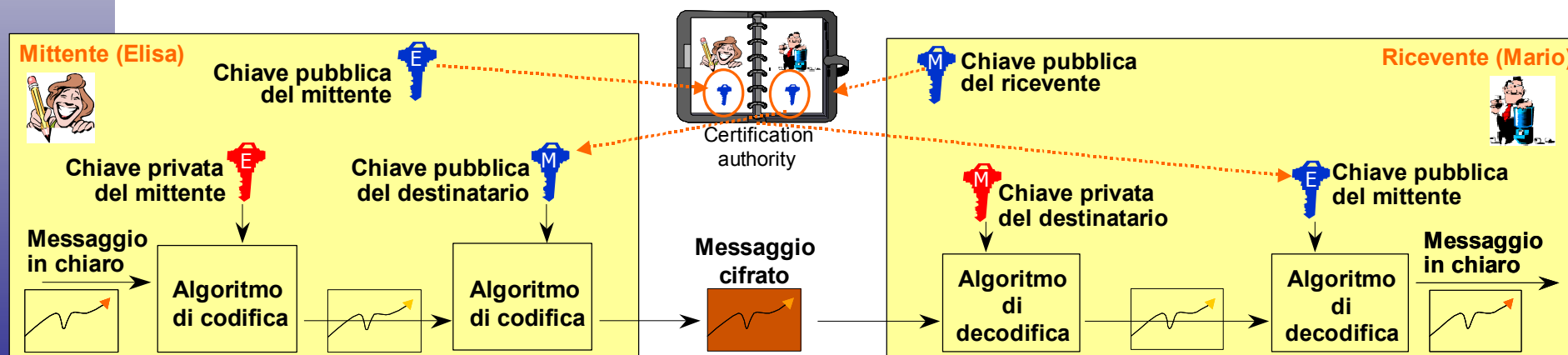
- Alice usa la propria chiave privata per cifrare il messaggio diretto a Bob
- Bob è sicuro che il messaggio provenga effettivamente da Alice: infatti solo Alice conosce la propria chiave privata e la chiave pubblica di Alice è l'unica che consente di decifrare il messaggio
- Non è garantita la riservatezza del messaggio: chiunque può usare la chiave pubblica di Alice per decifrare e quindi leggere il messaggio
- **Non ripudio** = impossibilità per il mittente di negare di essere l'autore del messaggio (equivale alla firma di un documento cartaceo)





Crittografia asimmetrica: integrità, autenticazione, confidenzialità

- Alice vuole essere sicura che il documento sia letto unicamente da Bob, garantendo anche la paternità del documento
- Si applica una doppia crittografia a chiave pubblica: Alice cifra il documento prima con la propria chiave privata, successivamente con la chiave pubblica di Bob
- **Autenticazione** - Bob è sicuro che il documento sia stato spedito da Alice: solo lei conosce la propria chiave privata e la sua chiave pubblica è garantita dalla CA
- **Confidenzialità** - Alice è sicura che il documento sia letto unicamente da Bob: solo quest'ultimo conosce la propria chiave privata
- **Integrità** - Bob è sicuro che il messaggio non sia stato modificato (altrimenti non sarebbe decodificabile)





Crittografia simmetrica VS asimmetrica

● Simmetrica

- La stessa chiave è utilizzata sia per codificare che per decodificare
- Gli algoritmi sono più veloci
- La gestione delle chiavi è problematica
- Non offre servizi di non ripudio

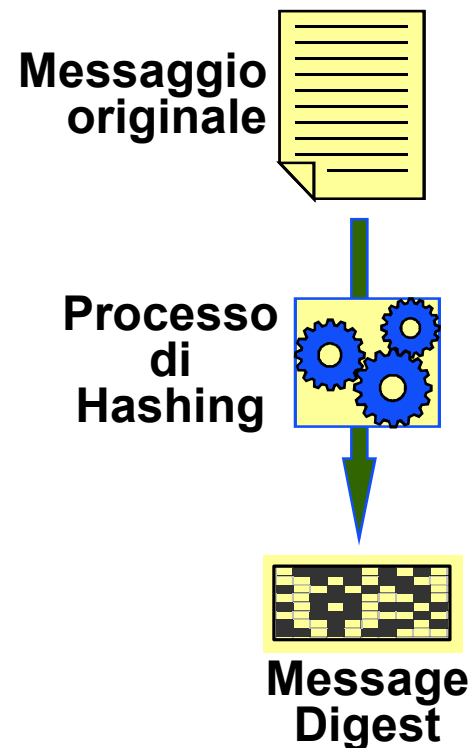
● Asimmetrica

- La chiave usata per codificare è diversa dalla chiave usata per decodificare
- Gli algoritmi sono più lenti
- La gestione delle chiavi è più semplice (la chiave privata la tengo solo io, la chiave pubblica è “pubblica” per definizione)
- Permette di avere servizi di non ripudio



Impronta (digest)

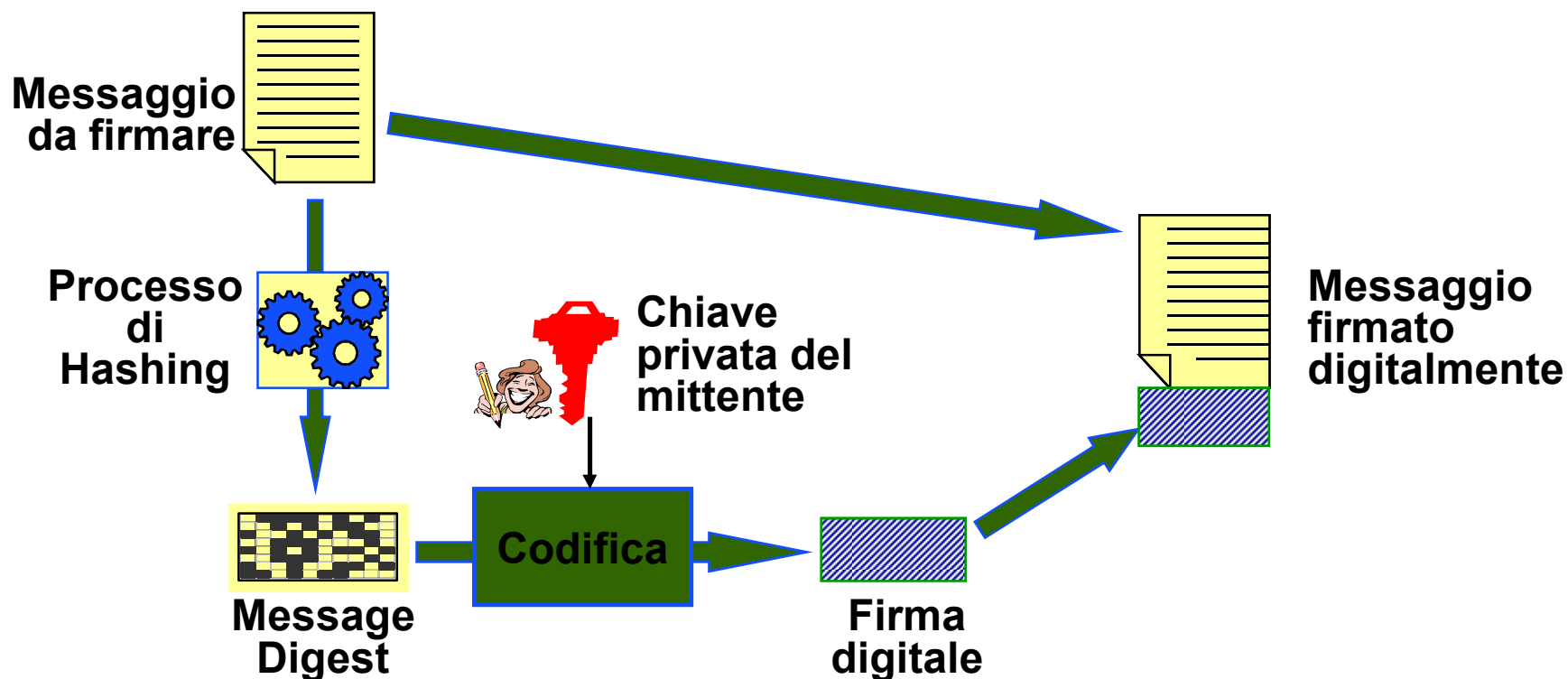
- L'impronta dei dati (digest) è una sorta di “sintesi” dei dati generata mediante appositi algoritmi, detti **algoritmi di digest** o **algoritmi di hash**
- La funzione di hash è una trasformazione di una stringa di dati in una stringa di dati più corta, avente le seguenti proprietà:
 - ha lunghezza fissa (ad es. 160 bit)
 - dati due messaggi diversi (anche di un solo bit), la probabilità di ottenere lo stesso digest è estremamente bassa
 - dato il digest, non è possibile risalire al messaggio che lo ha generato (la funzione è unidirezionale)
- Il digest di un messaggio può essere utilizzato per verificare che il contenuto di un messaggio non sia stato alterato (**integrità**)





Integrità, autenticità e non ripudio: Firma digitale

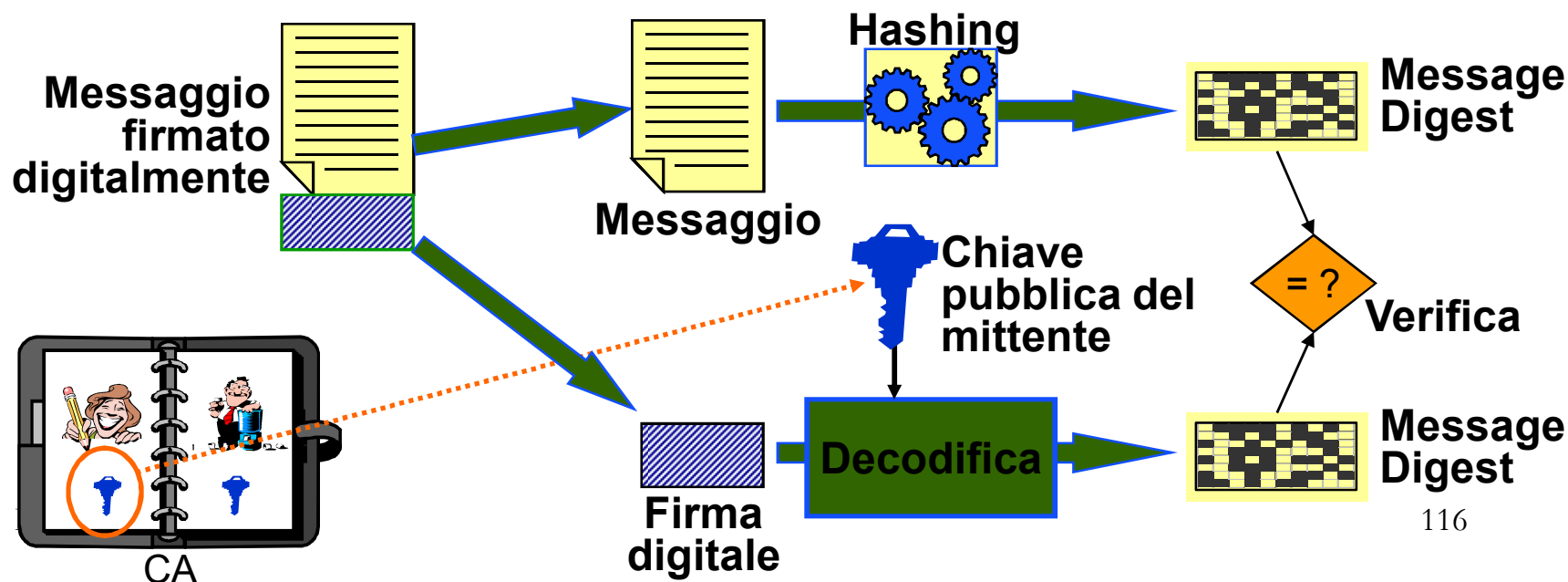
- Le funzioni di hash consentono di ottenere una “impronta digitale” del messaggio (*message digest*) basata sul suo contenuto.
- Cambiando anche un solo bit del messaggio originale cambia il valore del *message digest*
- Il *message digest* è quindi crittografato con la chiave privata del mittente e aggiunto al messaggio originale (in chiaro)





Integrità, autenticità e non ripudio: Firma digitale

- Per verificare che il messaggio ricevuto non è stato modificato durante la trasmissione e che il mittente è effettivamente chi dice di essere, il destinatario compie le seguenti operazioni:
 1. usando lo stesso algoritmo di hashing, crea un message digest del documento ricevuto
 2. usando la chiave pubblica del mittente (prelevata dalla CA), decodifica la firma digitale del mittente per ottenere il message digest del documento originale
 3. confronta i due message digest per verificare se essi coincidono: se i due message digest risultano diversi significa che il messaggio è stato modificato oppure il mittente non è chi dice di essere (ha firmato con una chiave privata diversa)





Firme non digitali VS firme digitali

• Firma non digitale

Milano, 1/6/97

Il sottoscritto, Mario Rossi, dichiara solennemente di essere debitore, nei confronti del signor Alberto Verdi, per una somma pari a \$1,000.

In fede,

Mario Rossi

• Firma digitale

-----BEGIN PGP SIGNED MESSAGE-----

Milano, 1/6/97

Il sottoscritto, Mario Rossi, dichiara solennemente di essere debitore, nei confronti del Signor Alberto Verdi, per una somma pari a \$1,000.

In fede,

Mario Rossi

-----BEGIN PGP SIGNATURE-----

iQCVAgUBLdKLSpGzE7b9kOu9AQFqAwP9HIgb0Flj9s2443
MnihEvGBT4Wilcs7IqMdfo//DiRoPsEXbndkS6f9WVASOu
gI+JdSxDjfEo1jVja9RpkNFDIOcvIZljmfoOYO4xXLzag1Tk0
rJs/UQüIgLYrSQVWeR5zdhReON6XUF420jKulct9WAN32L
osf3m1BMJ6t7I/+eQ==eRX1

-----END PGP SIGNATURE-----



Scambio di chiavi pubbliche CA e PKC

- Il problema non è garantire la riservatezza della chiave ma conoscere qual è la chiave pubblica e garantirne l'associazione certa con il suo titolare
- 2 soluzioni possibili:
 - quando qualcuno deve mandarci un messaggio ci deve prima chiedere la nostra chiave pubblica
 - pubblicazione delle chiavi pubbliche da parte di una **Certification Authority (CA)**
 - la CA garantisce la titolarità della chiave pubblica mediante certificati (**PKC: Public-Key Certificate**)
 - il PKC può essere anche fornito direttamente dal suo titolare

Certification Authority





Public Key Certificate: Standard X.509

		<i>Campo</i>	<i>Valore</i>
		Version	3
		serialNumber	58
CA emittente	{	Issuer	C=IT, O=SPQR, OU=Certification Authority
Periodo validità del PKC	{	Validity	7-feb-2002 : 31-dic-2003
Informazioni sul titolare	{	Subject	C=IT, O=SPQR, CN=Caio Gregorio
		subjectAlternativeName	RFC-822, caio.gregorio@spqr.it
Chiave pubblica e utilizzi per i quali è stata certificata	{	subjectPublicKeyInfo	RSA, 0101100...10110
		keyUsage	digitalSignature, nonRepudiation, keyExchange, keyAgreement
		extendedKeyUsage	EmailProtection
Firma digitale del certificato (per evitare alterazioni)	{	signatureAlgorithm	Md5WithRSAEncryption
		Signature	1101000...10011



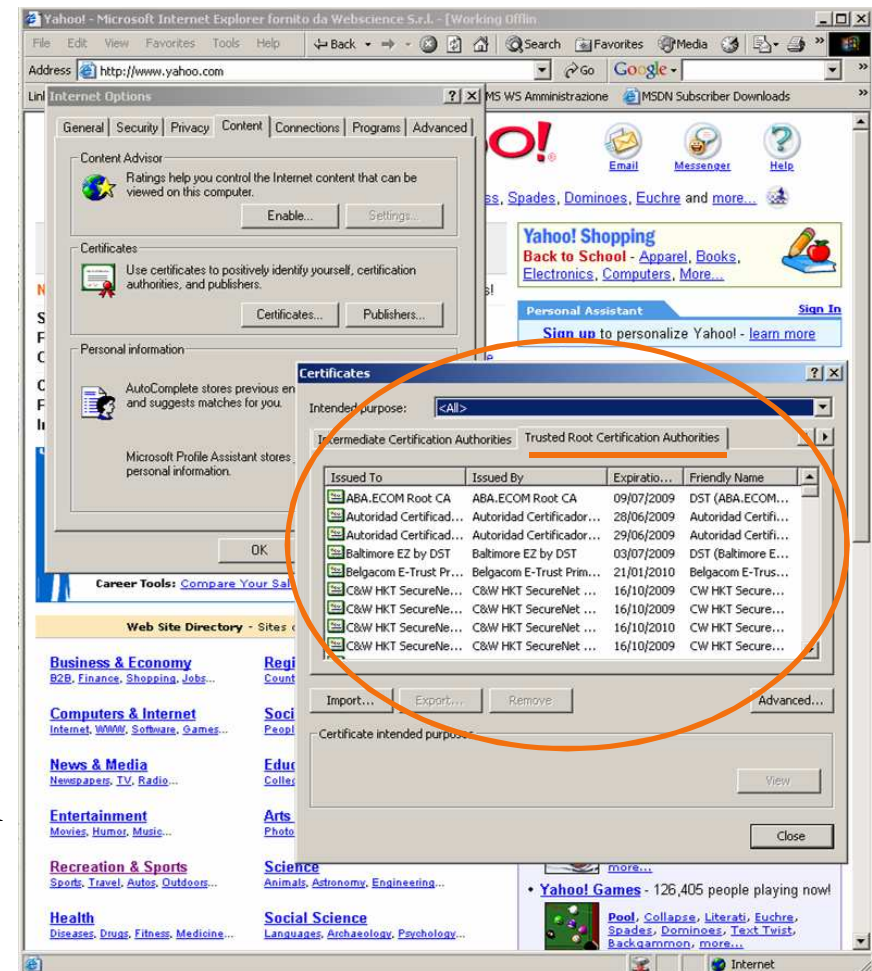
PKI - Gestione della chiave della CA

- Come faccio ad essere sicuro che la Chiave Pubblica della CA sia veramente la sua (chi certifica la CA)?

– Soluz. 1: conservare in ogni postazione di lavoro un elenco (protetto) delle chiavi pubbliche di tutte le CA fidate → ogni volta che una CA viene aggiunta o tolta dall'elenco devono essere aggiornate tutte le postazioni di lavoro

– Soluz. 2: conservare in ogni postazione di lavoro un elenco (protetto) di un insieme (ristretto) di **Root-CA**:

- certificano direttamente alcuni utenti
- certificano altre **CA subordinate**, formando una **gerarchia di CA**





PKI - Gerarchia di CA

