TCP/IP
un’introduzione

Introduzione

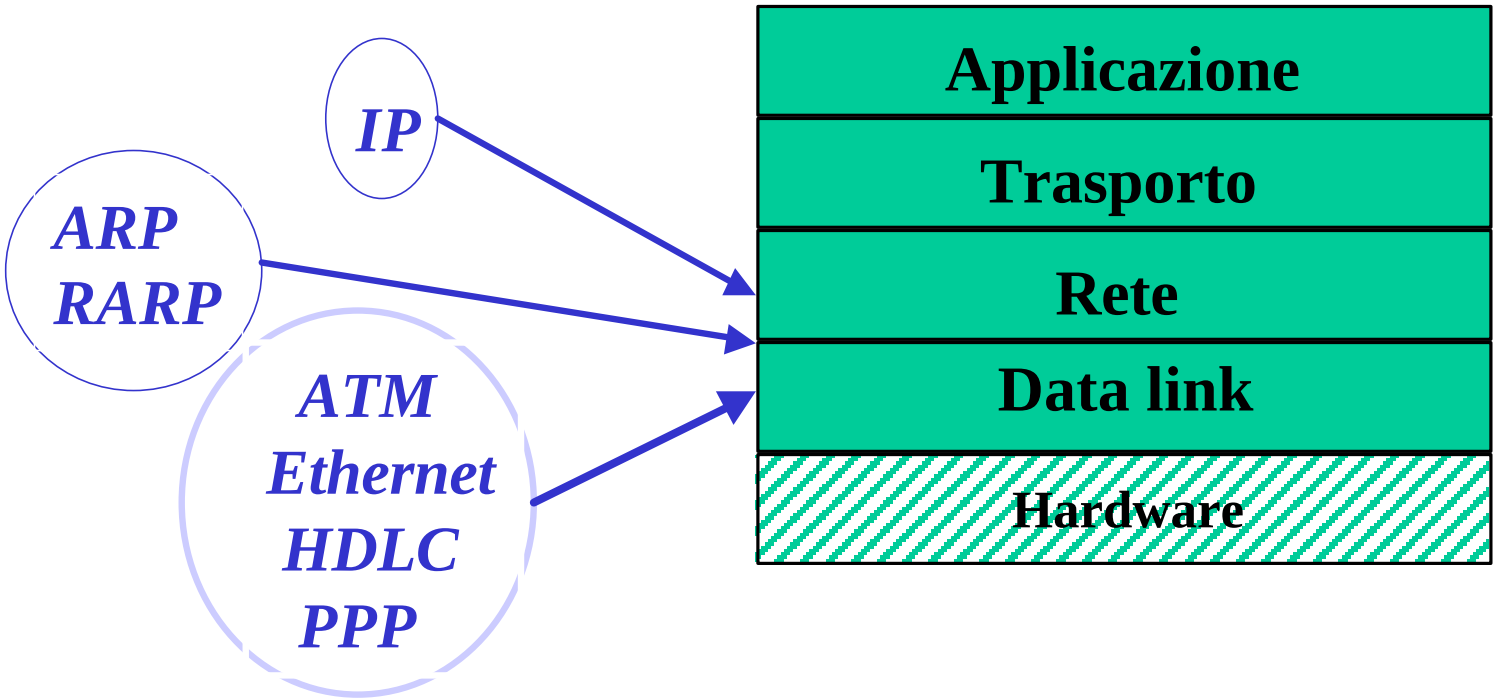
- Il successo di Internet (rate di crescita annuo > 200 %) e' dovuto all'uso di protocolli standard "aperti" (**IETF)**

- TCP/IP (***T****ransmission* ***C****ontrol* ***P****rotocol/****I****nternet* ***P****rotocol*) indica la suite di protocolli aperti, necessari per il funzionamento di Internet.

Pila ISO/OSI


7
Applicazione
6
Presentazione
5
Sessione
4
Trasporto
3
Rete
2
Data Link
1
Fisico

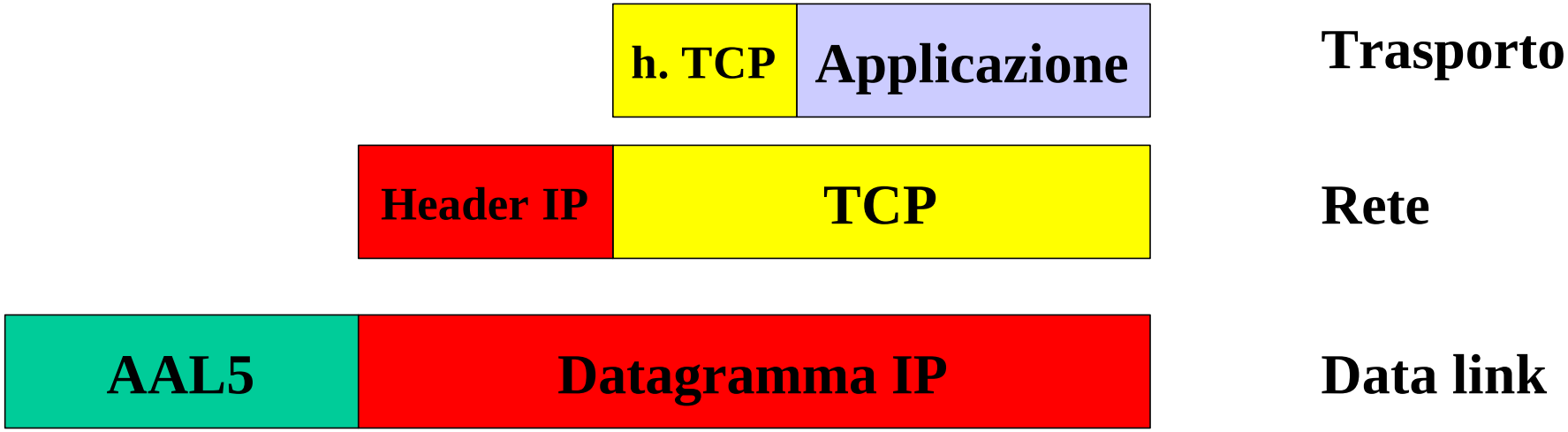
Livelli del TCP/IP (1)



Livelli del TCP/IP (2)

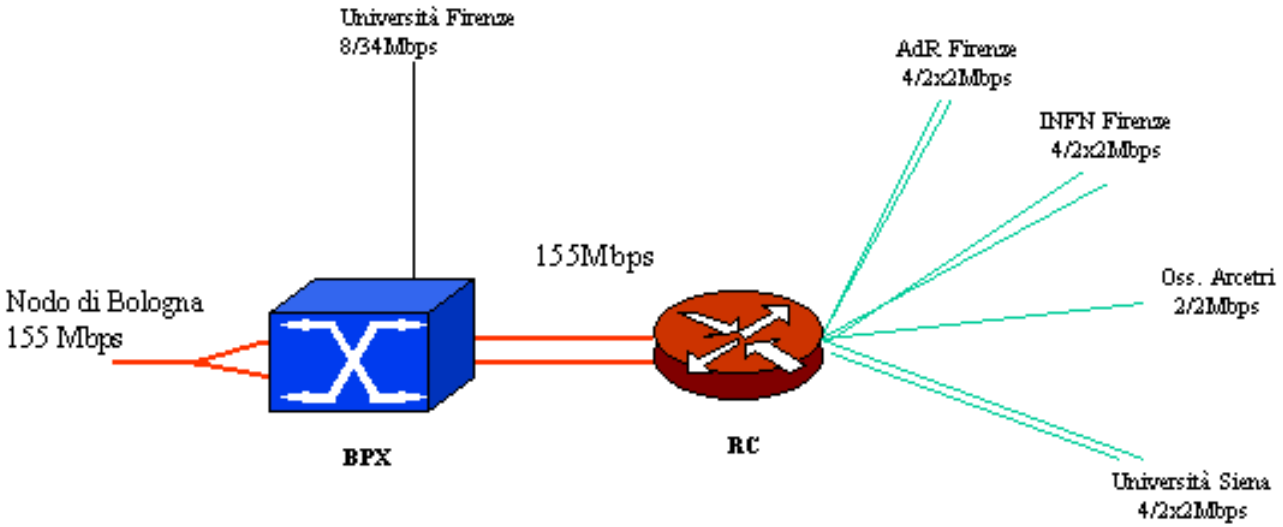
- Livello ***Trasporto*** – assicura la comunicazione end-end tra applicazioni su host diversi
- Livello ***Internet*** – assicura la comunicazione tra host diversi (datagrammi IP)
- Livello ***Data Link*** – responsabile dell'inoltro dei datagrammi IP su uno specifico tipo di rete (es. Ethernet, ATM, PPP, HDLC etc..)

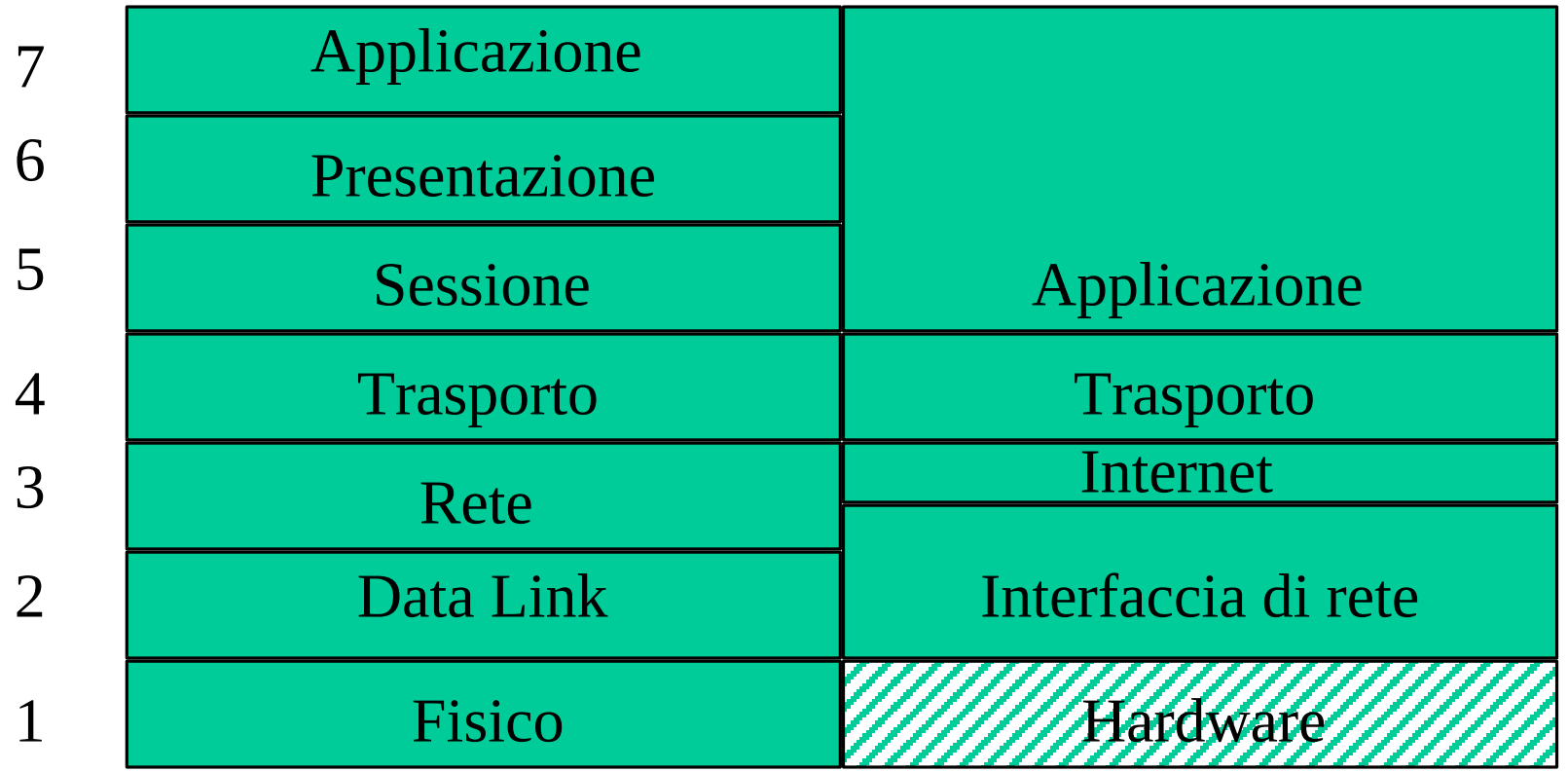
Incapsulamento



- Es.: struttura a livelli di GARR-B
  - IP/ATM/SDH (backbone)
  - IP/ATM/SDH o IP/ATM/PDH o IP/HDLC (accessi utente)

PoP di Firenze




7
6
5
4
3
2
1
Applicazione
Presentazione
Sessione
Trasporto
Rete
Data Link
Fisico
Applicazione
Trasporto
Internet
Interfaccia di rete
Hardware

Address Resolution Protocol

- Mapping indirizzi IP in indirizzi “fisici”
  - Host A chiede con un broadcast P_B di Host B
  - Host B risponde con IP_B
  - Host A memorizza abbinamento (cache)

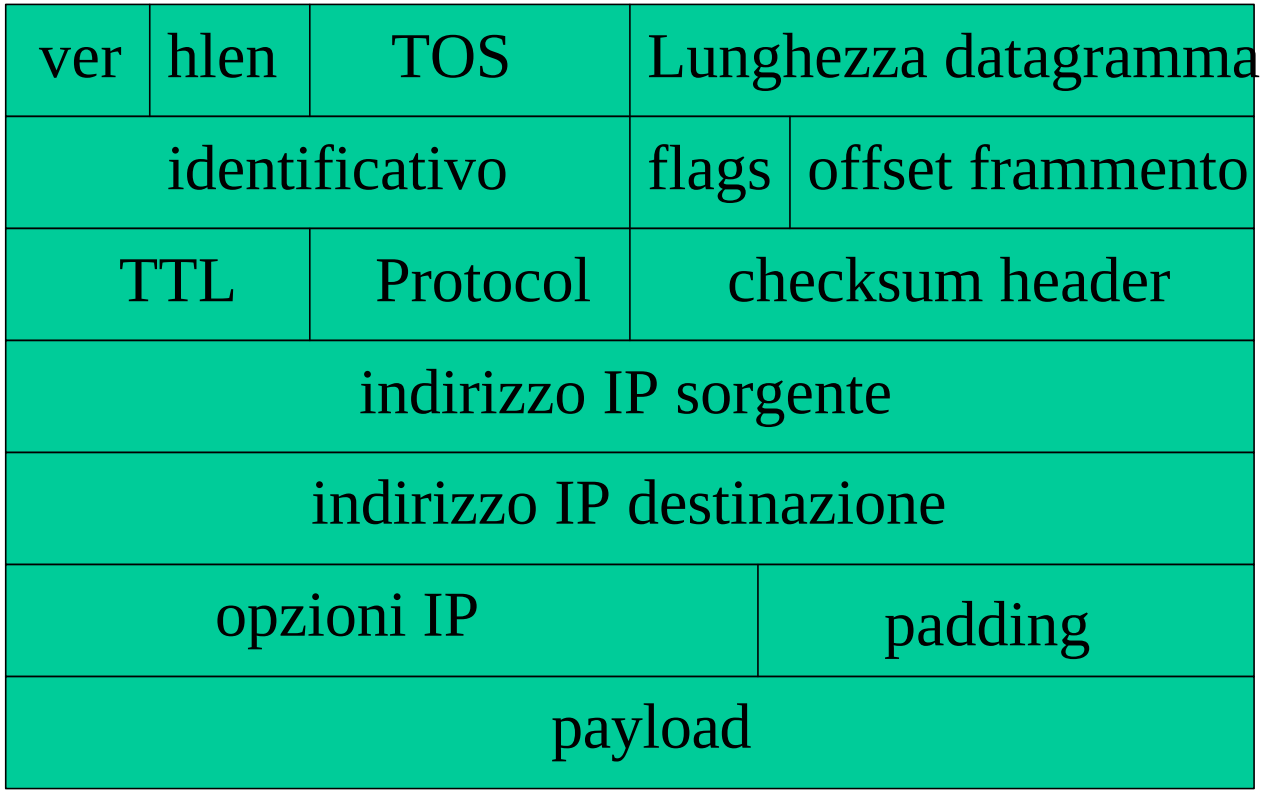
Reverse Address Resolution Protocol

- Mapping indirizzo “fisico” in indirizzo IP (es. Host senza disco)
  - Host A invia broadcast un messaggio RARP
  - RARP server risponde inviando indirizzo IP

Internet Protocol

- Sistema di inoltro di datagrammi
  - *Connectionless*
  - *Unreliable*
- Compiti del protocollo:
  - Definizione del datagramma
  - Routing dei pacchetti
  - Trattamento dei pacchetti
  - Diagnostica

Header IPv4


ver
hlen
TOS
Lunghezza datagramma
identificativo
flags
offset frammento
TTL
Protocol
checksum header
indirizzo IP sorgente
indirizzo IP destinazione
opzioni IP
padding
payload

Indirizzamento IPv4

- Indirizzi a 32 bit
- Indirizzi unicast
  - Classi A,B,C
  - Classless (prefisso/netmask)
- Indirizzi multicast (classe D)
- Indirizzi broadcast
- Indirizzi a scope globale
- Indirizzi di loopback: 127.0.0.0/8

Reti “nascoste”

Reti “nascoste” o “private” per intranet (RFC 1918)

- 10.0.0.0/8 (“classe A”)
- 172.16.0.0/12 (“classi B”)
- 192.168.0.0/16 (“classi C”)

Non devono essere annunciate all’esterno della LAN

Problemi con IPv4

- Spazio indirizzi insufficiente
- Difficolta’ renumbering
- Nessun supporto mobilita’
- Scarso supporto alla QoS
- Scarsa attenzione alla sicurezza

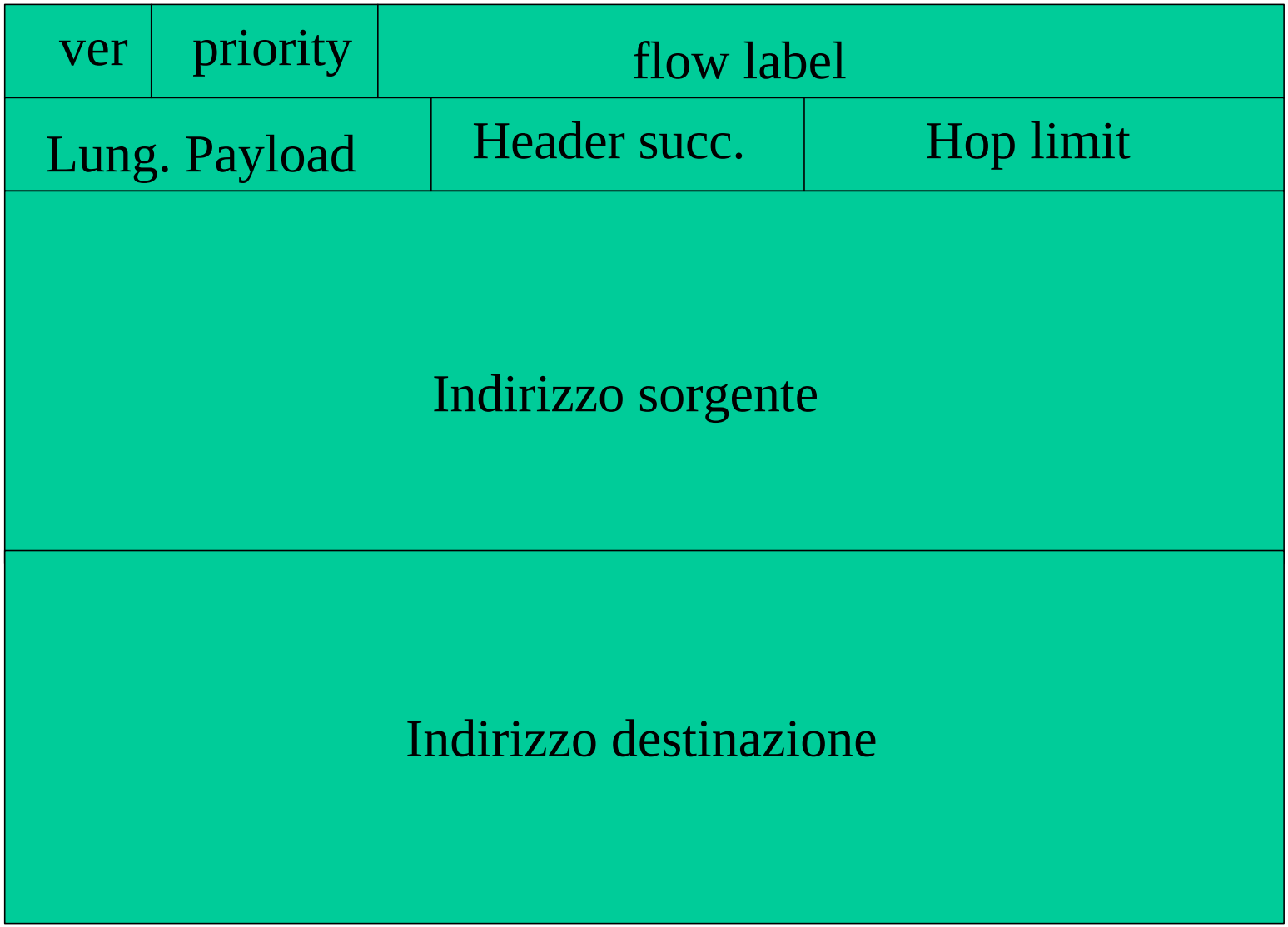
Problemi di sicurezza con IP

- Sniffing – non c’e’ protezione del payload a livello IP
  - Intercettazione dei messaggi (password etc..)
- Spoofing – Non e’ prevista autenticazione dell’IP sorgente
  - Attacchi con un solo messaggio (es. Smurfing)
  - Impersonificazione di un altro host

IPv6

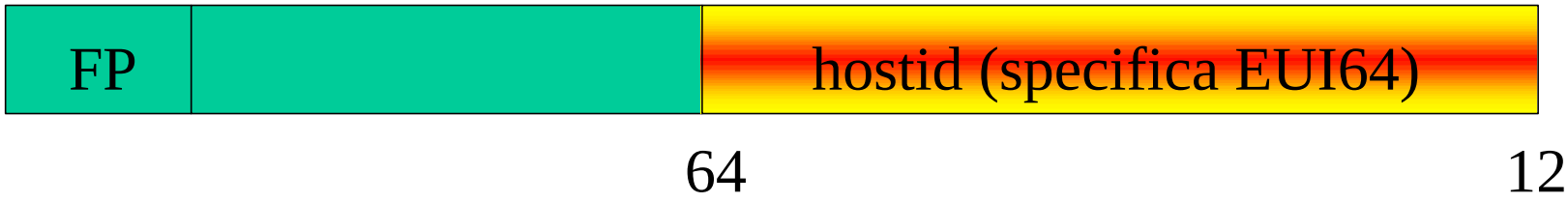
- Aumento spazio indirizzi
- Routing gerarchico
- Eliminazione della frammentazione
- Autoconfogurazione
- Supporto mobilita’
- Supporto QoS
- Supporto sicurezza

Header IPv6


ver
priority
flow label
Lung. Payload
Header succ.
Hop limit
Indirizzo sorgente
Indirizzo destinazione

Indirizzamento IPv6 (1)

- Indirizzi a 128 bit
  - Indirizzi unicast (**globali aggregabili, site-local, link-local**)

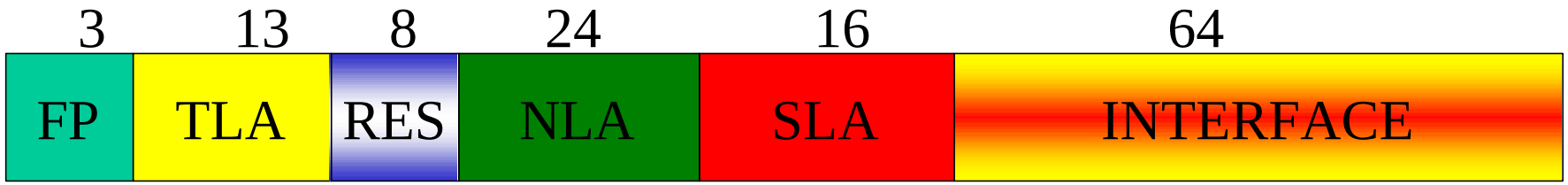


  - Indirizzi anycast
  - Indirizzi multicast

Non ci sono indirizzi broadcast

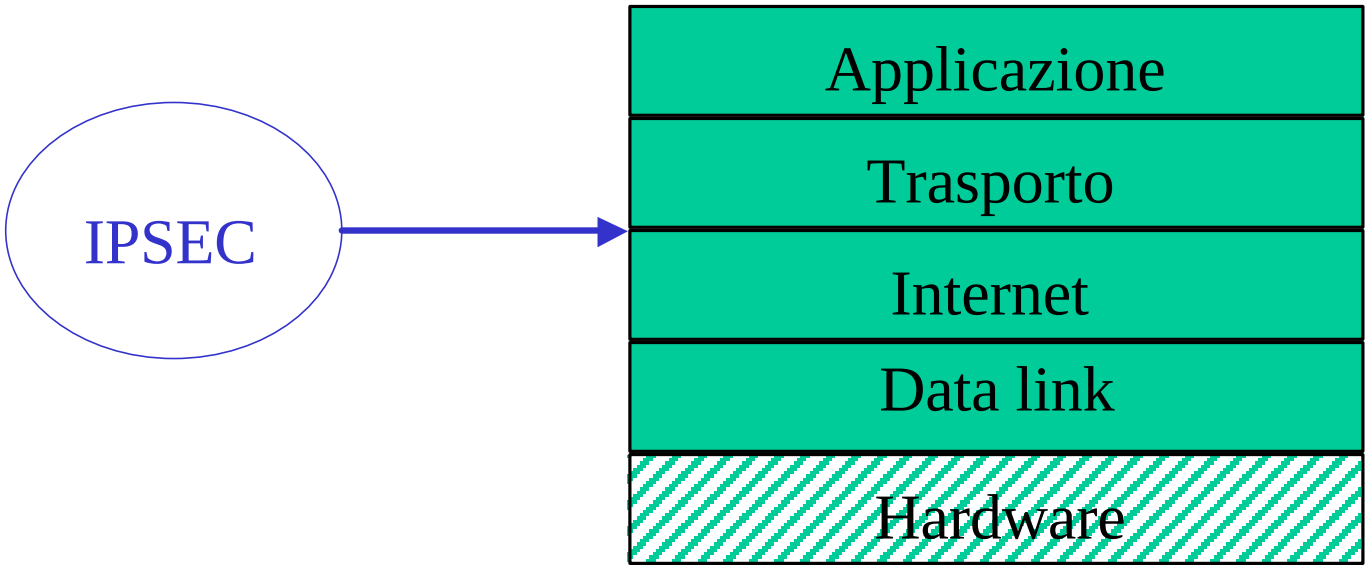
Indirizzamento IPv6 (2)

- Indirizzi unicast globali aggregabili: FP = 001 (RFC 2373)



- I RIR (es. RIPE) assegnano prefissi /48

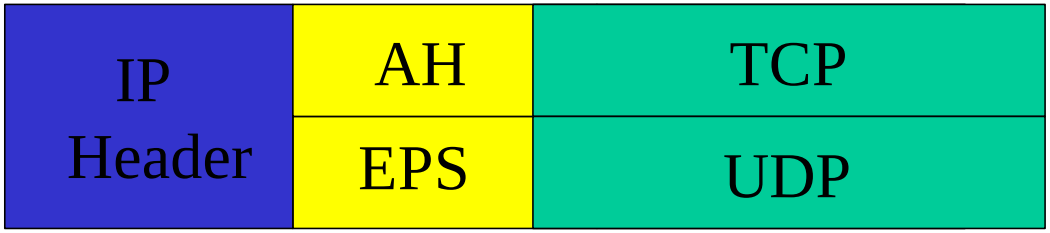
Livelli del TCP/IP



IP Security (1)

- IPSec RFC 2401
  - Protezione a livello 3 (Internet)
  - Opzionale in IPv4, parte integrante di IPv6
- ISAKMP (RFC 2408)
  - Negoziazione policy
  - Generazione chiavi

IP Security (2)



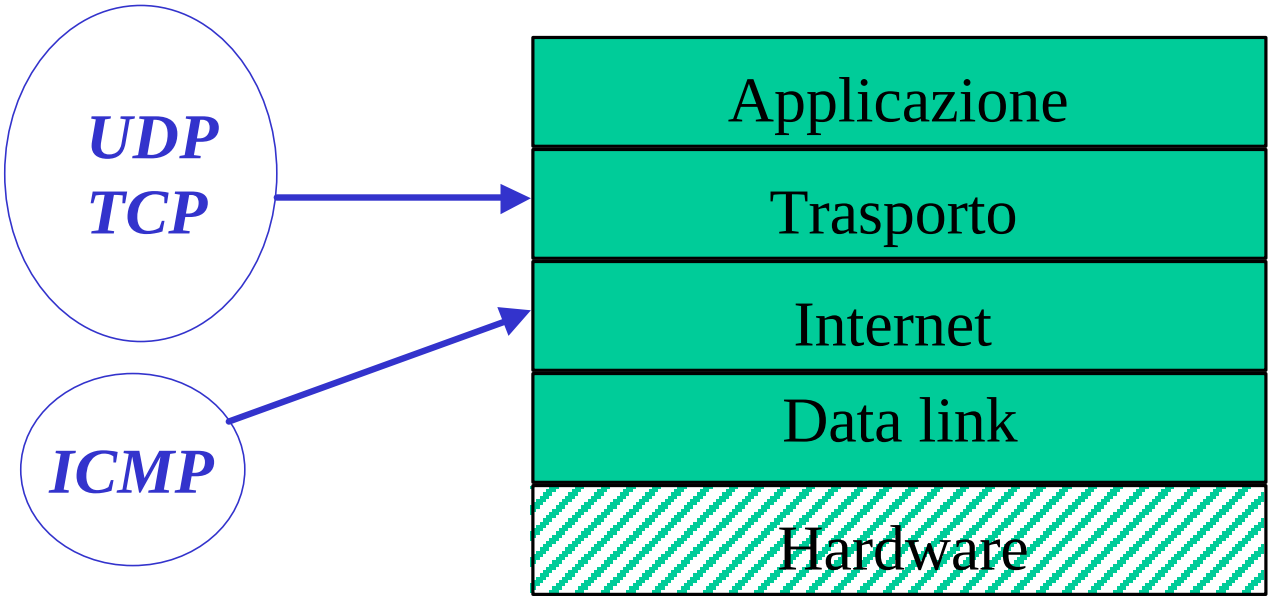
- Authentication Header (RFC 2402)
  - Integrita' datagrammi
  - Non repudiabilita' (se si usano certificati)
- Encapsulating Security Payload (RFC 2406)
  - Confidenzialita' dati
  - Integrita' dati
  - 2 modalita':
    - Tunnel (incapsula e cripta datagrammi IP)
    - Trasporto (incapsula e cripta TCP – UDP)

Internet Control Message Protocol

- Protocollo di servizio per IP.

- Vari tipi di messaggi:
  - Echo Reply
  - Destination Unreachable
  - Redirect
  - Source Quench

Livelli del TCP/IP



Porta

- Astrazione usata dai protocolli di trasporto per distinguere fra piu’ processi sullo stesso host
- Intero a 16 bit (0-65535)
- Per servizi standard identificativo assegnato dalla IANA

Socket

- Coppia (indirizzo IP, porta)
- Generalizzazione del meccanismo di accesso a file

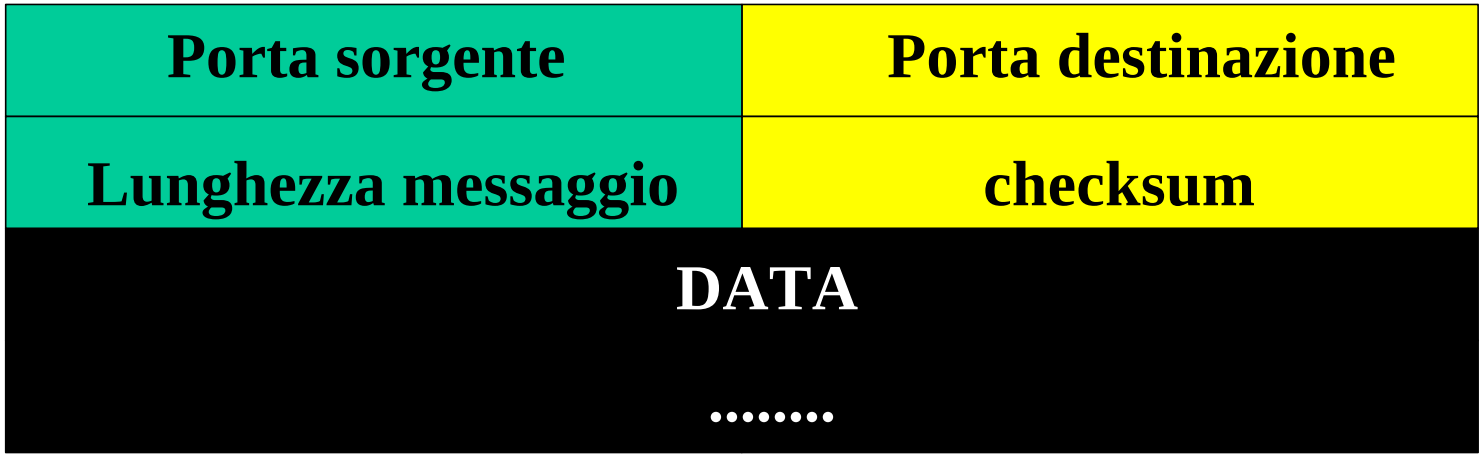
User Datagram Protocol (1)

- Protocollo connectionless (come IP)
  - nessuna garanzia di consegna
  - assenza controllo di flusso
  - assenza di correzione di errore

Controllo a cura del livello applicativo

User Datagram Protocol (2)

- Basato su socket



L’header e’ lungo 8 byte.

User Datagram Protocol (3)

- Pseudo Header (non viene trasmesso)

Verifica l’inoltro alla corretta destinazione

User Datagram Protocol (4)

- Tutti i controlli sul flusso sono a carico del livello applicativo

- Problema principale per la sicurezza di UDP e’ lo spoofing

- Consigliabile filtrare

BOOTstrap Protocol

- Risoluzione indirizzo IP client, subnet mask, gateway, boot server
  - Broadcast limitato (255.255.255.255) sia in richiesta che in risposta
  - Il protocollo si basa su UDP
  - Il server puo’ essere DHCP
- Il download del S.O. avviene poi con altro protocollo (es.: TFTP)

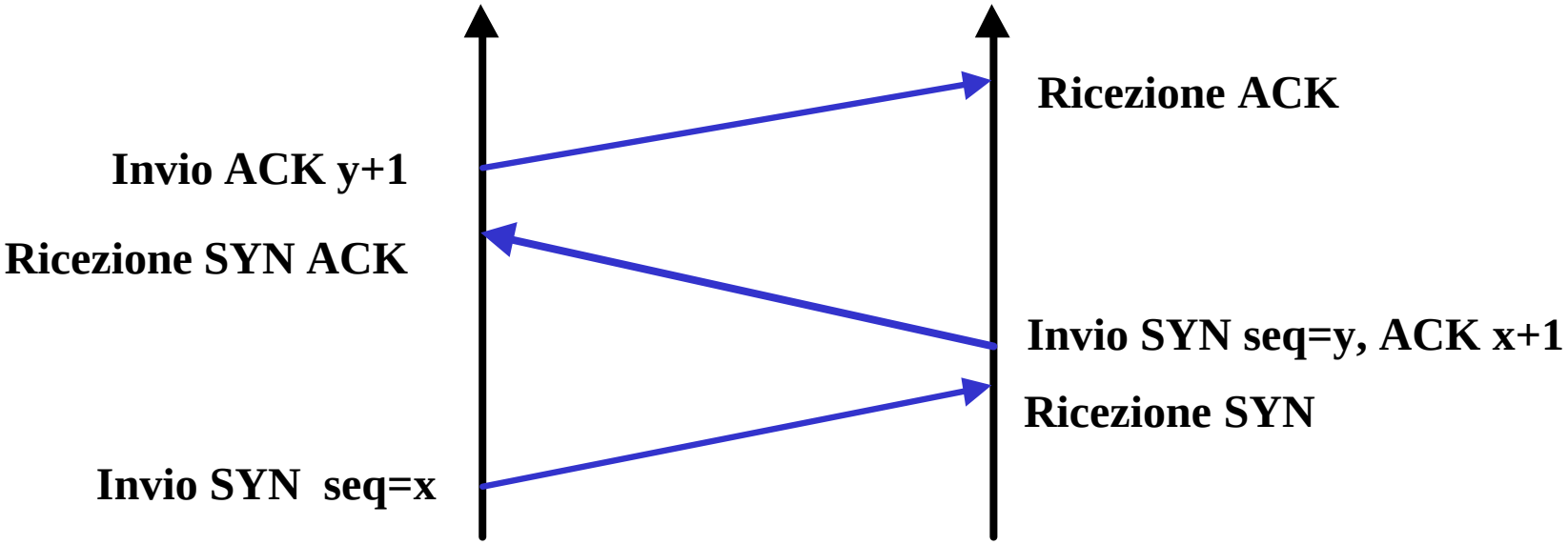
Trasmission Control Protocol (1)

- Protocollo connection-oriented
  - Controllo del flusso
  - Affidabilita’ della consegna
- Connessione virtuale tra due socket

<table>
<tr><td colspan="3">Porta sorgente</td><td>Porta destinazione</td></tr>
<tr><td colspan="4">Numero sequenza</td></tr>
<tr><td colspan="4">Numero di ACKW</td></tr>
<tr><td>Lun. H.</td><td>Res.</td><td>codice</td><td>finestra</td></tr>
<tr><td colspan="3">checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="3">options</td><td>padding</td></tr>
<tr><td colspan="4">DATA</td></tr>
<tr><td colspan="4">.....</td></tr>
</table>

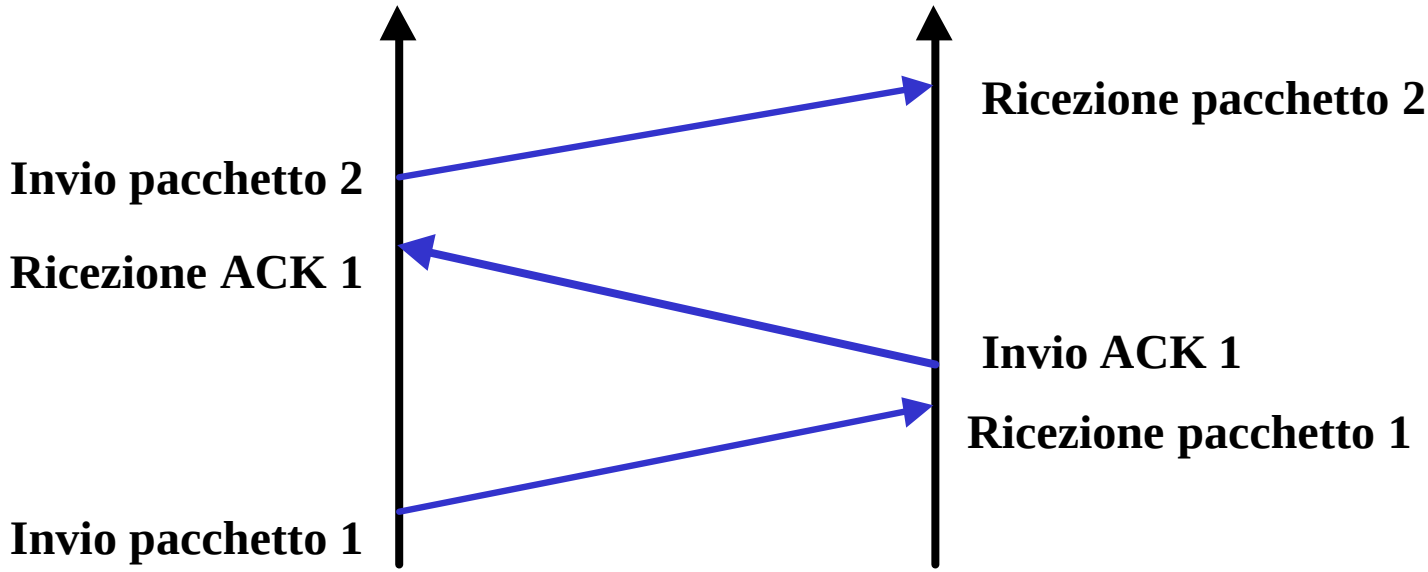
Trasmission Control Protocol (2)

- Inizio sessione TCP (handshake a 3 vie)



Trasmission Control Protocol (3)

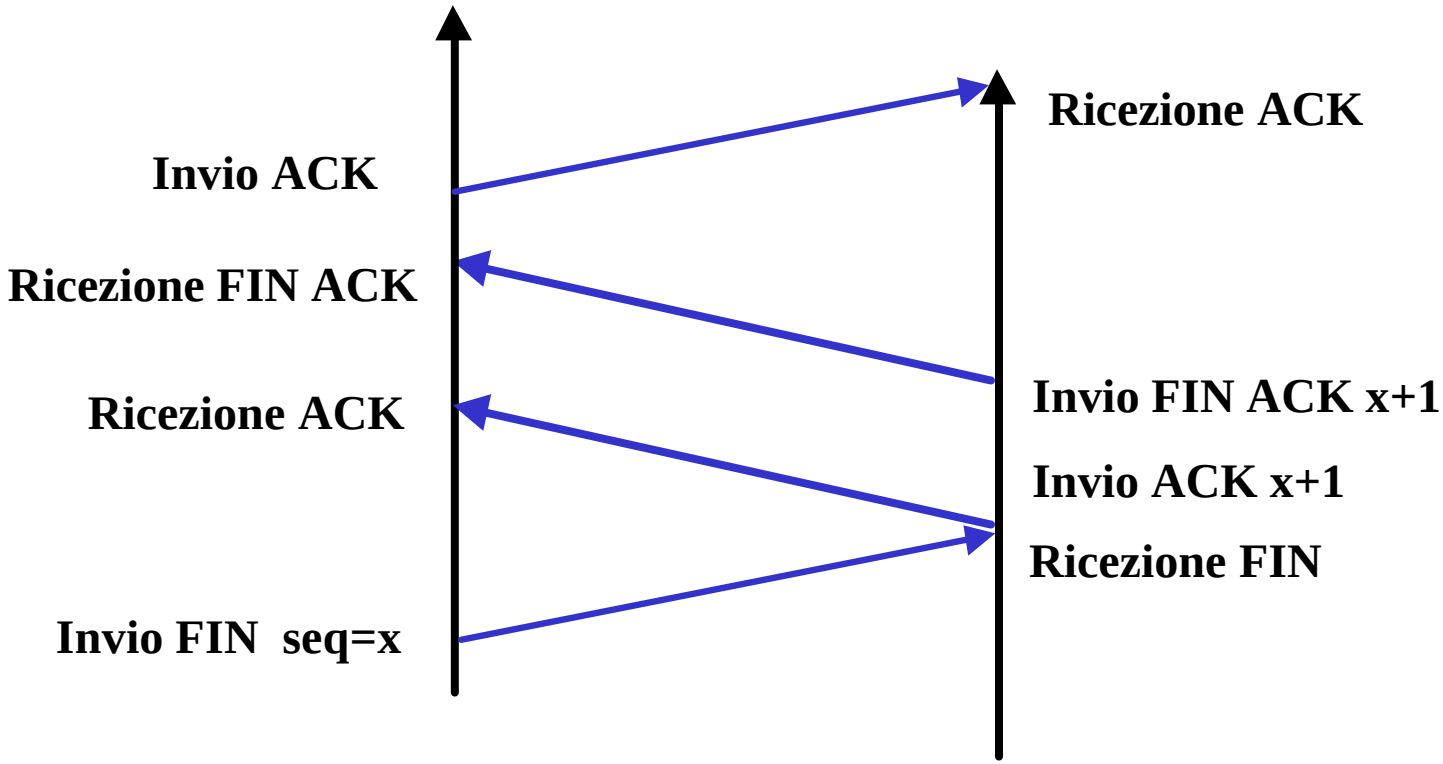
- Controllo trasmissione pacchetti



Il precedente meccanismo e' ottimizzato con il metodo delle "sliding windows" (controllato dal ricevente).

Trasmission Control Protocol (4)

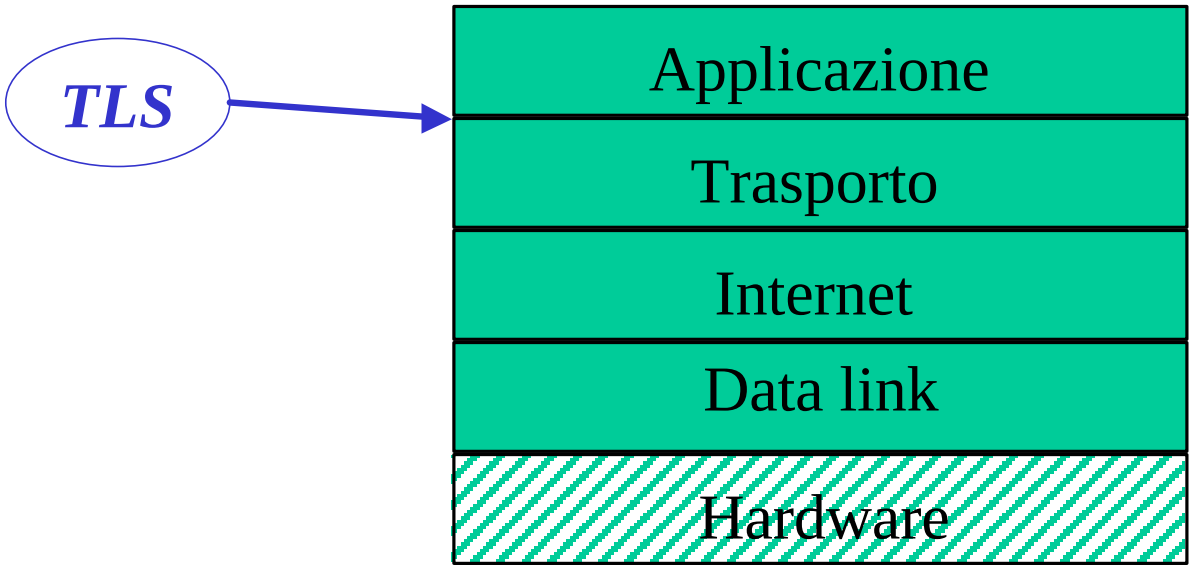
- Chiusura connessione



Trasmission Control Protocol (5)

- Spoofing piu’ difficile con il TCP
- Importante usare una sequenza non prevedibile
- Attenzione agli attacchi SYN-ACK!
- FIN
- RST

Livelli del TCP/IP



Transport Layer Security

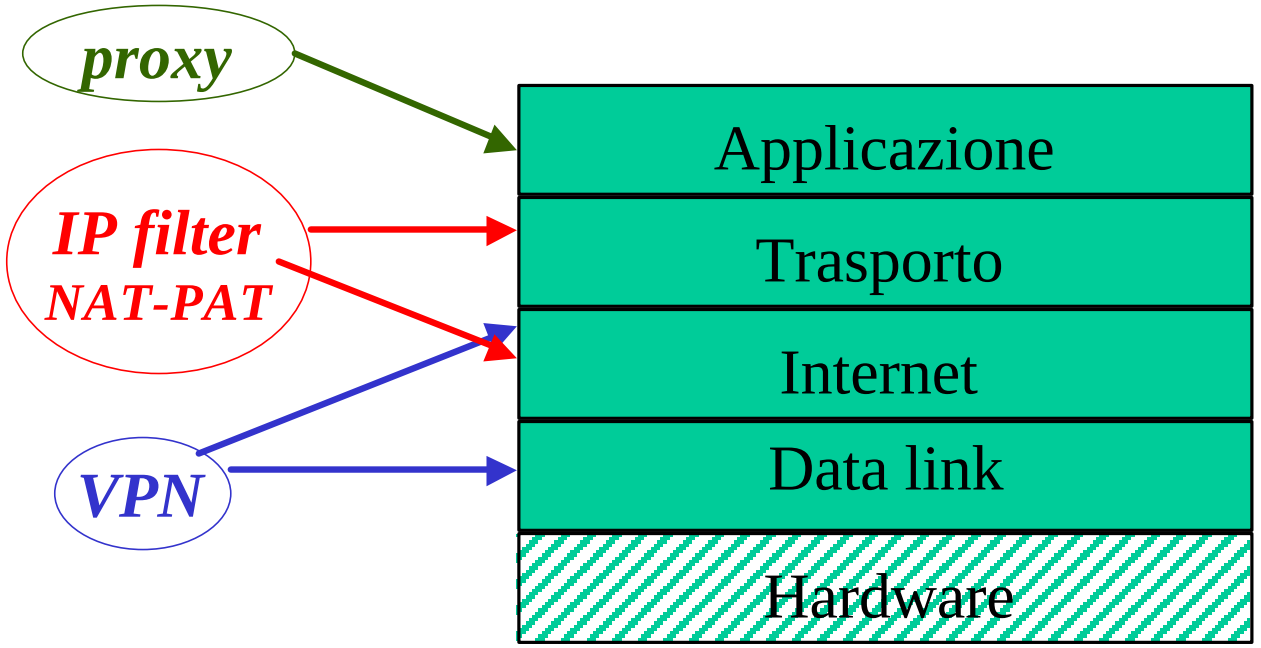
- Sicurezza sopra il livello di trasporto
- Evoluzione delle specifiche introdotte da NETSCAPE con SSL 3.0
- RFC 2246,2712,2817,2818
- Implementazioni basate su SSL 3.0:
  - OpenSSL
  - SSH

SSL/TLS (1)

- **SSL Handshake Protocol (SSLHP)**
  - **Autenticazione server (client)**
  - **Negoziazione algoritmo simmetrico da usare**
  - **Invio chiave segreta**
- **SSL Record Protocol (SSLRP)**
  - **Organizzazione dei dati**
  - **Criptazione/decriptazione dati**
- **SSL Alert Protocol**
  - **Inoltro messaggi di errore / allarme**
- **SSL Application Data Protocol**
  - **Trasporto dati**

tcpdump

SSL/TLS (2)


proxy
IP filter
NAT-PAT
VPN
Applicazione
Trasporto
Internet
Data link
Hardware

Bibliografia (1)

- IPv4
  - *Indirizzamento con CIDR:* RFC 1518
  - *Indirizzamento per intranet:* RFC 1918
- IPv6
  - *Definizione del protocollo:* RFC 2460
  - *Architettura degli indirizzi:* RFC 2373
  - *Estensioni al DNS:* RFC 1886, RFC 2874

Bibliografia (2)

- ARP
  - *Risoluzione indirizzi IP-Ethernet:* RFC 826
- RARP
  - *Descrizione del protocollo:* RFC 903
- BOOTP
  - RFC 2132
  - *Interoperabilita' tra DHCP e BOOTP:* RFC 1534

Bibliografia (3)

- IPSEC
  - *Definizione protocollo:* **RFC 2401**
  - *Authentication Header:* **RFC 2402**
  - *Encapsulating Security Payload:* **RFC 2406**
  - *ISAKMP:* **RFC 2408**
- TLS
  - *Definizione protocollo:* **RFC 2246**
  - *Integrazione di Kerberos in TLS:* **RFC 2712**
  - *HTTP e TLS:* **RFC 2817,2818**