11 - Applicazioni di rete, protocolli Internet e Sicurezza

Il World Wide Web (WWW)

- Insieme di *server* distribuito sulla rete, che permette di accedere a file (ipertesti) memorizzati in particolari directory su tutte le macchine collegate
- Per richiedere informazioni ai server Web si usano solitamente dei programmi detti Web *client* (o *browser* o navigatori, come Microsoft Explorer, Firefox, ...)
  - i navigatori si preoccupano di interagire con i server seguendo opportuni protocolli
    - generalmente **`http`** (*hypertext transfer protocol*) ma anche **`ftp`** *(file transfer protocol)* ecc.

World Wide Web: Esempio

- Vediamo cosa accade richiedendo l'accesso a una certa pagina del web

es: **`http://www.di.unipi.it/~andrea/IG09.html`**

  - **`www.di.unipi.it`**
    - è l'indirizzo IP in formato simbolico del server web dove si trova l'informazione cercata
  - il navigatore traduce questa richiesta
    - cioè la trasforma in un messaggio al server con tutti i dettagli necessari e secondo le regole del protocollo specificato (**`http`**)
    - **`~andrea/IG09.html`** viene inviato al server per individuare il file cercato (**`IG09.html`**) all'interno della directory **`andrea`** (il server sa come trovarli)

World Wide Web: Esempio 2

es: **`http://www.di.unipi.it/~andrea/IG09.html`**

- il server **`www.di.unipi.it`** risponde alla richiesta inviando il testo della pagina cercata (se la trova)
- il navigatore visualizza il contenuto della pagina usando una opportuna applicazione
- tipico formato è HTML (*Hypertext Markup Language*)
  - HTML permette di incapsulare nel testo le informazioni relative alla sua formattazione e diversi oggetti di tipo multimediale (immagini, suoni, etc)
  - *...piccola dimostrazione di HTML...*

World Wide Web: Esempio 3

es: **`http://www.di.unipi.it/~andrea/IG09.html`**

- **`//www.di.unipi.it/~andrea/IG09.html`**

  è detto URL (*Uniform Resource Locator*) e permette di localizzare in maniera univoca tutti i file pubblicati sulla rete.

La Posta Elettronica

- Ciascun dominio dedica un server all'invio della posta elettronica (server SMTP) e uno alla ricezione (server IMAP o POP3).

- Per inviare un messaggio so usa il protocollo SMTP (*simple mail transport protocol*): i messaggi spediti dagli utenti vengono inviati al server SMTP che si occupa di inviarli ai destinatari

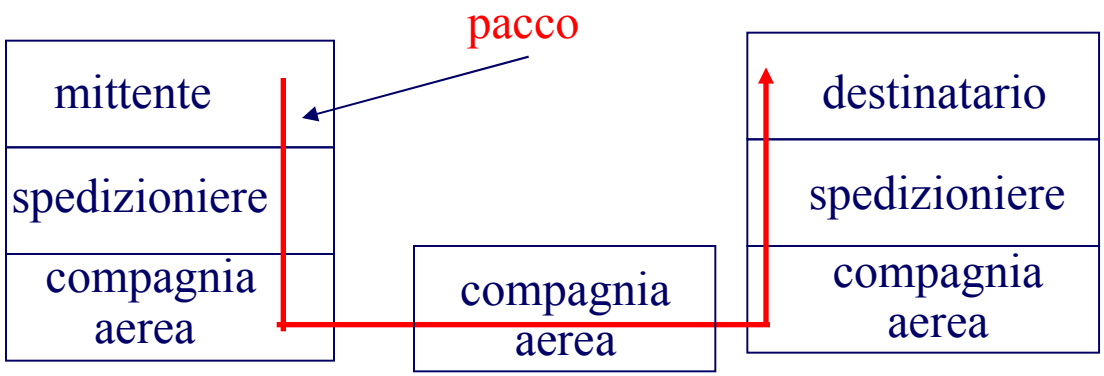
- Per ricevere messaggi ci sono sono vari protocolli, tra cui:
  - POP3: msg scaricati sulla memoria di massa
  - IMAP: msg sulla macchina che ospita il server

Architetture di rete

- I protocolli per lo scambio di informazioni su di una rete possono essere classificati secondo una gerarchia a livelli:
  - ogni protocollo disciplina un aspetto della comunicazione
- L'insieme dei protocolli usati da una rete costituisce l'architettura della rete
  - esistono architetture standard ufficiali (es. **ISO/OSI**)
  - l'architettura di Internet costituisce uno standard di fatto (*Internet Protocol Suite* o *TCP/IP*)

Comunicazione multilivello

- Organizzazione a pacchetti: ogni livello
  - aggiunge ai dati da trasmettere ricevuti dal livello superiore delle informazioni di controllo che sono usate al livello del nodo destinazione
  - passa il messaggio al livello inferiore e così via fino al livello 1
  - Esempio: invio di un pacco via aerea



Architettura ISO/OSI

- Open System Interconnection della International Organization for Standardization: è costituita da 7 livelli

- Il livello n di un calcolatore comunica (virtualmente) con il livello n di un altro calcolatore
- In realtà nessun dato viene trasferito da un livello n ad un altro ma passa ad un livello sottostante (o sovrastante, in ricezione)

Architettura ISO/OSI 2

- Livello 7

prevede i servizi che eseguono le applicazioni dell'utente (condivisione risorse, etc.)

Architettura ISO/OSI 3

- Livello 4

controlla il trasferimento dei dati al nodo destinazione. Quando i dati sono molto numerosi si occupa di frammentarli in più pacchetti o di gestire errori

Architettura ISO/OSI 4

- Livello 3

gestisce le tabelle di instradamento che determinano i nodi intermedi (ogni nodo è collegato solo a un certo numero di nodi)

Architettura ISO/OSI 5

- Livello 2

si occupa della trasmissione dei dati tra nodi adiacenti della rete, (cioè collegati fisicamente da un singolo canale di comunicazione).

Es.: CSMA/CD, Token ring, PPP.

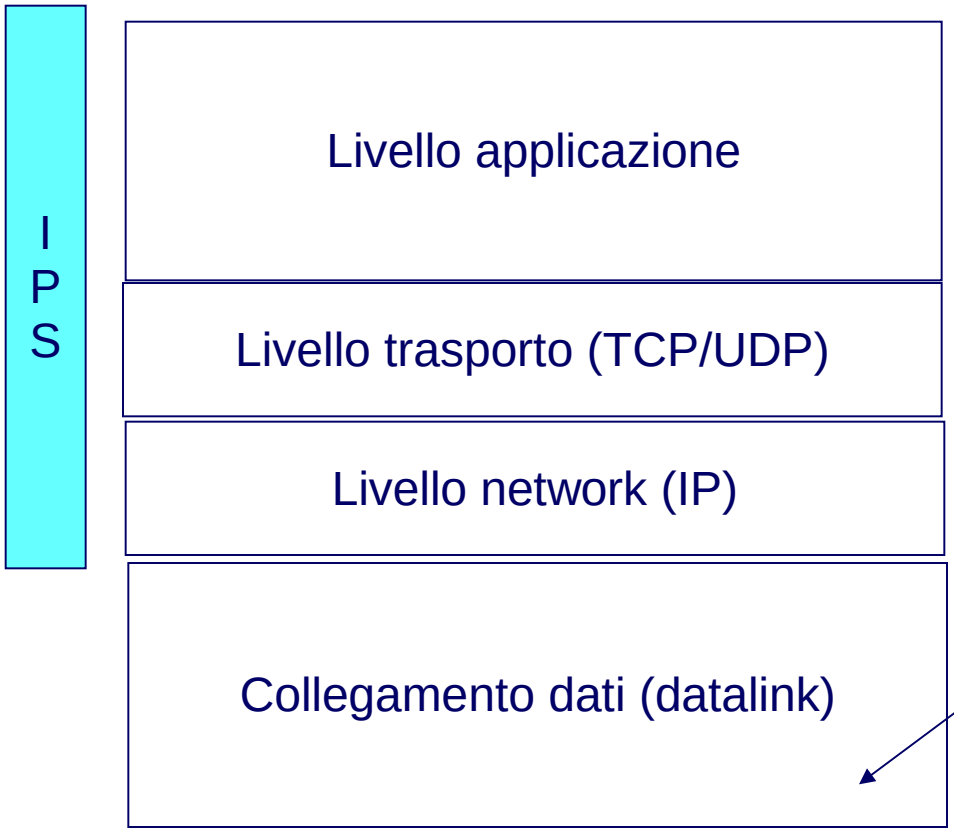
Architettura ISO/OSI 6

- Livello 1

L’Internet Protocol Suite

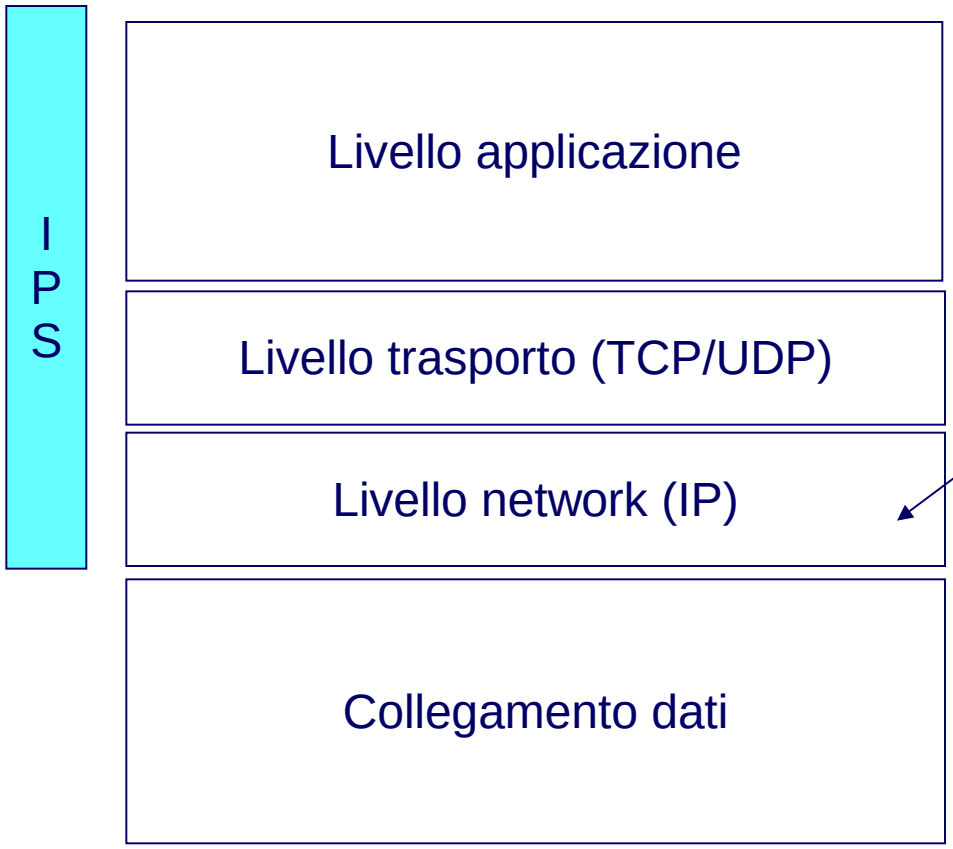
- L’Internet Protocol Suite (IPS) si occupa del trasferimento dei dati su Internet
- Viene impropriamente chiamato TCP/IP (dai nomi di due suoi protocolli)
- A differenza del modello ISO/OSI, non è un modello teorico e ha un’organizzazione a 4 livelli

L’Internet Protocol Suite 2



E’ il protocollo hw/sw che si occupa di trasmettere correttamente un singolo gruppo di bit (frame) fra due nodi collegati fisicamente in una rete omogenea.

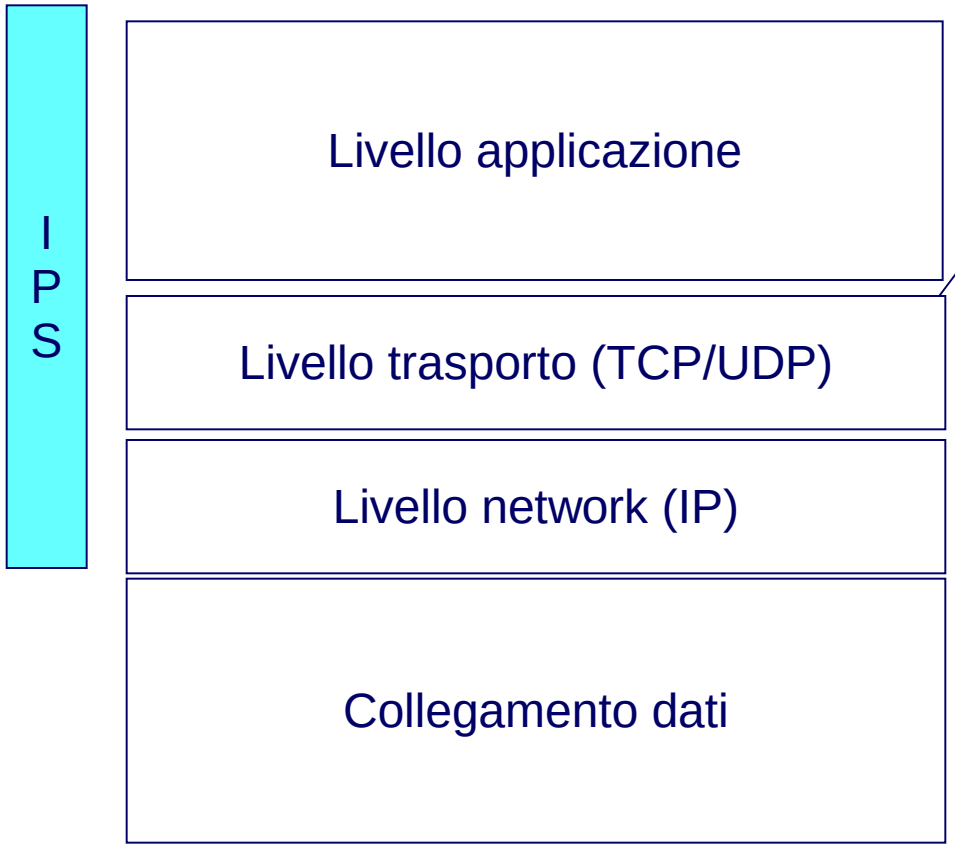
L’Internet Protocol Suite 3



Gestisce l’instradamento dei messaggi fra due nodi che non appartengono alla stessa rete omogenea.

È analogo a decidere che rotta fare seguire ad un treno merci in viaggio da Reggio Calabria a Milano…

L’Internet Protocol Suite 4

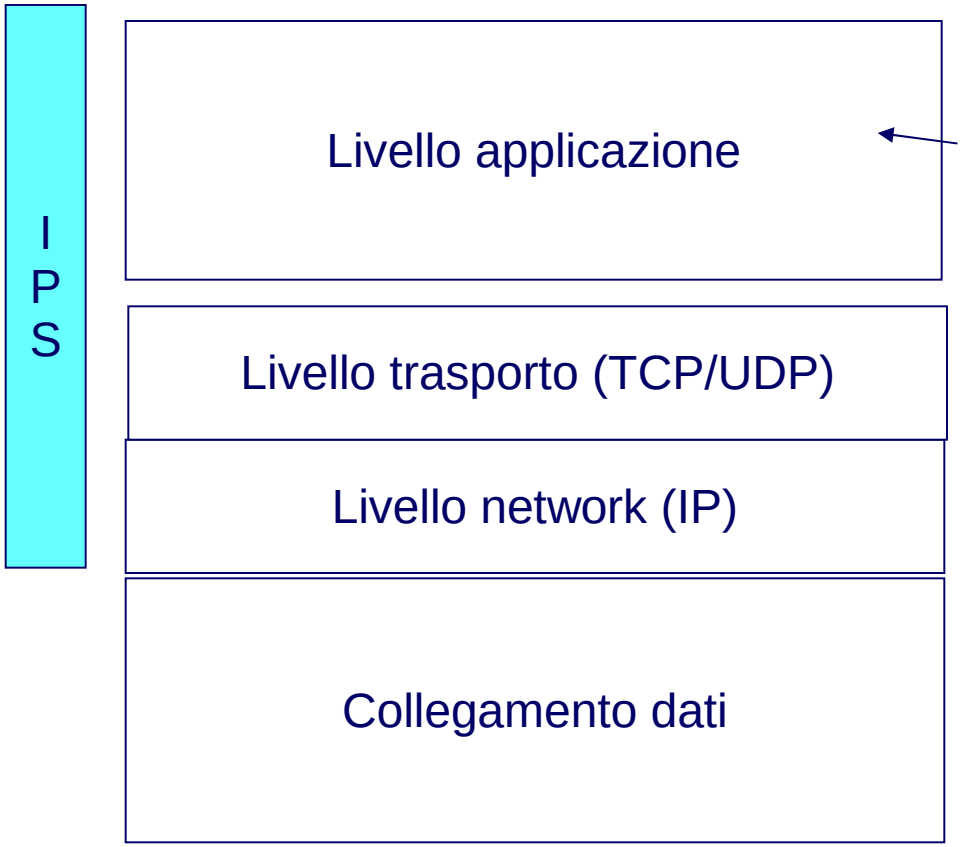


Controlla il trasferimento dei dati al nodo destinazione. Se il messaggio è troppo grosso lo spezza in più messaggi piccoli (pacchetti).

TCP controlla anche che ogni pacchetto sia stato trasmesso correttamente e ricostruisce il messaggio a destinazione.

UDP e TCP permettono a più utenti di usare la rete contemporaneamente

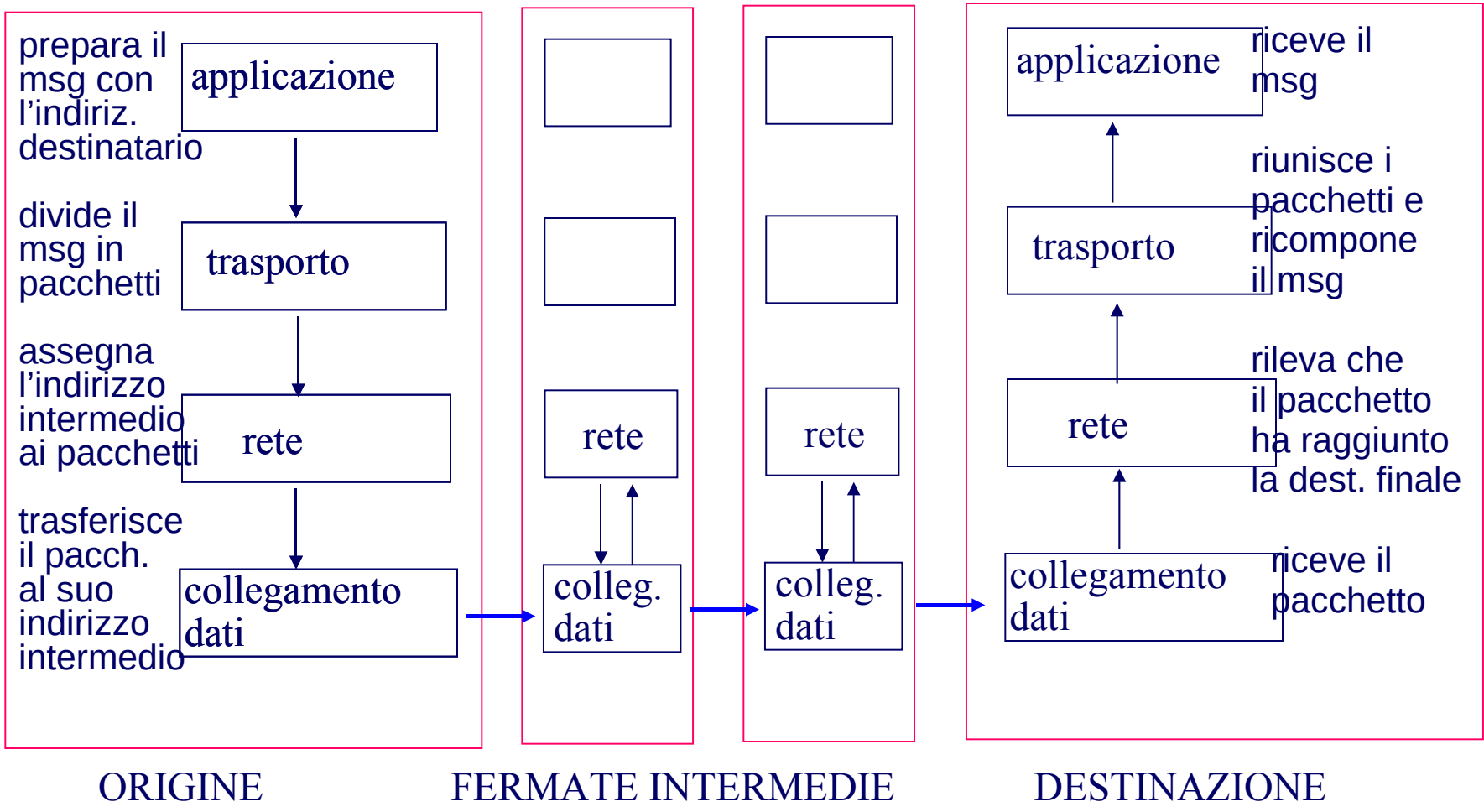
L’Internet Protocol Suite 4



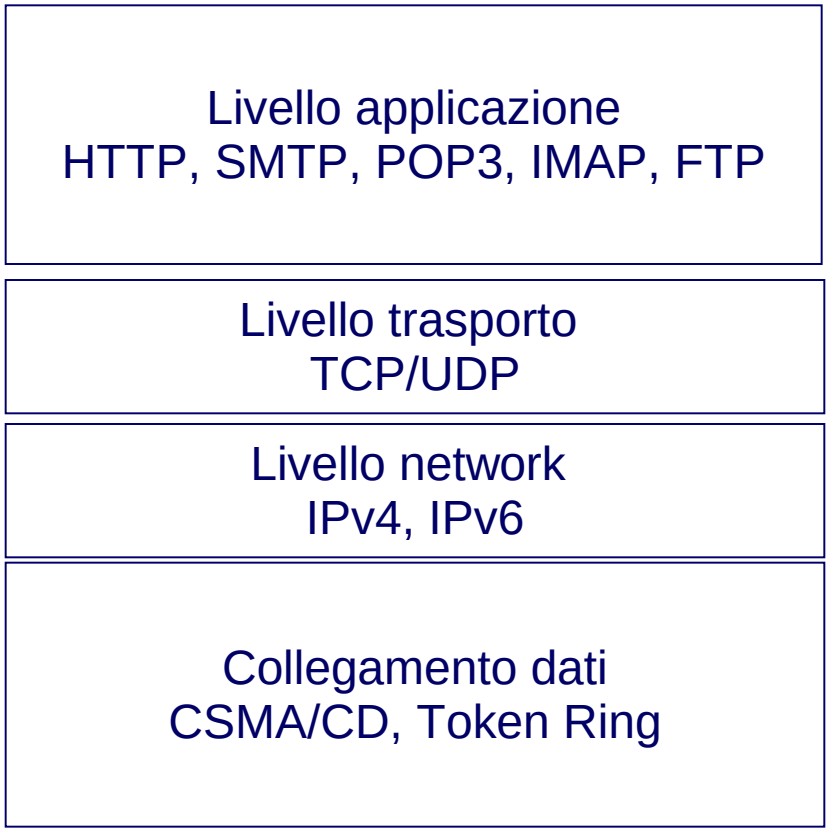
I protocolli più comuni sono
FTP (file transfer protocol)
per il trasferimento file
TELNET (connessione a
terminale remoto)
SMTP (per la posta elettronica)
e HTTP (per il World Wide Web)

L'Internet Protocol Suite 5

- Il tragitto di un messaggio attraverso Internet



L’Internet Protocol Suite 6



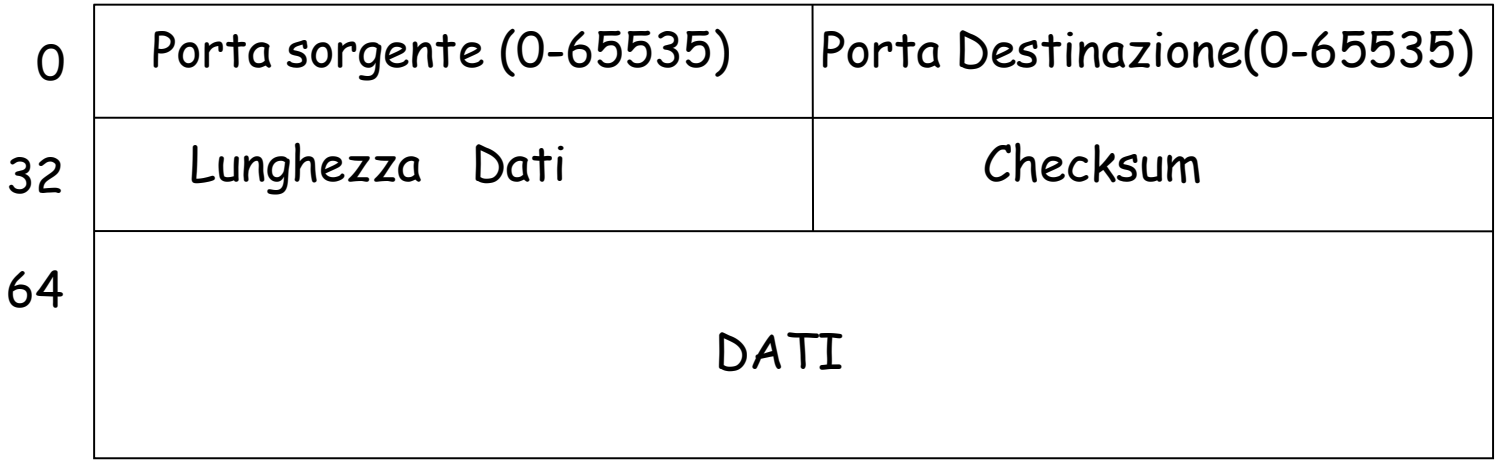
L'Internet Protocol Suite 7

- Internet Protocol (IP) gestisce 3 aspetti :
  - Fornisce uno schema di indirizzamento per tutti i computer collegati dalla rete di reti (*indirizzo IP*)
  - Decide il formato dei pacchetti che vengono trasmessi
    - le reti collegate hanno tecnologia diversa e quindi in generale formato e dimensione dei pacchetti diversa
  - Decide come instradare i vari pacchetti fino al nodo destinazione
    - la decisione viene presa in base ad una tabella di routing che spiega come comportarsi per i vari indirizzi
  - IP V6 è il nuovo protocollo che usa 128 bit anziché (per evitare la saturazione degli IP address)

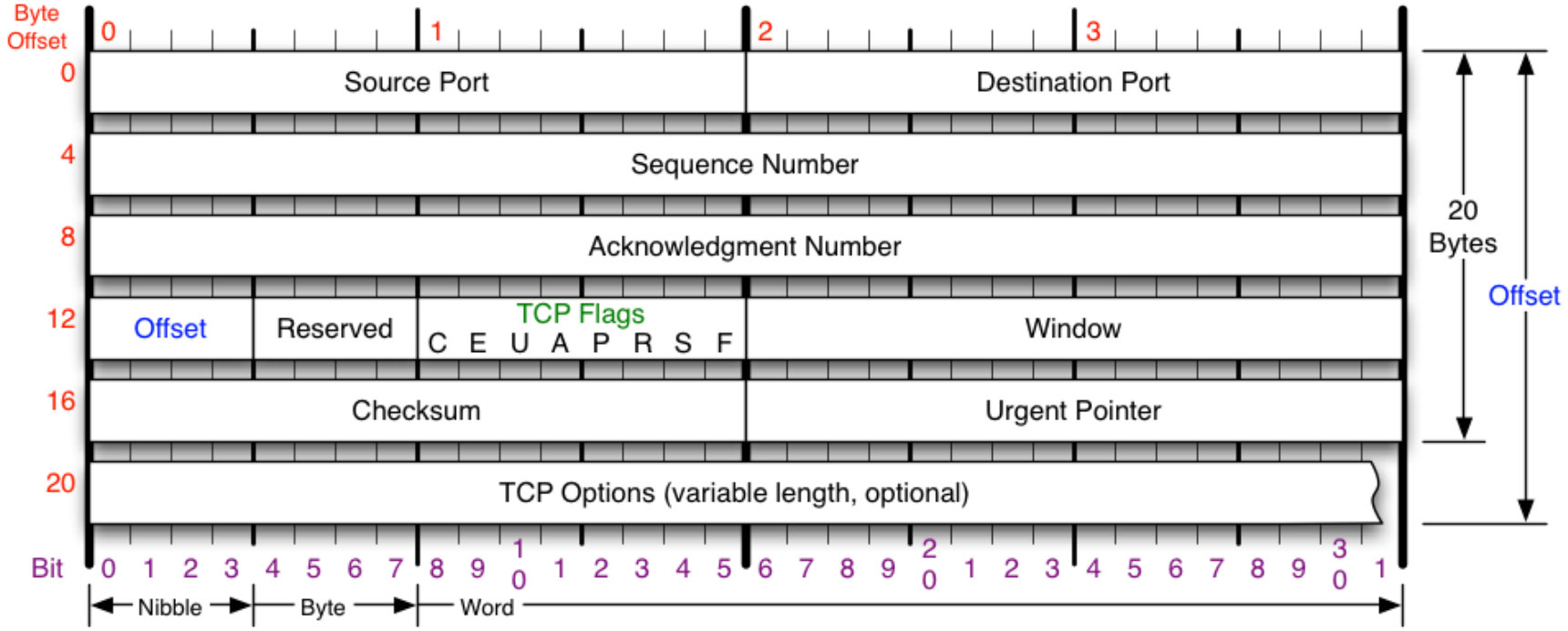
FORMATO DEL PACCHETTO IP

L'HEADER UDP

- Datagram UDP = unità di trasmissione definita dal protocollo UDP
- Ogni datagram UDP
  - viene incapsulato in un singolo pacchetto IP
  - definisce un header che viene aggiunto all'header IP



TCP Header



TCP Flags

C E U A P R S F

Congestion Window

- C 0x80 Reduced (CWR)
- E 0x40 ECN Echo (ECE)
- U 0x20 Urgent
- A 0x10 Ack
- P 0x08 Push
- R 0x04 Reset
- S 0x02 Syn
- F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Sicurezza nelle reti

Tipologie di attacco

- Invio di software dannoso che può essere trasferito su un computer o attaccarlo a distanza
  - **Virus**: quando un programma ospite viene eseguito, anche il virus viene eseguito (può corrompere/cancellare porzioni di SO)
  - **Cavallo di Troia**: programma che entra sotto forma di applicazione legale. Una volta entrato può eseguire codice dannoso
  - **Spyware**: raccoglie informazioni sul computer ospite e le riporta a un altro computer (per ottenere per es. password e dati personali)

Tipologie di attacco 2

- **Phishing** (password phishing): è un modo esplicito di ottenere informazioni chiedendole (es: con uso di posta elettronica)
- **DoS** (denial of service): software eseguito su un altro computer e che sovraccarica la macchina attaccata (il software viene installato su uno o più computer ignari)
- **Spam**: proliferare di email “spazzatura” (adottato per phishing e cavalli di Troia)

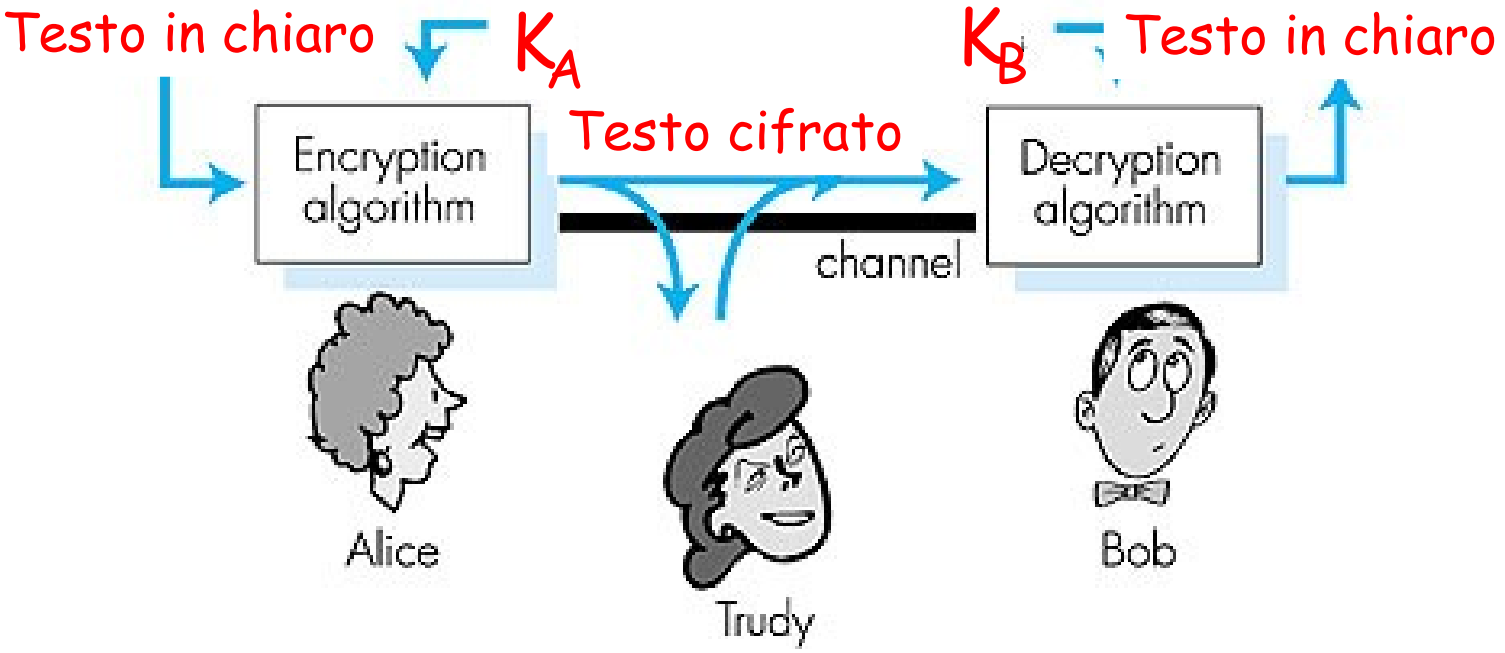
Rimedi e protezioni

- **Firewall**: installato presso il gateway di un dominio, per filtrare messaggi (contro DoS)
- **Filtri anti-spam**: varianti di firewall per fermare messaggi indesiderati di posta elettronica; possono essere istruiti
- **Software antivirus**

Crittografia

- Le tecniche crittografiche vengono usate per proteggere dati privati (es. passwd, num. carta di credito) quando i msg vengono comunicati su reti pubbliche.
- La crittografia si usa per garantire proprietà come:
  - autenticazione (un msg deve dare garanzia di provenire da un certo mittente)
  - segretezza (solo il mittente e il destinatario conoscono il contenuto di un msg)
- Molte applicazioni internet sono state modificate incorporando la crittografia (es. il protocollo HTTPS è basato su SSL)

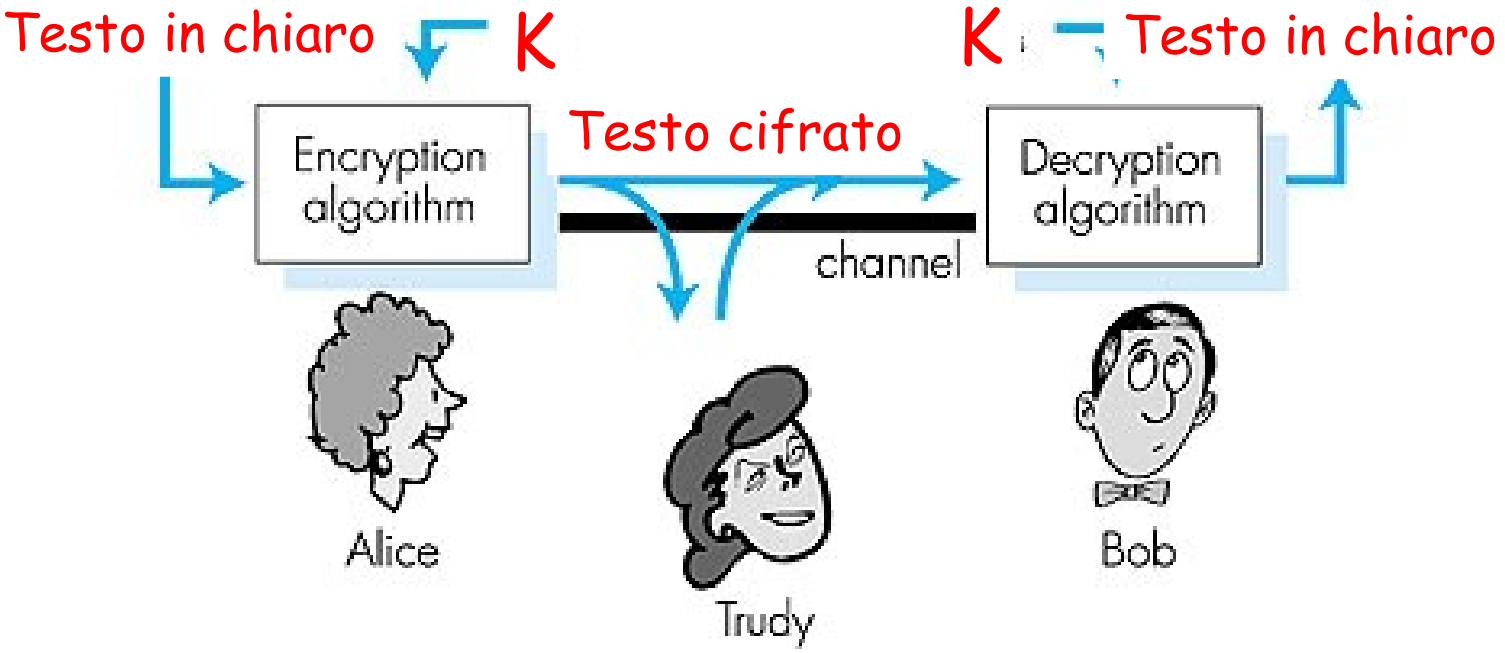
Crittografia 2



Chiave simmetrica: le chiave del mittente e del destinatario sono identiche

Chiave pubblica: la chiave di cifratura è pubblica, mentre la chiave di decifratura è segreta

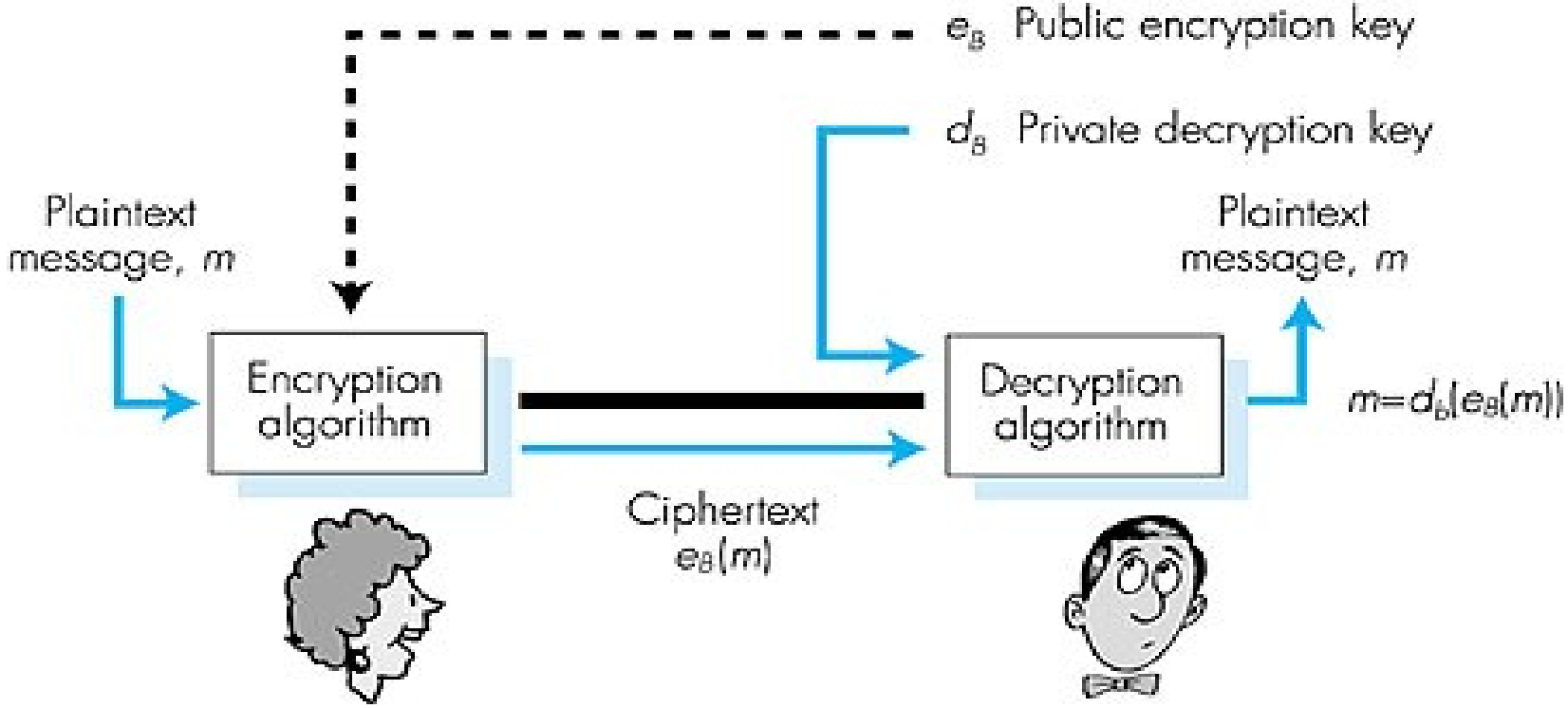
Crittografia: chiave simmetrica



A: E(K,M) = C (cioè, il testo cifrato C è ottenuto criptando M con la chiave K)

B: D(K,C) = M (cioè, il testo in chiaro M è ottenuto decriptando C con la stessa chiave K)

Crittografia: chiave pubblica



A: $E(e_B,M) = C$ (cioè, il testo cifrato C è ottenuto criptando M con la chiave pubblica del destinatario e_B)

B: $D(d_B,C) = M$ (cioè, il testo in chiaro M è ottenuto decriptando C con la chiave privata del destinatario e_B)

Autorità e chiavi pubbliche

- L'Autorità di Certificazione (CA) crea un certificato che lega la chiave pubblica ad una determinata entità.
- Le entità (persone, router, etc.) possono registrare la propria chiave pubblica con CA.