



SAPIENZA  
UNIVERSITÀ DI ROMA

UNIVERSITÀ "SAPIENZA" DI ROMA  
FACOLTÀ DI INFORMATICA

---

## Reti di Elaboratori

---

Appunti integrati con il libro "Computer Networking: A Top-Down Approach", J. F. Kurose, K. W. Ross

*Author*  
Simone Bianco

25 maggio 2023

# Indice

<b>0 Introduzione</b>	<b>1</b>
<b>1 Introduzione alle reti</b>	<b>2</b>
1.1 Rete, Host e Collegamenti . . . . .	2
1.2 Struttura di Internet . . . . .	4
1.3 Pacchetti, Forwarding e Routing . . . . .	7
1.4 Misura delle prestazioni . . . . .	9
1.5 Stack protocollare TCP/IP . . . . .	14
<b>2 Livello di Applicazione</b>	<b>18</b>
2.1 Principi delle applicazioni di rete . . . . .	18
2.2 Web e Protocollo HTTP . . . . .	21
2.2.1 Messaggi di richiesta e risposta . . . . .	23
2.2.2 Versioni di HTTP . . . . .	26
2.2.3 Cookies e Web Caching . . . . .	27
2.3 Posta elettronica . . . . .	28
2.3.1 Protocolli SMTP e MIME . . . . .	29
2.3.2 Protocolli POP3 e IMAP . . . . .	31
2.4 Domain Name System (DNS) . . . . .	33
2.4.1 Gerarchia server DNS . . . . .	33
2.4.2 Protocollo DNS . . . . .	36
2.5 Trasferimento di file . . . . .	37
2.5.1 Protocollo FTP . . . . .	37
2.5.2 Protocollo BitTorrent . . . . .	39
<b>3 Livello di Trasporto</b>	<b>40</b>
3.1 Multiplexing e Demultiplexing . . . . .	40
3.2 Protocollo UDP . . . . .	42
3.3 Trasferimento affidabile dei dati . . . . .	44
3.3.1 Protocollo RDT 1.0 e 2.0 . . . . .	46
3.3.2 Protocollo RDT 2.1 e 2.2 . . . . .	47
3.3.3 Protocollo RDT 3.0 . . . . .	49
3.3.4 Go-back-N e Selective repeat . . . . .	51
3.4 Protocollo TCP . . . . .	56
3.4.1 Gestione del timeout e stima del RTT . . . . .	58
3.4.2 Controllo del flusso . . . . .	60
3.4.3 Gestione della connessione . . . . .	61

---

3.5	Controllo della congestione . . . . .	64
3.5.1	Cause e costi della congestione . . . . .	64
3.5.2	Controllo della congestione nel TCP . . . . .	67
3.6	Equità nei protocolli di trasporto . . . . .	73
<b>4</b>	<b>Livello di Rete</b>	<b>74</b>
4.1	Panoramica del livello di rete . . . . .	74
4.2	Architettura e funzionalità dei router . . . . .	76
4.2.1	Accodamento nelle porte . . . . .	79
4.2.2	Scheduling dei pacchetti . . . . .	81
4.2.3	Frammentazione dei datagrammi . . . . .	82
4.3	Protocollo IP . . . . .	83
4.3.1	Protocollo DHCP e indirizzamento gerarchico . . . . .	85
4.3.2	Servizio NAT e Protocollo IPv6 . . . . .	87
4.4	Protocollo ICMP e Traceroute . . . . .	90
4.5	API OpenFlow e forwarding generalizzato . . . . .	92
4.6	Principi architetturali di Internet . . . . .	94
4.7	Algoritmi di instradamento . . . . .	95
4.7.1	Algoritmo link-state di Dijkstra . . . . .	96
4.7.2	Algoritmo Distance-vector . . . . .	98
4.8	Instradamento intra-AS e inter-AS . . . . .	103
4.8.1	Protocolli RIP e OSPF . . . . .	104
4.8.2	Protocollo BGP . . . . .	107
4.9	Tipologie di instradamento . . . . .	111
4.9.1	Unicast e Broadcast . . . . .	111
4.9.2	Multicast . . . . .	113
4.10	Software Defined Networking (SDN) . . . . .	116
4.11	Amministrazione della rete . . . . .	121
<b>5</b>	<b>Livello di collegamento</b>	<b>124</b>
5.1	Panoramica del livello di collegamento . . . . .	124
5.2	Rilevamento e correzione degli errori . . . . .	126
5.3	Collegamenti e protocolli MAC . . . . .	129
5.3.1	Protocolli MAC a partizionamento del canale . . . . .	129
5.3.2	Protocolli MAC ad accesso casuale . . . . .	134
5.3.3	Protocollo MAC a rotazione . . . . .	138
5.4	Indirizzamento locale (indirizzo MAC) . . . . .	139
5.4.1	Protocollo ARP . . . . .	140
5.4.2	Instradamento verso un'altra sottorete . . . . .	142
5.5	LAN cablate . . . . .	144
5.5.1	Standard Ethernet . . . . .	144
5.5.2	Funzionalità dello switch . . . . .	145
5.5.3	Virtual LAN (VLAN) . . . . .	147
5.5.4	Reti point-to-point e protocollo PPP . . . . .	149
5.6	LAN wireless (WLAN) . . . . .	150
5.6.1	Caratteristiche ed architettura di reti wireless . . . . .	150
5.6.2	Gestione delle collisioni nel wireless . . . . .	153
5.6.3	Bluetooth ed RFID . . . . .	158

<b>6 Sicurezza della rete</b>	<b>160</b>
6.1 Principi di crittografia . . . . .	161
6.1.1 Crittosistema RSA . . . . .	164
6.2 Autenticazione ed Integrità del messaggio . . . . .	166
6.2.1 Firma digitale e Message digest . . . . .	169
6.2.2 Certification Authorities (CA) . . . . .	171
6.3 Sicurezza della posta elettronica . . . . .	173
6.4 Sicurezza a livello di trasporto (TLS) . . . . .	174
6.4.1 Protocollo TLS 1.3 . . . . .	177
6.5 Sicurezza a livello di rete (IPsec) . . . . .	179
6.5.1 Protocollo ESP . . . . .	180

# Capitolo 0

## Introduzione

# Capitolo 1

## Introduzione alle reti

### 1.1 Rete, Host e Collegamenti

#### Definition 1. Rete e Link

Una **rete** è un'infrastruttura composta da dispositivi detti **nodi della rete** in grado di scambiarsi informazioni tramite dei mezzi di comunicazione, wireless o cablati, detti **link (o collegamenti)**

#### Definition 2. Nodi di una rete

I **nodi** costituenti una rete vengono differenziati in **due macro-categorie**:

- **Sistemi terminali**, differenziati a loro volta in
  - **Host**, ossia un dispositivo di proprietà dell'utente dedicato ad eseguire applicazioni utente
  - **Server**, ossia un dispositivo di elevate prestazioni destinato ad eseguire programmi che forniscono un servizio a diverse applicazioni utente
- **Dispositivi di interconnessione**, ossia dei dispositivi atti a modificare o prolungare il segnale ricevuto, differenziati a loro volta in:
  - **Router**, ossia dispositivi che collegano una rete ad una o più reti
  - **Switch**, ossia dispositivi che collegano più sistemi terminali all'interno di una rete
  - **Modem**, ossia dispositivi in grado di trasformare la codifica dei dati in segnale e viceversa

In particolare, classifichiamo le varie tipologie di rete in:

- **Personal Area Network (PAN)**, avente scala ridotta, solitamente equivalente a pochi metri (es: una rete Bluetooth)

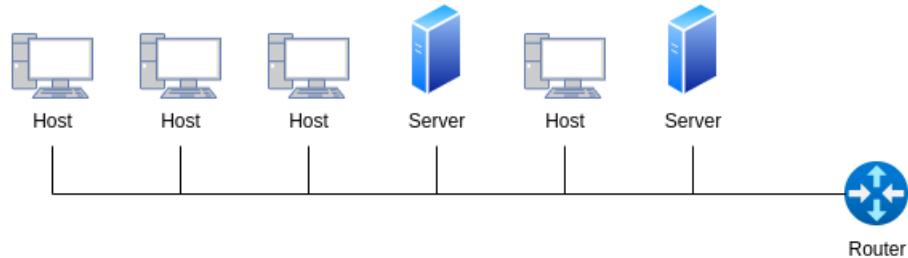
- **Local Area Network (LAN)**, solitamente corrispondente ad una rete privata che collega i sistemi terminali di un appartamento (es: una rete Wi-Fi o Ethernet). Ogni sistema terminale possiede un indirizzo che lo identifica univocamente all'interno della LAN.

Si differenziano in **LAN con cavo condiviso**, ossia dove tutti i dispositivi sono connessi al router tramite un cavo comune, e **LAN con switch**, ossia dove tutti i dispositivi sono connessi ad uno o più switch, i quali a loro volta sono connessi al router

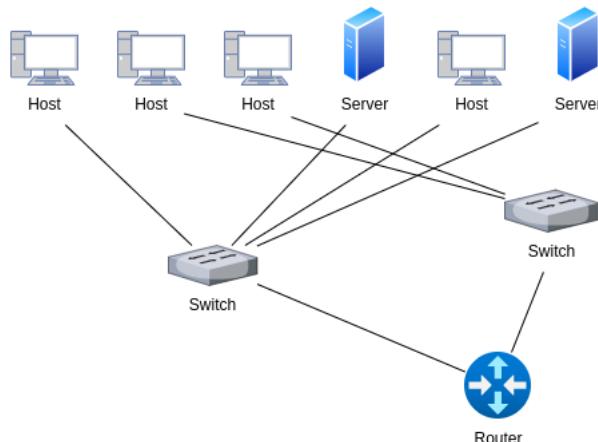
- **Metropolitan Area Network (MAN)**, avente scala pari ad una città
  - **Wide Area Network (WAN)**, avente scala pari ad un paese o una nazione, solitamente gestita da un **Internet Service Provider (ISP)**.
- Si differenziano in **WAN point-to-point**, ossia collegante due reti tramite un singolo mezzo di trasmissione, e **WAN a commutazione**, ossia collegante più reti tramite più mezzi e dispositivi di collegamento
- **L'Internet**, avente scala globale

Esempi:

- **LAN a cavo condiviso**



- **LAN con switch**



- **Rete composta**



I supporti fisici utilizzabili per una trasmissione si differenziano in:

- **Doppino intrecciato** (ad esempio un cavo Ethernet), composto da due fili di rame isolati, uno utilizzato per inviare i dati ed uno per riceverli
- **Cavo coassiale**, composto da due conduttori di rame concentrici, entrambi bidirezionali, avente una larghezza di banda maggiore
- **Cavo in fibra ottica**, composto da una fibra di vetro che trasporta impulsi luminosi (dunque alla velocità della luce) al suo interno, ognuno rappresentante un singolo bit
- **Trasmissione wireless**, realizzata tramite l'invio di un segnale radio propagato nell'aria (es: rete cellulare, satellitare o Wi-Fi)

## 1.2 Struttura di Internet

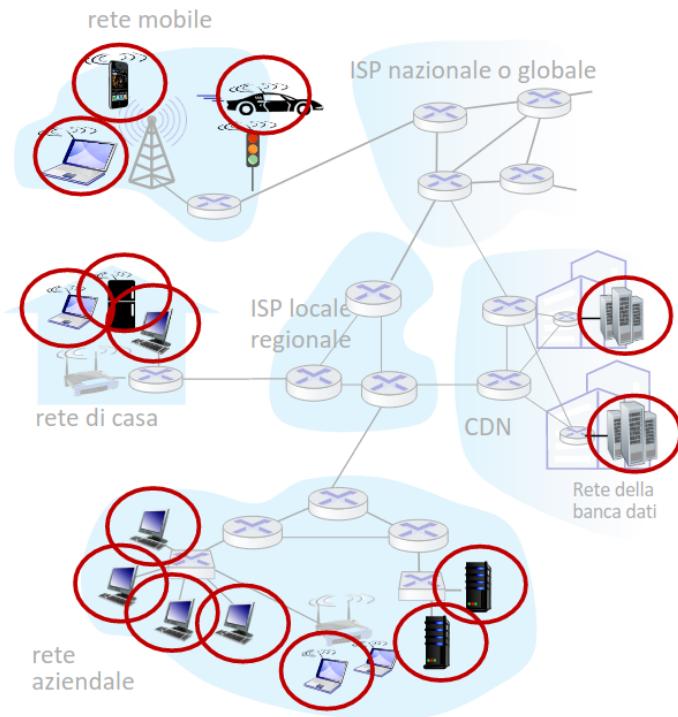
### Definition 3. Rete internet

Definiamo come **internet** (abbreviativo di internetwork) una **rete di reti**, ossia una rete che mette in comunicazione due o più reti tra di loro.

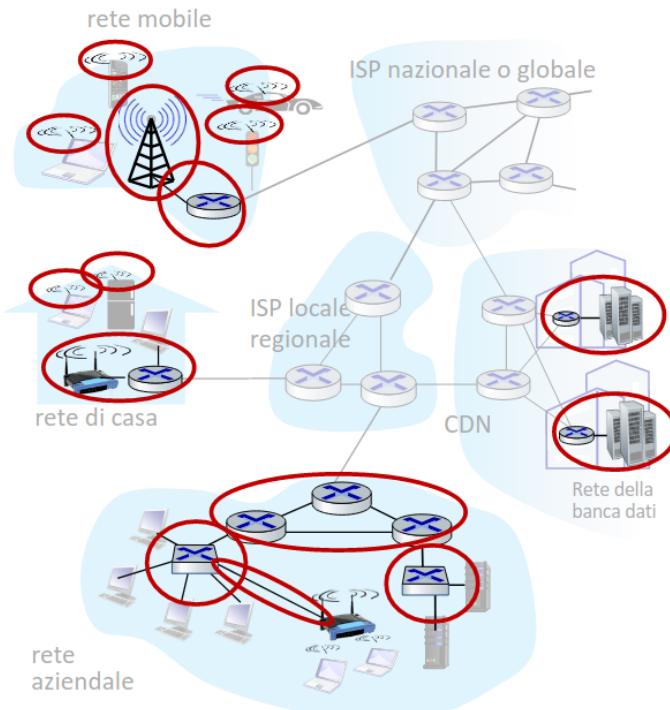
**Attenzione:** nonostante ciò che viene comunemente chiamato l'**Internet** sia una internet, è necessario puntualizzare che con tale termine comune viene indicata la **rete di tutte le reti**.

Al suo interno, la struttura di Internet risulta essere composta da:

- **Periferia della rete (network edge)**, corrispondente all'insieme di tutti i sistemi terminali connessi.

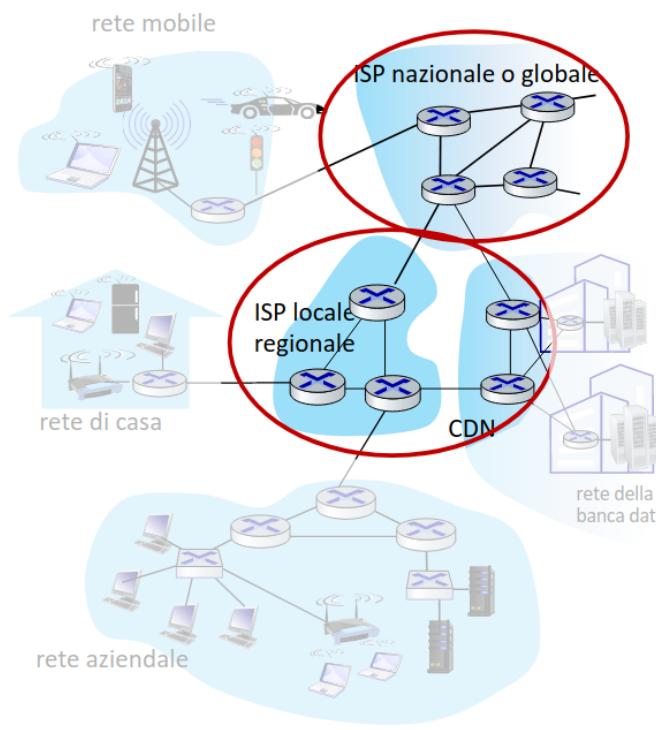


- **Reti di accesso (access network)**, corrispondente ai collegamenti fisici che connettono un sistema terminale al primo **edge router**, ossia il primo router presente nel percorso dal sistema terminale di origine ad un qualsiasi altro sistema terminale di destinazione.



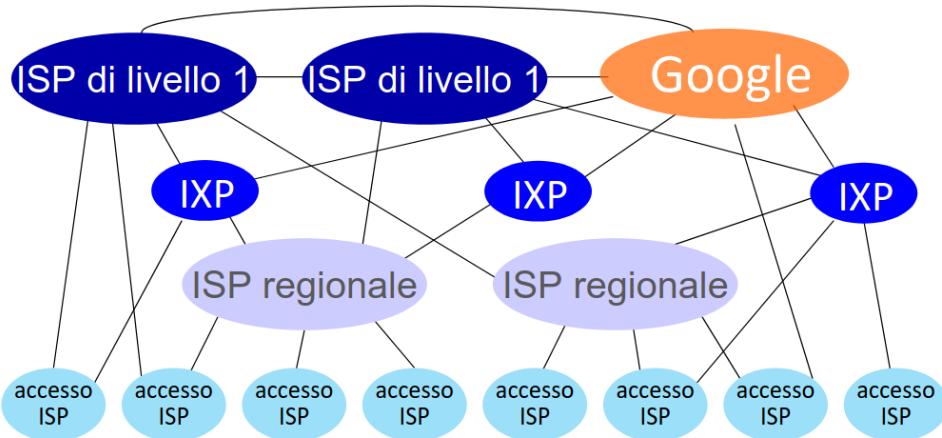
In particolare, l'accesso all'Internet può essere effettuato in più modi:

- **Accesso via cavo**, tramite supporti fisici connessi direttamente ad una rete di distribuzione, detta **cable headend** (es: il centralino di un ISP).
- **Accesso via Digital Subscriber Line (DSL)**, dove viene utilizzata la linea telefonica esistente per collegarsi alla rete dell'ISP
- **Accesso via Wireless LAN (WLAN)**, tramite un collegamento wireless ad una stazione base detta **access point** connessa con il router, a sua volta connesso con un cable headend
- **Accesso via rete cellulare**, dove viene utilizzata la rete cellulare esistente per collegarsi alla rete dell'ISP
- **Accesso via rete aziendale**, tramite una rete aziendale (o universitaria, privata, ...) direttamente connessa ad Internet
- **Nucleo di rete (core o backbone)**, ossia un sistema di router interconnessi tra di loro, corrispondente all'insieme di nodi cui viene realizzata la vera interconnessione tra tutte le reti.



In particolare, all'interno del backbone di Internet sono presenti **più livelli di reti ISP** (es: regionali, nazionali, aziendali, ...), le quali devono essere interconnesse tra di loro tramite degli **Internet Exchange Point (IXP)**.

Inoltre, nel recente periodo, nel backbone di Internet sono state integrate anche delle grandi reti private aziendali, ossia le **reti dei content provider** (es: Google, Netflix, ...), le quali, ormai, funzionano come vere e proprie ISP.



## 1.3 Pacchetti, Forwarding e Routing

### Definition 4. Pacchetto e Velocità di trasmissione

Dato un messaggio  $m$  da trasferire tra due terminali, definiamo come **pacchetti** l'insieme di blocchi di  $L$  bit tali che  $m = \{p_1, \dots, p_k\}$ .

Ogni pacchetto viene trasmesso nella rete ad una **velocità di trasmissione  $R$**  (anche detta larghezza di banda o capacità del collegamento).

### Definition 5. Forwarding e Routing

Le funzioni fondamentali di una rete si dividono in:

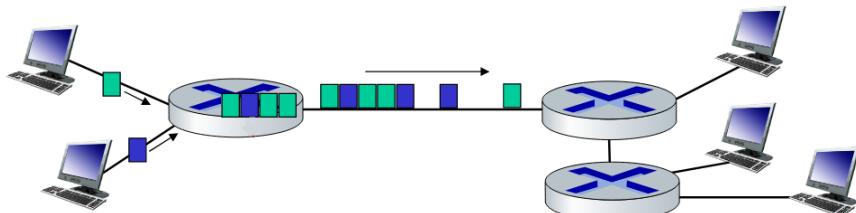
- **Forwarding o Switching (commutazione)**, ossia un'azione locale tramite cui vengono spostati i pacchetti in arrivo dal collegamento di ingresso del router al collegamento appropriato di uscita. Viene effettuato attraverso una **local forwarding table**, contenente gli indirizzi dei nodi locali
- **Routing (instradamento)**, ossia un'azione globale tramite cui vengono determinati i percorsi origine-destinazione seguiti dai pacchetti. Viene effettuato tramite **algoritmi di instradamento**

In particolare, la commutazione può avvenire in due modi:

- **Commutazione di pacchetto:**

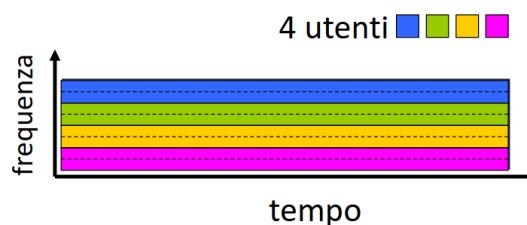
- La rete inoltra i pacchetti da un router all'altro attraverso i collegamenti presenti nell'instradamento dall'origine alla destinazione.
- Una volta inviato, un pacchetto deve completamente raggiungere il nodo a cui sta attualmente venendo inviato prima di poter essere trasmesso al collegamento successivo (**store & forward**)

- Se la velocità di trasmissione sul link di entrata supera la velocità di trasmissione di quello in uscita, i pacchetti verranno messi all'interno di una coda, in attesa di essere trasmessi sul link di uscita
- Se il buffer della coda raggiunge capienza massima, i pacchetti verranno scartati (**perdita di pacchetti**), per poi, se necessario, essere rinviati

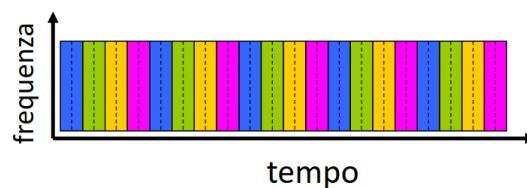


- **Commutazione di circuito:**

- La banda dei mezzi di trasmissione viene **suddivisa** in parti, riservando ognuna di essere ad una comunicazione tra un'origine ed una destinazione.
- Per via di tale suddivisione, il numero di utenti massimo della rete risulta essere **limitato dal numero di suddivisioni**
- La suddivisione può essere effettuata in due modalità:
  - \* **Frequency Division Multiplexing (FDM)**, dove le frequenze del mezzo di trasmissione vengono suddivise in bande di frequenza, ognuna di esse riservata ad una singola comunicazione, la quale può utilizzare al massimo la banda ad essa riservata



- \* **Time Division Multiplexing (TDM)**, dove il tempo viene suddiviso in slot, ognuno di essi riservato ad una singola comunicazione, la quale può utilizzare l'intera banda del mezzo per il breve lasso di tempo dedicato.



Nonostante la **commutazione di pacchetto** permetta l'accesso di un numero maggiore di utenti e non necessiti di stabilire una configurazione del collegamento, la presenza di una possibile perdita di pacchetti rende tale tipo di commutazione prettamente ottimo per **trasmissioni "bursty"**, ossia intermittenti e con lunghi periodi di inattività.

## 1.4 Misura delle prestazioni

### Definition 6. Larghezza di banda e Transmission rate

Con il termine **larghezza di banda (bandwidth)** indichiamo due concetti strettamente legati tra loro:

- La quantità (espressa in  $Hz$ ) rappresentante la **larghezza dell'intervallo di frequenze** utilizzato dal sistema trasmittivo, ossia l'intervallo di frequenze utilizzato dal sistema trasmittivo. Maggiore è tale quantità, maggiore è la quantità di informazioni veicolabili tramite il mezzo di trasmissione.
- La quantità (espressa in  $b/s$ ) detta anche **transmission rate (o bit rate)** rappresentante la **quantità di bit al secondo** che un link **garantisce di trasmettere**. Tale quantità è proporzionale alla larghezza di banda (in  $Hz$ )

### Definition 7. Throughput

Con il termine **throughput** indichiamo la **quantità di bit** al secondo che **passano attraverso un nodo** della rete.

### Observation 1

A differenza del **transmission rate**, il quale fornisce una misura della **potenziale velocità di un link**, il **throughput** fornisce una misura dell'**effettiva velocità di un link**.

In generale, dunque, si ha che

$$T < R$$

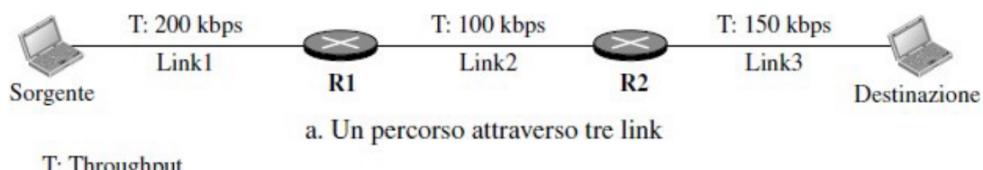
dove  $T$  è il throughput e  $R$  è il transmission rate

### Definition 8. Collo di bottiglia

Dato un percorso end-to-end, ossia tra un dispositivo e un altro, definiamo come **collo di bottiglia** il link limitante il throughput dei link presenti su tale percorso

Esempio:

- Consideriamo il seguente percorso



- Il link  $L_2$  risulta essere il collo di bottiglia di tale percorso, limitando il throughput del percorso a 100 kb/s

**Definition 9. Delay di trasmissione**

Definiamo come **delay (o latenza) di trasmissione** il tempo necessario ad un nodo per immettere un pacchetto su un link, corrispondente a:

$$D_t = \frac{L}{R}$$

dove  $L$  è la dimensione del pacchetto e  $R$  è il transmission rate del link

**Definition 10. Delay di propagazione**

Definiamo come **delay (o latenza) di propagazione** il tempo impiegato dall'**ultimo bit di blocco di dati** posto su un link ad essere propagato fino al nodo di destinazione, corrispondente a:

$$D_p = \frac{k}{v}$$

dove  $k$  è la lunghezza del link e  $v$  è la velocità di propagazione del link

**Definition 11. Delay di un pacchetto**

Definiamo come **delay (o latenza) di un pacchetto** il tempo totale necessario ad un pacchetto per essere inviato completamente da un nodo origine ad un nodo destinatario

$$D_n = D_e + D_q + D_t + D_p$$

dove:

- $D_e$  è il **delay di elaborazione del nodo**, dipendente dalle operazioni di controllo svolte dal nodo
- $D_q$  è il **delay di queueing**, ossia l'attesa del pacchetto all'interno della coda del nodo prima di essere trasmesso, dipendente dalla quantità di pacchetti presenti nella coda
- $D_t$  è il delay di trasmissione del link
- $D_p$  è il delay di propagazione del link

**Proposition 1. Prodotto rate per delay di propagazione**

Dato un link con transmission rate  $R$  e delay di propagazione  $D_p$ , il prodotto

$$B_{max} = R \cdot D_p = \frac{L \cdot k}{D_t \cdot v}$$

rappresenta il **massimo numero di bit distribuiti tutto sul cavo** contemporaneamente

**Esempi:**

1. Si consideri un router A che trasmette pacchetti, ognuno di lunghezza  $L = 4000$  bit, su un canale di trasmissione con rate  $R = 10 \text{ Mb/s}$  verso un router B all'altro estremo del link. Si supponga che il delay di propagazione sia pari a 0.2 ms.

- Quanto impiega il router A a trasmettere un pacchetto al router B?

$$D_t = \frac{L}{R} = \frac{4 \cdot 10^3 \text{ b}}{10^7 \text{ b/s}} = 4 \cdot 10^{-4} \text{ s} = 0.4 \text{ ms}$$

- Quanto impiega il router A a trasmettere un bit al router B?

$$D_{1b} = \frac{1}{R} = \frac{1 \text{ b}}{10^7 \text{ b/s}} = 10^{-7} \text{ s} = 0.1 \mu\text{s}$$

- Qual è il massimo numero di pacchetti al secondo che possono essere trasmessi sul link?

$$\begin{aligned} 1 \text{ P} &= 4000 \text{ b} \implies 1 \text{ b} = \frac{1}{4000} \text{ P} \implies \\ &\implies R = 10^7 \text{ b/s} = \frac{10^7}{4000} \text{ P/s} = \frac{1}{4} \cdot 10^3 \text{ P/s} = 2500 \text{ P/s} \end{aligned}$$

- Supponendo che il router A invii i pacchetti uno dopo l'altro senza introdurre ritardi tra la trasmissione di un pacchetto e il successivo, quanto tempo impiega il router B a ricevere 4 pacchetti?

Poiché i pacchetti vengono inviati senza alcun delay tra di essi, possiamo considerare tali pacchetti come un unico grande pacchetto di dimensione  $4 \cdot L$ , implicando che

$$D_{4t} = \frac{4 \cdot L}{R} = \frac{16 \cdot 10^3 \text{ b}}{10^7 \text{ b/s}} = 16 \cdot 10^{-4} \text{ s} = 1.6 \text{ ms}$$

Inoltre, per lo stesso motivo, il tempo di propagazione rimarrà inalterato, poiché esso non dipende dalla lunghezza del pacchetto, ma solo dalla lunghezza e della velocità di propagazione del link. Di conseguenza, il tempo totale impiegato sarà  $1.6 \text{ ms} + 0.2 \text{ ms} = 1.8 \text{ ms}$

- Qual è il massimo numero di bit e il numero di pacchetti che possono essere presenti sul canale?

$$P_{max} = R \cdot D_p = 10^7 \text{ b/s} \cdot 0.2 \text{ ms} = 2000 \text{ b} = \frac{1}{2} \text{ P}$$

2. Si consideri un host A che vuole inviare un file molto grande, 4 milioni di byte, a un host B. Il percorso tra A e B ha 3 link  $L_1, L_2, L_3$ , ognuno di lunghezza 300 km, ciascuno con rate rispettivo  $R_1 = 500 \text{ kb/s}$ ,  $R_2 = 2 \text{ Mb/s}$  e  $R_3 = 1 \text{ Mb/s}$ .

- Assumendo l'assenza di ulteriore traffico nella rete, qual è il throughput per il file transfer?

Poiché il link  $L_1$  risulta essere il collo di bottiglia del percorso, il throughput risulta essere  $R_1 = 500 \text{ kb/s}$

- Qual è il tempo totale impiegato per trasferire il file all'host B assumendo che i link siano cavi in fibra ottica?

Poiché non vi è specificata la lunghezza di ogni pacchetto, assumiamo che il file venga inviato come un unico grande pacchetto, implicando che  $L = 4 \cdot 10^6 \text{ b} = 32 \cdot 10^6 \text{ b}$ .

Di conseguenza, si ha che:

$$D_t(L_1) = \frac{32 \cdot 10^6 \text{ b}}{5 \cdot 10^5 \text{ b/s}} = 64 \text{ s}$$

$$D_t(L_2) = \frac{32 \cdot 10^6 \text{ b}}{2 \cdot 10^6 \text{ b/s}} = 16 \text{ s}$$

$$D_t(L_3) = \frac{32 \cdot 10^6 \text{ b}}{1 \cdot 10^6 \text{ b/s}} = 32 \text{ s}$$

Poiché  $L_1, L_2, L_3$  sono cavi in fibra ottica, la velocità di propagazione su di essi corrisponde alla velocità della luce, pari a  $\sim 3 \cdot 10^8 \text{ m/s}$ . Dunque, il delay di propagazione di ogni link corrisponderà a:

$$D_p = \frac{3 \cdot 10^5 \text{ m}}{3 \cdot 10^8 \text{ m/s}} = 1 \text{ ms}$$

Infine, concludiamo che il tempo totale impiegato corrisponda a:

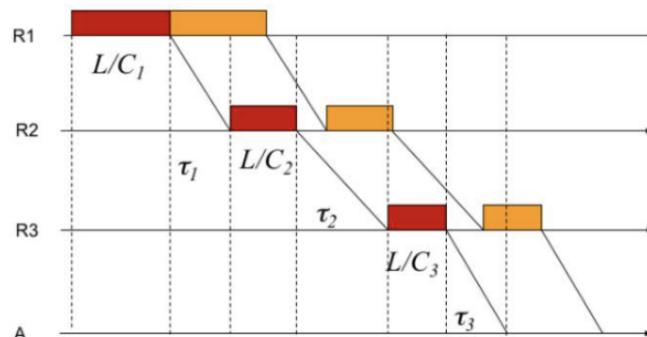
$$D_{tot} = D_t(L_1) + D_t(L_2) + D_t(L_3) + 3 \cdot D_p = 64 \text{ s} + 16 \text{ s} + 32 \text{ s} + 3 \cdot 1 \text{ ms} = 112,003 \text{ s}$$

3. Si consideri la rete nella seguente figura, dove  $C_1, C_2, C_3$  e  $\tau_1, \tau_2, \tau_3$  sono rispettivamente i transmission rate e i delay di propagazione dei tre link.

Al tempo  $t = 0$ , la coda di uscita di  $R_1$  contiene 2 pacchetti diretti ad  $A$ . Assumendo che la lunghezza dei pacchetti sia  $L = 512 \text{ b}$ , si indichi per ciascun pacchetto l'istante in cui esso viene completamente ricevuto da  $A$ .



Per aiutarci durante il calcolo, tracciamo il contenuto di ogni coda al passare del tempo:



Dunque, il tempo totale impiegato dal primo pacchetto corrisponderà a:

$$T_1 = \frac{L}{C_1} + \tau_1 + \frac{L}{C_2} + \tau_2 + \frac{L}{C_3} + \tau_3 = 4 \text{ ms} + 1 \text{ ms} + 2 \text{ ms} + 2 \text{ ms} + 1 \text{ ms} + 1 \text{ ms} = 11 \text{ ms}$$

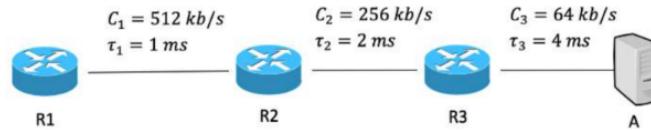
Analogamente, il tempo totale impiegato dal secondo pacchetto corrisponderà a:

$$T_2 = 2 \cdot \frac{L}{C_1} + \tau_1 + \frac{L}{C_2} + \tau_2 + \frac{L}{C_3} + \tau_3 = 8 \text{ ms} + 1 \text{ ms} + 2 \text{ ms} + 2 \text{ ms} + 1 \text{ ms} + 1 \text{ ms} = 15 \text{ ms}$$

4. Si consideri la rete nella seguente figura, dove  $C_1, C_2, C_3$  e  $\tau_1, \tau_2, \tau_3$  sono rispettivamente i transmission rate e i delay di propagazione dei tre link.

Al tempo  $t = 0$ , la coda di uscita di  $R_1$  contiene 2 pacchetti diretti ad  $A$ . Assumendo che la lunghezza dei pacchetti sia  $L = 512 \text{ b}$ , si indichi per ciascun pacchetto l'istante in cui esso viene completamente ricevuto da  $A$ .

Inoltre, supponendo che vi siano  $n$  pacchetti, si indichi una formula generica descrivente per ciascun pacchetto l'istante in cui esso viene completamente ricevuto da  $A$



Come nel caso precedente, tracciamo il contenuto di ogni coda al passare del tempo:



Il tempo totale impiegato dal primo pacchetto corrisponderà a:

$$T_1 = \frac{L}{C_1} + \tau_1 + \frac{L}{C_2} + \tau_2 + \frac{L}{C_3} + \tau_3 = 1 \text{ ms} + 1 \text{ ms} + 2 \text{ ms} + 2 \text{ ms} + 8 \text{ ms} + 4 \text{ ms} = 18 \text{ ms}$$

Notiamo come, a differenza del caso precedente, il secondo pacchetto giunge nelle code successive mentre il primo pacchetto deve essere ancora completamente spedito, implicando che esso debba essere inserito nella coda di attesa.

Dunque, una volta raggiunta la coda finale, il secondo pacchetto potrà essere inviato solo una volta completato il primo pacchetto.

Di conseguenza, il suo tempo totale di ricezione corrisponde a:

$$T_2 = T_1 + \frac{L}{C_3} = 18 \text{ ms} + 8 \text{ ms} = 26 \text{ ms}$$

Applicando lo stesso ragionamento nel caso di  $n$  pacchetti, la formula generica descrivente l'istante di ricezione dell' $n$ -esimo pacchetto corrisponde a:

$$T_n = T_{n-1} + \frac{L}{C_3} = T_{n-2} + 2 \cdot \frac{L}{C_3} = \dots = T_1 + (n-1) \frac{L}{C_3} = 18 \text{ ms} + 8(n-1) \text{ ms}$$

## 1.5 Stack protocollare TCP/IP

### Definition 12. Protocollo

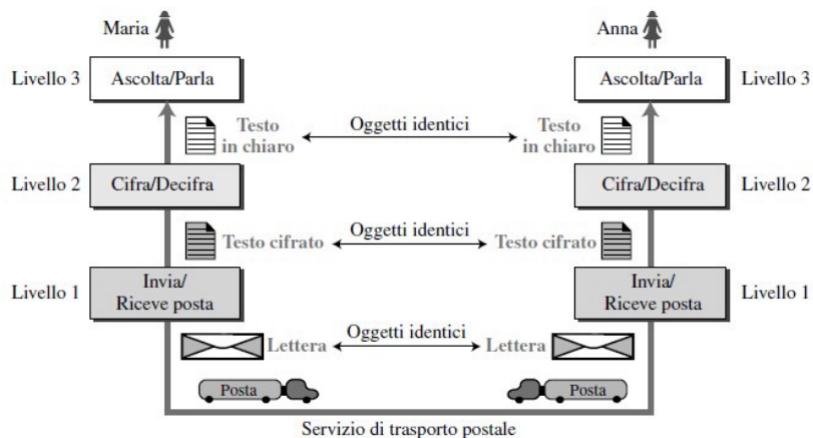
Un **protocollo** definisce l'insieme di **regole** che il dispositivo mittente e il dispositivo destinatario, così come tutti i sistemi intermedi coinvolti, devono rispettare per essere in grado di comunicare.

In situazioni più complesse, potrebbe essere opportuno suddividere i compiti necessari alla comunicazione fra **più livelli (layer)**, nel qual caso è richiesto **un protocollo per ciascun livello**. Tramite un layering dei protocolli, dunque, è possibile suddividere un compito complesso in compiti più semplici, ognuno gestibile da un singolo protocollo.

In particolare, ogni layer è **indipendente dagli altri** (modularizzazione), utilizzando i servizi forniti dal layer inferiore e offrendo servizi al layer superiore.

Ogni layer, dunque, può essere considerato come una **black box** con opportuni ingressi ed uscite, senza necessità di essere a conoscenza delle modalità con cui i dati in ingresso vengano trasformati in quelli di uscita.

Quando è richiesta una **comunicazione bidirezionale**, ciascun layer deve essere in grado di effettuare entrambi i compiti richiesti, ossia manipolare i dati in input per inviarli al livello superiore o manipolarli per inviarli al livello inferiore.



In particolare, l'effetto ottenuto tramite una suddivisione in uno stack di layer equivalenti permette l'instaurazione di un **collegamento logico** tra ogni livello dello stack: il protocollo implementato in ciascun livello specifica una comunicazione diretta tra i pari livelli delle due parti: il layer  $N$  di un dispositivo comunica solo ed esclusivamente con il layer  $N$  di tutti i dispositivi.



Inoltre, per via dell'estrema modularizzazione ottenuta, viene facilitata la manutenzione e l'aggiornamento del sistema, poiché il cambiando dell'implementazione del servizio di un layer rimane trasparente al resto del sistema.

### Definition 13. Stack protocollare TCP/IP

La principale forma di stack protocollare utilizzata corrisponde allo **stack protocolare TCP/IP**, la cui struttura a layer corrisponde a:

- **Livello di Applicazione**, il quale fornisce supporto alle applicazioni facente uso della rete (protocolli HTTP, SMTP, FTP, DNS, ...).
- **Livello di Trasporto**, il quale gestisce il trasferimento dei pacchetti dal processo del dispositivo mittente a quello del dispositivo destinatario (protocolli TCP, UDP, ...).
- **Livello di Rete**, il quale gestisce l'instradamento dei pacchetti dall'origine alla destinazione (protocolli IP, ...).
- **Livello di Collegamento (o Link)**, il quale gestisce la trasmissione dei pacchetti da un nodo a quello successivo sul percorso (protocolli Ethernet, Wi-Fi, PPP, ...). Lungo il percorso, un pacchetto può essere gestito da protocolli diversi.
- **Livello Fisico**, dove avviene il vero e proprio trasferimento dei singoli bit

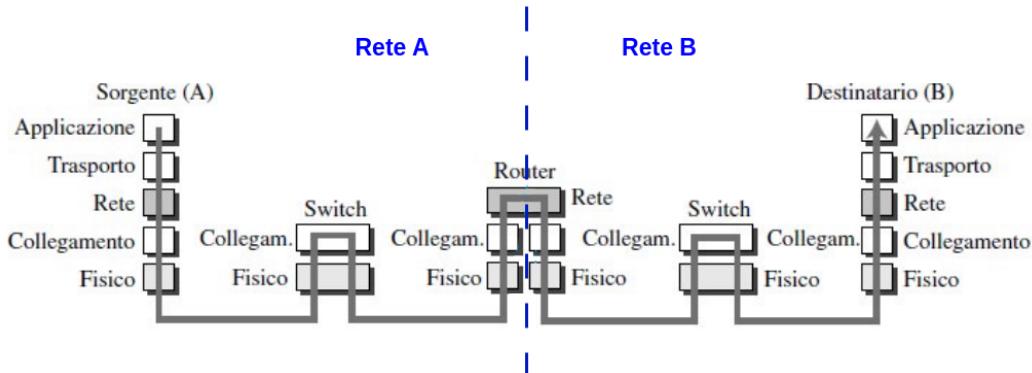


I livelli di Applicazione e di Trasporto sono gestiti tramite **software**, mentre i livelli di Collegamento e Fisico tramite **hardware**.

Durante l'invio di un pacchetto, quest'ultimo, partendo dal livello applicazione del dispositivo sorgente, **percorre tutti i layer dello stack protocollare**, fino a giungere al livello fisico, dove viene effettivamente inviato al nodo successivo.

Tutti i nodi intermedi presenti sul percorso lavoreranno utilizzando solo i livelli necessari. In particolare, ogni dispositivo utilizzerà il livello di collegamento, in modo da poter spedire il pacchetto stesso verso il nodo successivo del percorso.

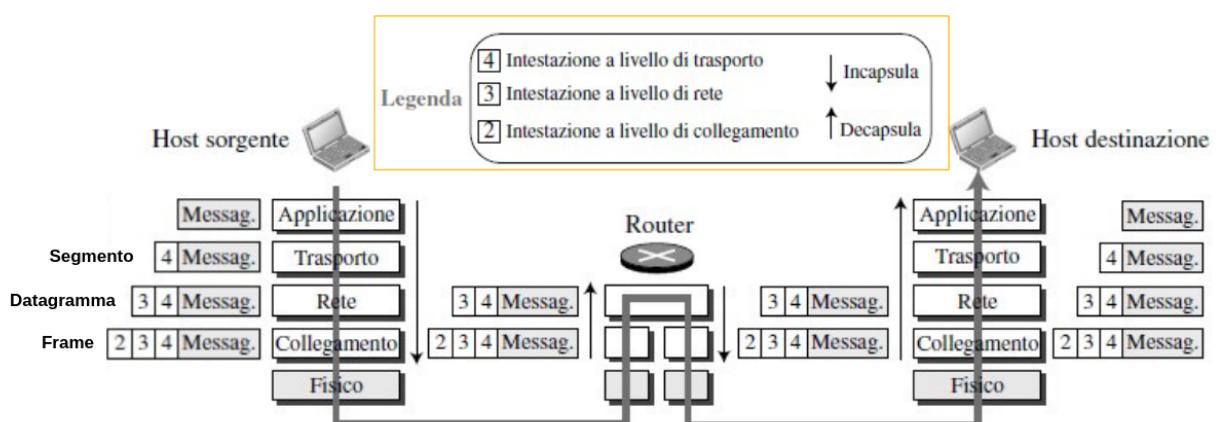
Nel caso in cui si raggiunga il **punto di scambio tra due reti**, solitamente un edge router, verrà utilizzato anche il livello di rete.



Prima di essere spedito al livello inferiore, ogni pacchetto viene **incapsulato**: una volta ricevuto il pacchetto dal layer superiore, il layer attuale applica un proprio **header (o intestazione)**, aggiungendo informazioni necessarie al layer del dispositivo di destinazione corrispondente a quello attuale.

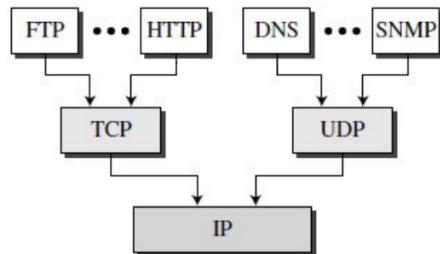
In particolare, ad ogni livello un pacchetto assume il nome di:

- **Messaggio (al livello di applicazione)**, corrispondente al pacchetto originale, senza alcuna intestazione
- **Segmento (al livello di trasporto)**, corrispondente al messaggio ricevuto dal layer superiore a cui viene aggiunto un header di trasporto
- **Datagramma (al livello di rete)**, corrispondente al segmento ricevuto dal layer superiore a cui viene aggiunto un header di rete
- **Frame (al livello di collegamento)**, corrispondente al datagramma ricevuto dal layer superiore a cui viene aggiunto un header di collegamento

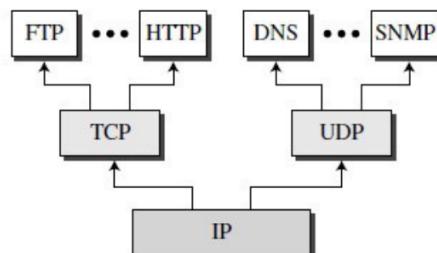


Poiché lo stack protocollare TCP/IP prevede la presenza di **più protocolli nello stesso livello**, ogni livello deve essere in grado di effettuare operazioni di:

- **Multiplexing**, dove ogni protocollo deve essere in grado di encapsulare (uno alla volta) i pacchetti ricevuti da più protocolli presenti al livello superiore



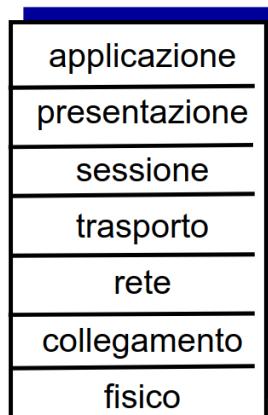
- **Demultiplexing**, dove ogni protocollo deve essere in grado di decapsulare i pacchetti ricevuti ed inviarli a più protocolli presenti nel livello superiore



Per realizzare ciò, nell'header di ogni layer viene inserito un **campo speciale** in grado di identificare quale sia il protocollo di appartenenza di tale pacchetto.

Un'evoluzione dello stack protocollare TCP/IP è il **modello Open Systems Interconnection (OSI)**, dove vengono interposti due livelli tra il livello di applicazione e il livello di trasporto:

- **Livello di Presentazione**, utilizzato per consentire alle applicazioni di interpretare i dati (es: crittografia, compressione, ...)
- **Livello di Sicurezza**, utilizzato per gestire servizi come la sincronizzazione o il ripristino dello scambio di dati



# Capitolo 2

## Livello di Applicazione

### 2.1 Principi delle applicazioni di rete

#### Definition 14. Paradigma di comunicazione

Un **paradigma di comunicazione** è una metodologia di scambio informazioni e gestione delle connessioni all'interno di una rete, principalmente all'interno di Internet.

In particolare, i due principali paradigmi utilizzati sono:

- **Paradigma Client-Server**, dove i sistemi terminali vengono divisi in due categorie:
  - **Client**, il quale comunica solo ed esclusivamente con un server, **richiedendo dei servizi** a quest'ultimo, e può rimanere anche inattivo se non necessario, implicando che esso possa avere indirizzi IP dinamici nel tempo. In particolare, per tali caratteristiche, non vi è una comunicazione client-client, ma solo una comunicazione client-server-client
  - **Server**, il quale possiede un indirizzo IP permanente, rimanendo sempre attivo in attesa di **fornire servizi** ai vari client richiedenti

Ad esempio, i protocolli HTTP, FTP e IMAP sono basati su tale paradigma

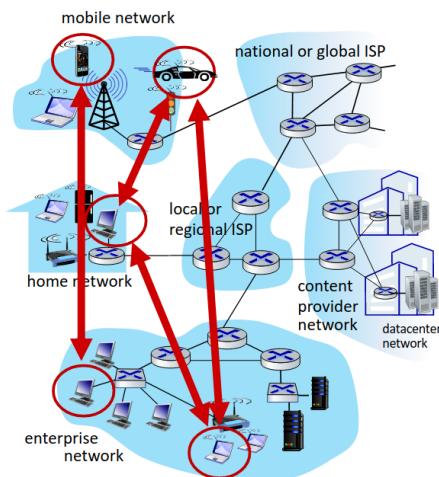


- **Paradigma Peer-to-Peer (P2P)**, dove i sistemi terminali vengono detti **peer** (tradotto: *pari, di equal importanza*) ed ognuno di essi è in grado di comunicare direttamente con ogni altro peer (assumendo quindi sia il compito di client che di server).

In particolare, ogni peer **richiede e fornisce servizi ad altri peer**, rendendo il sistema **estremamente scalabile**: ogni nuovo peer incrementa le capacità di servizio e le richieste di servizio.

Inoltre, come nel caso dei client, ogni peer può connettersi alla rete in modo intermittente utilizzando IP dinamici, diminuendo temporaneamente la quantità di servizi fornibili nella rete. Di conseguenza, la loro gestione risulta estremamente più complessa, ma anche più performante nel caso di un numero elevato di peer.

Un classico esempio di utilizzo del paradigma P2P risultano essere i vari protocolli legati al torrenting e alla condivisione di file di grandi dimensioni.



### Definition 15. Processo

Un **processo** è un programma in esecuzione all'interno di un sistema terminale.

In particolare, un **processo client** è un processo che avvia una comunicazione, mentre un **processo server** è un processo che attende di essere contattato da un processo client.

All'interno dello stesso sistema, due processi comunicano tra di loro utilizzando una comunicazione **inter-process**, definita dal sistema operativo. I processi situati su sistemi diversi, invece, comunicano tra di loro tramite **scambio di messaggi**

### Definition 16. Socket

Un **socket** è un'**astrazione software** tramite cui un processo può inviare e ricevere messaggi tramite il socket di un altro processo. Per poter comunicare, dunque, due processi devono connettersi tramite due socket (uno ciascuno), identificati da una coppia <Indirizzo\_IP, Numero\_Porta>

Ogni protocollo a livello di applicazione definisce:

- Le tipologie di messaggi scambiati (es: richiesta e risposta)
- La sintassi del messaggio
- La semantica del messaggio
- Le regole per come e quando i processi inviano e rispondono ai messaggi

In particolare, i protocolli a tale livello si differenziano in **protocolli aperti**, ossia definiti secondo uno standard pubblico ed adottato comunemente da ogni applicazione (es: HTTP, FTP, ...), e **protocolli proprietari**, ossia non pubblici e fini all'applicazione stessa (es: Skype, ...).

Per poter funzionare correttamente, ogni applicazione di rete necessita di alcuni **servizi di trasporto**. In particolare, esse possono necessitare di:

- **Integrità dei dati**, ossia un trasferimento dei dati affidabile al 100%, senza alcuna perdita di pacchetto o corruzione dei dati
- **Garanzie temporali**, ossia un basso ritardo per la ricezione dei dati
- **Garanzie di throughput**, ossia una quantità minima di throughput dati
- **Sicurezza**, ad esempio crittografia o integrità dei dati a seguito di manomissioni

### Definition 17. Transmission Control Protocol (TCP)

Il **Transmission Control Protocol (TCP)** è un protocollo risiedente sul **layer di trasporto** in grado di fornire **trasporto affidabile**, ossia senza perdita di alcun pacchetto, e controllo del flusso e della congestione, in cambio di un'assenza di garanzie temporali, di throughput e di sicurezza.

Inoltre, il protocollo TCP è **orientato alla connessione**, ossia richiedente una configurazione (**handshaking**) tra il processo client e il processo server

### Definition 18. User Datagram Protocol (UDP)

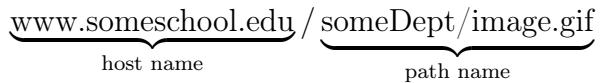
L'**User Datagram Protocol (UDP)** è un protocollo risiedente sul **layer di trasporto** in grado di fornire **trasporto veloce** poiché **non orientato alla connessione** ed **estremamente scarno**, ossia sprovvisto di: trasporto affidabile, controllo del flusso e della congestione e garanzie temporali, di throughput e di sicurezza

Poiché per loro natura i protocolli TCP ed UDP sono privi di garanzie di sicurezza, i messaggi scambiati tra socket TCP e UDP risultano sprovvisti di crittografia, attraversando il percorso instradato completamente in chiaro ed essendo quindi leggibili e manipolabili da qualsiasi dispositivo intermedio.

Per ovviare tale problema, viene implementato a livello di applicazione il protocollo **Transport Layer Security (TLS)** tramite socket realizzati con librerie software specifiche, fornendo connessioni crittografate, integrità dei dati ed autenticazione dell'end-point.

## 2.2 Web e Protocollo HTTP

Una pagina web è composta da **oggetti**, ognuno dei quali può essere archiviato su un diverso web server. In particolare, una pagina web consiste in un **file HTML** il quale include diversi oggetti referenziati tramite vari URL



### Definition 19. Protocollo HTTP

Il **protocollo HTTP (Hypertext Transfer Protocol)** è un protocollo a livello di applicazione utilizzato per la realizzazione di servizi web. La sua porta di riferimento comune all'interno dei socket è la **porta 80**.

Il protocollo HTTP è **stateless**, ossia non conservante alcuna informazione sulle richieste passate, e basato sul **paradigma client-server**, dove il client invia messaggi detti **richieste** e il server invia messaggi detti **risposte**.

Inoltre, il protocollo HTTP fa uso del **protocollo TCP**:

1. Il client avvia una connessione TCP con il server utilizzando la porta 80, rimanendo in attesa che il server accetti la connessione (TCP handshaking)
2. Vengono scambiati messaggi HTTP tra client e server
3. La connessione TCP viene chiusa

Le **connessioni HTTP** si differenziano in due tipologie:

- **Connessione non persistente**, dove viene aperta la connessione TCP e viene inviato massimo un oggetto prima di chiudere la connessione TCP
- **Connessione persistente (HTTP/1.1)**, dove viene aperta la connessione TCP e vengono inviati multipli oggetti in successione prima di chiudere la connessione TCP

**Esempio:**

1. Supponiamo che un utente inserisca l'URL dell'oggetto "www.someSchool.edu/ someDepartment/home.index", contenente del testo e 10 riferimenti ad immagini.
2. Il client HTTP dell'utente (browser, cURL, ...) avvia la connessione TCP con il server HTTP tramite la porta 80
3. Il server HTTP sull'host "www.someSchool.edu" riceve la richiesta di connessione, accettandola e notificando il client
4. Il client HTTP invia un messaggio di richiesta HTTP, contenente il path dell'oggetto desiderato, ossia "/someDept/index.html"
5. Il server HTTP riceve il messaggio di richiesta e invia il messaggio di risposta contenente l'oggetto desiderato, il quale a sua volta contiene i riferimenti alle 10 immagini.

6. A questo punto, si creano due scenari:

- Se la connessione non è persistente, il server chiude immediatamente la connessione TCP, implicando che l'intero processo debba essere ripetuto per tutti e 10 i riferimenti necessari
- Se la connessione è persistente, il client invierà in successione altre 10 richieste al server, richiedendo quindi solo la ripetizione dei passaggi 4 e 5 (per 10 volte), per poi chiudere la connessione TCP

### Definition 20. Round Trip Time (RTT)

Definiamo come **Round Trip Time (RTT)** il tempo impiegato da un pacchetto di piccole dimensioni per compiere il percorso client-server-client

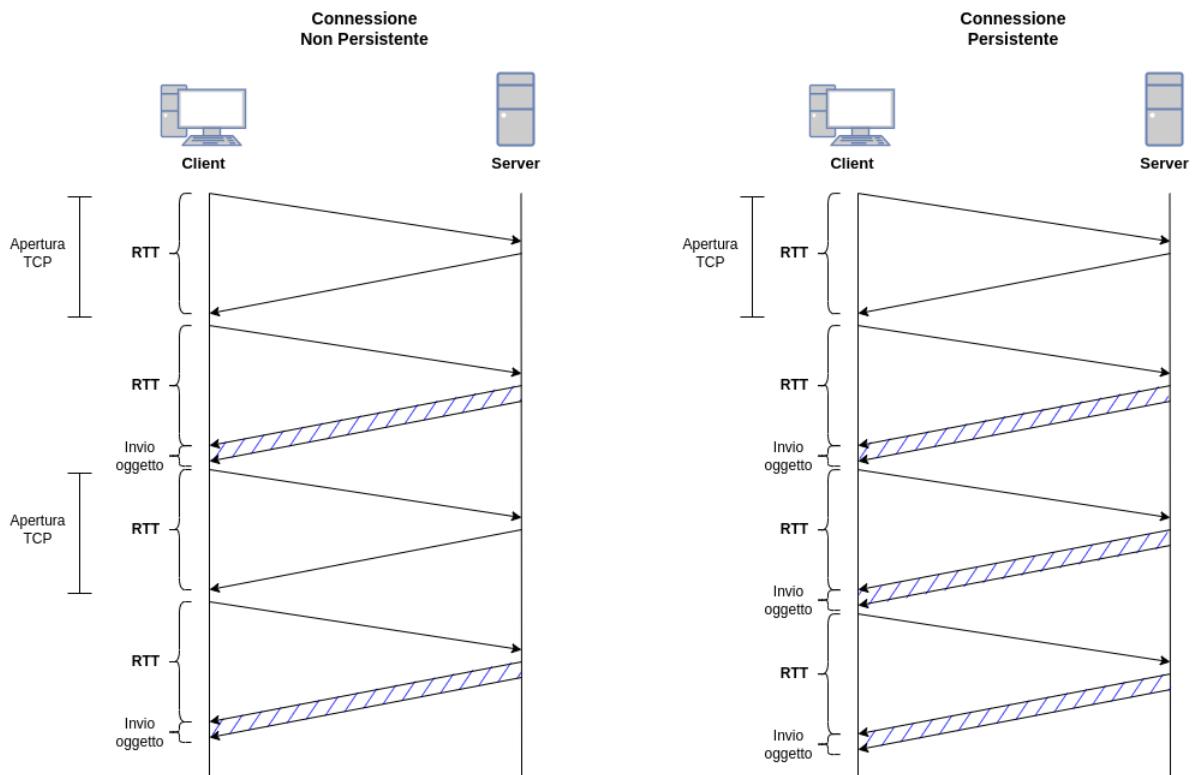
### Observation 2. Tempo di risposta HTTP

Se la **connessione non è persistente**, per ogni oggetto sono necessari due RTT, uno per avviare la connessione TCP ed uno per l'invio di richiesta e risposta, seguiti dal tempo necessario ad inviare l'oggetto

$$T_{tot} = (2 \text{ RTT} + \text{Tempo invio ogg.}) \cdot \text{Num. Oggetti}$$

Se la **connessione è persistente**, invece, saranno necessari un RTT per poter stabilire la connessione TCP, seguiti da un solo RTT per oggetto (con annesso tempo di invio)

$$T_{tot} = 1 \text{ RTT} + (1 \text{ RTT} + \text{Tempo invio ogg.}) \cdot \text{Num. Oggetti}$$



### 2.2.1 Messaggi di richiesta e risposta

I messaggi HTTP di **richiesta** e **risposta** vengono formattati un formato leggibile dall'uomo (in particolare, in codice ASCII).

Ogni messaggio di **richiesta HTTP** viene strutturato nel seguente modo:

- Una **riga di richiesta**, composta dal **metodo** utilizzato, il path richiesto e la versione di HTTP utilizzata, seguiti da un carattere di ritorno a capo, ossia \r, ed un carattere di avanzamento di riga, ossia \n

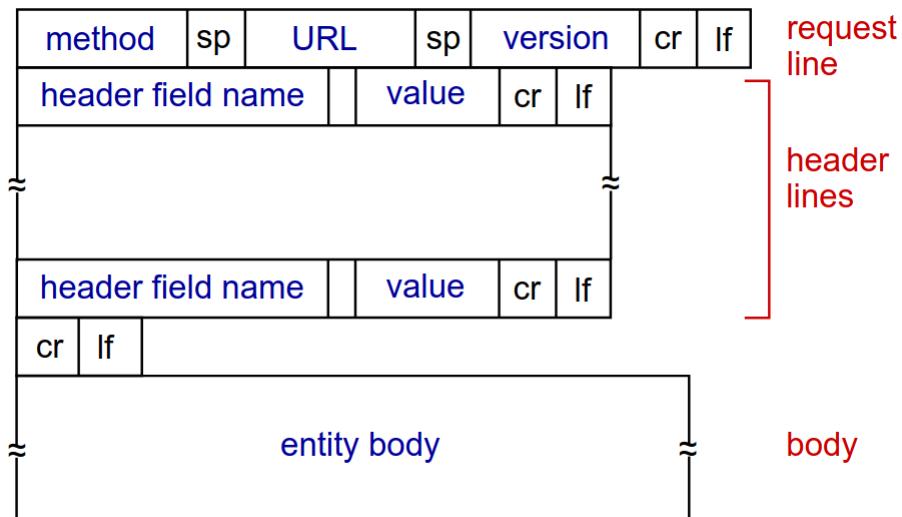
I **metodi** principali inseribili all'interno della riga di richiesta sono:

- **Metodo GET**, utilizzato per l'invio di dati al server, i quali vengono inseriti all'interno dell'URL a seguito di un carattere '?'  
(es: `www.mysite.com/search?user=myuser`)
- **Metodo POST**, utilizzato per l'invio di dati al server, i quali vengono aggiunti all'interno del body del messaggio (rimanendo quindi parzialmente offuscati all'utente)
- **Metodo HEAD**, utilizzato per richiedere solo l'header di risposta che verrebbe restituito dalla destinazione a seguito di una richiesta GET
- **Metodo PUT**, utilizzato per caricare un nuovo file o sostituirne uno esistente all'interno della destinazione (non più utilizzato poiché estremamente insicuro)
- Un **header (o intestazione)**, composto da varie linee contenenti informazioni utili alla connessione

Alcuni esempi di campi inseribili all'interno di un header di richiesta sono:

Campo Header	Descrizione
User-agent	Indica il programma client utilizzato
Accept	Indica il formato dei contenuti che il client è in grado di accettare
Accept-charset	Famiglia di caratteri che il client è in grado di gestire
Accept-encoding	Schema di codifica supportato dal client
Accept-language	Linguaggio preferito dal client
Authorization	Indica le credenziali possedute dal client
Host	Host e numero di porta del client
Date	Data e ora del messaggio
Upgrade	Specifica il protocollo di comunicazione preferito
Cookie	Comunica un cookie al server
If-Modified-Since	Invia il documento solo se è più recente della data specificata

- Un **body (o contenuto)**, ossia il vero contenuto del messaggio da inviare (solitamente vuoto a meno dell'uso del metodo POST)



Esempio:

```
GET /index.html HTTP/1.1\r\n
Host: www-net.cs.umass.edu\r\n
User-Agent: Firefox/3.6.10\r\n
Accept: text/html,application/xhtml+xml\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7\r\n
Keep-Alive: 115\r\n
Connection: keep-alive\r\n
\r\n
```

Analogamente, ogni messaggio di **risposta HTTP** viene strutturato in modo simile, ma con alcune differenze:

- Una **riga di stato**, composta dalla versione di HTTP utilizzata, un **codice di status** e una **frase di status** descrivente in breve il codice di status

I **codici di status** si dividono in 5 categorie:

- **Codici 1xx**, indicanti che la risposta ricevuta contiene solamente informazioni  
(es: 100 Continue indica che il server è pronto a ricevere la richiesta del client)
- **Codici 2xx**, indicanti che la richiesta effettuata è andata a buon fine  
(es: 200 OK indica che la richiesta ha avuto successo e l'oggetto richiesto è stato trovato, 204 No Content indica che la richiesta ha avuto successo ma l'oggetto richiesto non contiene nulla al suo interno)
- **Codici 3xx**, indicanti che è stato effettuato un reindirizzamento a seguito della richiesta effettuata  
(es: 301 Moved Permanently indica che l'oggetto richiesto possiede un path diverso da quello richiesto, reindirizzando automaticamente tutte le richieste successive del client)

- **Codici 4xx**, indicanti un errore nella richiesta del client  
(es: **403 Forbidden** indica che il client non possiede i requisiti per accedere all'oggetto richiesto, **404 Not Found** indica che l'oggetto richiesto non esiste )
- **Codici 5xx**, indicanti un errore per cui il server non è riuscito a completare la richiesta  
(es: **500 Internal Server Error** indica un errore sconosciuto all'interno del server, **503 Service Unavailable** indica che il server è attualmente non disponibile)
- Un **header (o intestazione)**, composto da varie linee contenenti informazioni utili alla risposta

Alcuni esempi di campi inseribili all'interno di un header di risposta sono:

Campo Header	Descrizione
Date	Data e ora attuale
Upgrade	Specifica il protocollo di comunicazione preferito
Server	Indica il programma server utilizzato
Set-Cookie	Il server richiede al client di memorizzare un cookie
Content-Encoding	Specifica lo schema di codifica
Content-Language	Specifica la lingua utilizzata nel documento
Content-Length	Indica la lunghezza del documento
Content-Type	Specifica la tipologia del documento
Location	Chiede al client di inviare la richiesta ad un altro sito
Last-modified	Fornisce data e ora dell'ultima modifica del documento

- Un **body (o contenuto)**, ossia il vero contenuto del messaggio da restituire (in particolare, l'oggetto richiesto)

Esempio:

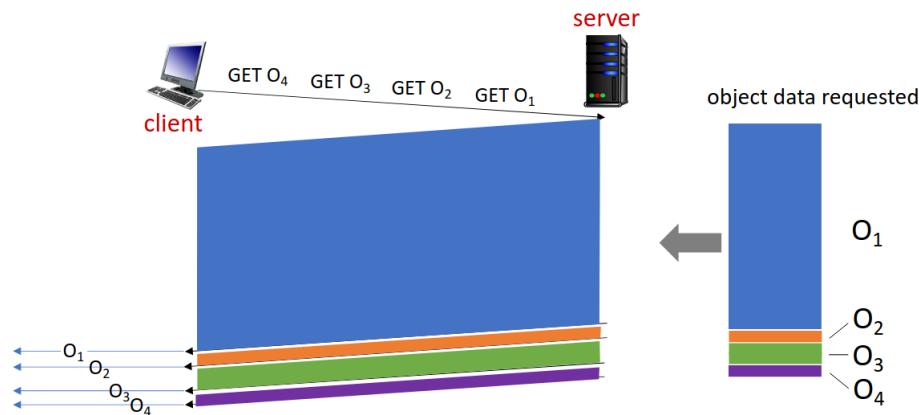
```

HTTP/1.1 200 OK\r\n
Date: Sun, 26 Sep 2010 20:09:20 GMT\r\n
Server: Apache/2.0.52 (CentOS)\r\n
Last-Modified: Tue, 30 Oct 2007 17:00:02 GMT\r\n
Accept-Ranges: bytes\r\n
Content-Length: 2652\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=ISO-8859-1\r\n
\r\n
[document content...]
[...]
[document content...]
```

### 2.2.2 Versioni di HTTP

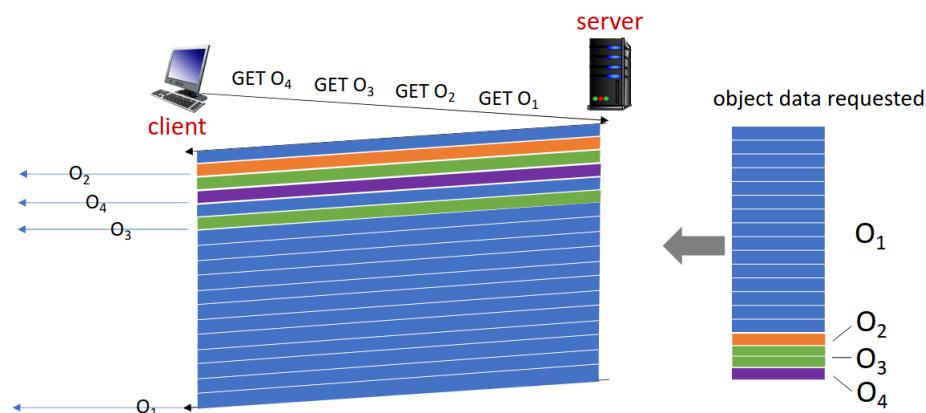
Come già discusso, il **protocollo HTTP/1.1** ha introdotto la possibilità di poter effettuare più richieste GET in successione tramite una singola connessione TCP. Tuttavia, tale modifica ha introdotto ulteriori problematiche:

- Il server risponde alle richieste GET nell'ordine in cui vengono effettuate (**First Come First Served (FCFS)**)
- Un oggetto di piccole dimensioni potrebbe dover attendere la trasmissione di oggetti di grandi dimensioni richiesti prima di esso (**blocco head-of-line (HOL)**)
- La perdita di un segmento TCP causa lo stallo del trasferimento di un oggetto



Per risolvere tali problematiche, il **protocollo HTTP/2** introduce una maggiore flessibilità al server nell'invio di oggetti al client:

- L'ordine di trasmissione degli oggetti richiesti viene stabilito in base alla priorità dell'oggetto specificata dal client
- Gli oggetti vengono **divisi in frame**, schedulati in modo da mitigare il blocco HOL
- Possono essere inviati più oggetti contemporaneamente (**multiplexing**)



Il **protocollo HTTP/3**, invece, risolve le ultime problematiche rimanenti all'interno del protocollo HTTP/2, tramite l'aggiunta di controlli sulla sicurezza, sugli errori e sulla congestione per oggetto, utilizzando il **protocollo QUIC** (basato su UDP) al posto del protocollo TCP.

### 2.2.3 Cookies e Web Caching

#### Definition 21. Cookie

Un **cookie** è un **piccolo file di testo** contenente brevi informazioni (preferenze sull'utilizzo, parametri preferiti, token di autorizzazione, ...) salvato all'interno di un client da parte di un server web

Poiché il protocollo HTTP è un protocollo **stateless**, i cookie vengono utilizzati all'interno delle applicazioni web per conservare indirettamente alcune informazioni sulle varie comunicazioni client-server effettuate, rendendo ogni richiesta HTTP indipendente dall'altra.

A seguito di un messaggio di risposta da un web server contenente il campo header **Set-Cookie**, il client salva il contenuto del cookie all'interno di un file. Durante le **succesive richieste** effettuate dallo stesso client allo stesso server, tutti i cookie impostati da tale server vengono **allegati ad ogni richiesta HTTP**.

Soltanente, il cookie fornito dal server contiene un ID univoco, in modo da legare una voce nel suo database interno a quel client specifico.



La **durata di un cookie** inviato viene specificata tramite un campo header **Max-Age**, tramite il quale viene specificato il tempo di vita di tale cookie in **secondi**. Allo scadere di tali secondi, il client eliminerà automaticamente tale cookie. Inoltre, non c'è limite alla quantità di secondi specificabili, implicando che sia possibile specificare anche una quantità di secondi pari a mesi o anni

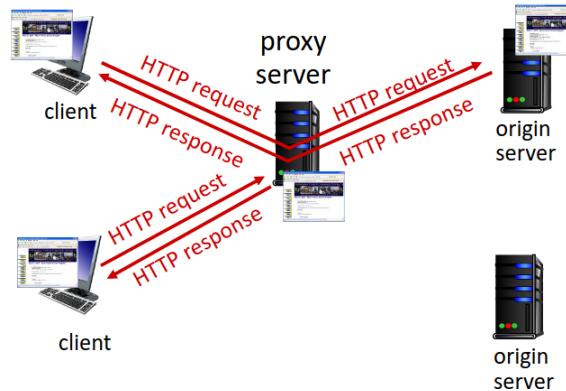
### Definition 22. Proxy Server

Un **proxy server** è un server utilizzato come **intermediario** tra un client e il vero server destinatario.

Solitamente, tale tipologia server viene utilizzato per il **web caching**:

- Se il documento richiesto **è presente** nella cache del proxy server, esso viene restituito al client senza dover raggiungere il server originale
- Se il documento richiesto **non è presente** nella cache, il proxy server inoltra la richiesta del client al server di origine, memorizzando nella sua cache il documento ricevuto nella risposta, restituendolo al client

Tramite il web caching è possibile ridurre notevolmente i tempi di risposta e il traffico nei link di accesso alla rete del server di origine, consentendo ai fornitori di contenuti di essere più efficienti.



## 2.3 Posta elettronica

Il servizio di **posta elettronica** è costituito da tre entità fondamentali:

- Uno **User agent (UA)**, detto anche *mail reader*, è un processo attivo sul client utente attivato dall'utente stesso o da un timer. Si occupa di informare l'utente nel caso in cui sia disponibile una nuova email da leggere nella sua casella di posta.
- Inoltre, lo user agent permette la composizione, l'editing, l'invio e la lettura di messaggi di posta elettronica. Ogni messaggio di posta inviato da un UA viene passato ad un MTA
- **Mail Transfer Agent (MTA)**, è un processo attivo su un mail server utilizzato per il trasferimento Internet di un messaggio ricevuto da un UA o da un altro MTA
- **Mail Access Agent (MAA)**, è un processo attivo su un mail server utilizzato per leggere i messaggi di posta in arrivo

Ogni **mail server** è dotato di una **casella di posta (mailbox)**, contenente i messaggi in arrivo per l'utente, ed una **coda di messaggi**, contenente i messaggi dell'utente ancora da inviare.



### 2.3.1 Protocolli SMTP e MIME

#### Definition 23. Protocollo SMTP

Il **protocollo SMTP** (Simple Mail Transfer Protocol) è un protocollo a livello di applicazione utilizzato per l'invio di messaggi di posta elettronica in formato ASCII. La sua porta di riferimento comune all'interno dei socket è la **porta 25**.

Il protocollo SMTP effettua un **trasferimento diretto**, ossia dal mail server mittente a quello destinatario (dunque senza mail server intermedi), basato su un'**interazione comando/risposta**: viene inviato un comando in testo ASCII e viene ricevuta una risposta equivalente ad un codice di stato.

Inoltre, il protocollo SMTP fa uso del **protocollo TCP**:

- Il client avvia una connessione TCP con il server utilizzando la porta 25, rimanendo in attesa che il server accetti la connessione (TCP handshaking)
- Vengono scambiati messaggi di posta tra client e server (**connessione persistente**)
- La connessione TCP viene chiusa

#### Esempio:

- Alice usa il suo UA per comporre il messaggio da inviare all'indirizzo di posta elettronica `bob@someschool.edu`
- L'UA di Alice invia il messaggio al mail server di Alice, il quale porrà tale messaggio nella sua coda di messaggi. Successivamente, il client SMTP presente sul mail server di Alice apre una connessione TCP con il mail server di Bob
- Il client SMTP invia il messaggio di Alice sulla connessione TCP tramite il suo MTA

4. Il mail server di Bob riceve il messaggio e lo pone nella casella di posta di Bob
5. Bob invoca il suo UA per leggere il messaggio, il quale preleverà il messaggio tramite l'MAA presente sul suo mail server

(NB: tale operazione *non* è svolta dal protocollo SMTP, bensì dal protocollo POP3 o dal protocollo IMAP che vedremo in seguito)



In particolare, lo scambio di messaggi viene gestito dal protocollo SMTP nel seguente modo:

1. Il client SMTP **tenta di stabilire** una connessione TCP sulla porta 25 con il server STMP. Se il server è attivo, la connessione TCP viene stabilita. Altrimenti, il client riproverà dopo un determinato lasso di tempo.
2. Una volta stabilita la connessione, il client e il server effettuano una **forma aggiuntiva di handshaking**, dove il client indica al server l'indirizzo email del mittente e del destinatario
3. Il client invia il messaggio sulla connessione TCP. Una volta ricevuto il messaggio, se ci sono altri messaggi da inviare viene utilizzata la stessa connessione TCP (**connessione persistente**). Altrimenti, il client invia al server una richiesta di chiusura della connessione.

#### Esempio:

- Di seguito, vediamo un esempio di interazione tra un server SMTP, indicato con S, e un client SMTP, indicato con C.

```

S: 220 hamburger.edu
C: HELO crepes.fr
S: 250 Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection

```

Lo **standard RFC 822** definisce la struttura che ogni messaggio di posta elettronica deve assumere:

- Un **header** composto dai seguenti campi:

Campo Header	Descrizione
To	L'indirizzo del destinatario
From	L'indirizzo del mittente
CC	Indirizzi aggiuntivi di mittenti a cui far sapere dell'invio e il contenuto di tale email (abbreviativo di Carbon Copy)
BCC	Analogo al CC, ma non vengono mostrati al destinatario (abbreviativo di Blind CC)
Subject	L'argomento del messaggio
Sender	Il nome del mittente

- Un **body**, contenente il messaggio da inviare (**solo caratteri ASCII**)

Per poter inviare contenuti diversi dal semplice test ASCII, gli standard RFC 2045 e 2046 definiscono il **protocollo MIME (Multipurpose Internet Mail Extension)**, in grado di estendere i normali messaggi di posta elettronica in messaggi multimediali.

Vengono aggiunte alcune righe all'interno dell'header del messaggio inviato, in particolare una riga **Version**, indicante la **versione del protocollo** MIME utilizzata, e una riga **Type**, indicante il **tipo di dati multimediali** inviati, i quali, prima di essere spediti, vengono convertiti in una **codifica testuale** (solitamente base64), specificata da un campo aggiuntivo **Content-Transfer-Encoding**, in modo da poter essere trasmesso sottoforma di testo ASCII, per poi venir decodificati una volta che il messaggio è giunto al destinatario.

### 2.3.2 Protocolli POP3 e IMAP

#### Definition 24. Protocollo POP3

Il **protocollo POP3 (Post Office Protocol vers. 3)** è un protocollo **stateless** a livello di applicazione utilizzato per il download di messaggi di posta elettronica ricevuti. La sua porta di riferimento comune all'interno dei socket è la **porta 110**.

Per stabilire una connessione, il protocollo POP3 fa uso del **protocollo TCP**, effettuando quindi l'handshake TCP, per poi procedere nelle seguenti tre fasi:

1. **Autorizzazione**, dove lo UA invia nome utente e password per essere identificato dal mail server
2. **Transazione**, dove lo UA recupera i messaggi nella casella di posta dell'utente
3. **Aggiornamento**, dove, successivamente all'invio di un messaggio QUIT da parte dello UA, viene terminata la connessione e vengono rimossi dal mail server i messaggi contrassegnati durante la fase precedente

**Esempio:**

- Se la richiesta effettuata viene eseguita correttamente, il server risponderà con +OK, altrimenti con -ERR. Il comando retr permette di scaricare il messaggio, mentre il comando dele permette di marcare i messaggi da eliminare

```

S: +OK POP3 server ready
C: user rob
S: +OK
C: pass hungry
S: +OK user successfully logged on
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off

```

- Successivamente, viene attivata la fase di aggiornamento, cancellando dal mail server i messaggi marcati tramite dele

Oltre ad essere un protocollo stateless, il protocollo POP3 non fornisce all'utente la possibilità di creare **cartelle remote** tra cui poter suddividere i messaggi, costringendo la creazione di tali cartelle solo a livello locale, implicando che esse non siano condivise tra i vari dispositivi dell'utente.

### Definition 25. Protocollo IMAP

Il **protocollo IMAP (Internet Message Access Protocol)** è un protocollo a livello di applicazione utilizzato per l'accesso ai messaggi di posta elettronica ricevuti. La sua porta di riferimento comune all'interno dei socket è la **porta 143**.

A differenza del protocollo POP3, tutti i messaggi vengono **conservati nel mail server**, permettendo all'utente di avere solo copie locali. Per via di ciò, il protocollo IMAP permette di:

- Associare ogni messaggio ricevuto ad una cartella, detta **inbox**
- Creare cartelle remote e spostare messaggi tra di esse
- Effettuare ricerche nelle cartelle remote
- Conservare lo stato tra le varie sessioni dell'utente (protocollo **stateful**)

## 2.4 Domain Name System (DNS)

### Definition 26. Domain Name System (DNS)

Il **Domain Name System (DNS)** è un sistema utilizzato per mappare singoli nodi di una rete ad un **nome** che li identifichi. Viene realizzato tramite un database distribuito, implementato come una gerarchia di **name server**.

Tra le funzioni fornite dal servizio DNS troviamo:

- **Traduzione** da nome host all'indirizzo IP relativo
- **Distribuzione del carico**, permettendo a più indirizzi IP, ognuno legato ad un server copia di quello originale, di corrispondere ad un unico nome. Quando un client effettua una richiesta, il servizio restituisce l'insieme di indirizzi legati a tale nome in un ordine casuale (rotazione DNS)
- **Host Aliasing**, ossia l'associazione di più sinonimi (alias) allo stesso indirizzo IP, permettendo l'associazione di un nome più semplice rispetto ad uno complesso  
(es: al nome `relay1.west-coast.enterprise.com` associamo l'alias `enterprise.com` e l'alias `www.enterprise.com`)

Per via delle sue funzioni, il servizio DNS risulta essere **fondamentale** per Internet.

In particolare, la **decentralizzazione** del servizio DNS risulta essere critica: se il servizio fosse centralizzato (ossia effettuato da un singolo nodo o rete) sarebbe sufficiente un singolo punto di fallimento affinché il servizio diventi inutilizzabili. Inoltre, se il servizio fosse centralizzato si avrebbe un volume di traffico troppo elevato dovuto alle miliardi di richieste effettuate giornalmente (es: il server DNS Comcast riceve 600 miliardi di richieste al giorno)

### 2.4.1 Gerarchia server DNS

Poiché il mapping DNS è **distribuito** su svariati server, dove in particolare nessuno di essi mantiene il mapping di tutti gli IP possibili (un IP corrisponde a 32 bit, dunque  $2^{32}$  IP possibili), il database tramite cui viene realizzato il servizio DNS è **gerarchico**, seguendo la struttura di un albero:

- **Root Server**:
  - Radice dell'albero
  - Viene interrogato da qualsiasi server DNS che non sia in grado di risolvere il nome di un server TLD (ossia restituire l'IP legato ad esso)
- **Server Top-Level Domain (TLD)**:
  - Viene interrogato per risolvere il nome di un server DNS autoritativo
  - Responsabili di domini come `.com`, `.org`, `.net`, ... e tutti i domini nazionali di primo livello, ossia `.it`, `.uk`, `.fr`, ...

- **Server autoritativi (o di competenza):**

- Viene interrogato per risolvere il nome di un host pubblicamente accessibile, solitamente all'interno di un'organizzazione
- Ogni organizzazione con host pubblicamente accessibili deve fornire i record DNS di pubblico dominio che mappano i nomi di tali host ai loro indirizzi IP

- **Server DNS locali (o default name server):**

- Non appartengono alla gerarchia. Ogni ISP ne è dotato
- Possiedono una cache locale delle recenti coppie di mappatura nome-indirizzo (potrebbero non essere aggiornate)
- Funge da proxy iniziale tra il client e il root server: se il nome non è nella cache del server locale, la richiesta viene inoltrata al root server



### Esempio:

1. Il client vuole ottenere l'indirizzo IP dell'host `www.amazon.com`
2. Viene contattato il server DNS locale dell'ISP di riferimento. Se il nome non viene risolto, si procede col passo successivo.
3. Viene contattato il root server per trovare l'indirizzo IP del server TLD `.com`
4. Viene contattato il server TLD `.com` per trovare l'indirizzo IP del server autoritativo `amazon.com`
5. Viene contattato il server autoritativo `amazon.com` per trovare l'indirizzo IP dell'host `www.amazon.com`

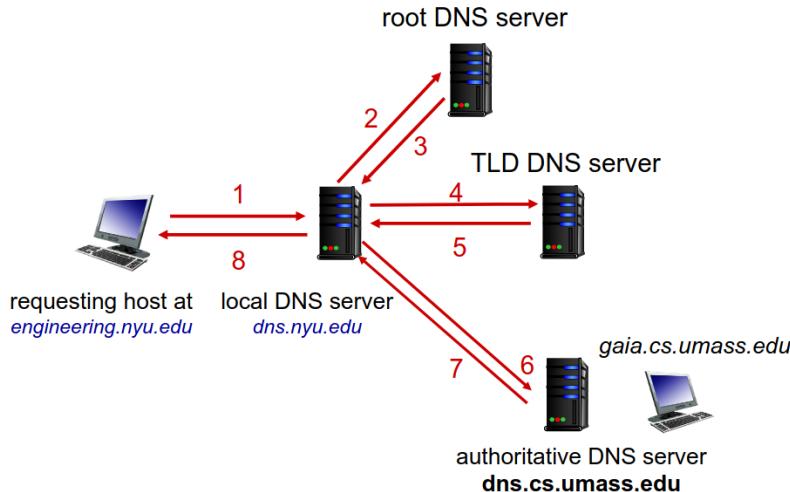
Ogni volta che un server DNS viene a conoscenza di una mappatura, essa viene **memorizzata** all'interno della cache, utilizzando tali record per rispondere a query future. I record presenti nella cache vengono cancellati allo scadere di un **TTL (Time-to-live)** o a seguito di un comando manuale.

Soltanente, all'interno della cache dei server DNS locali sono presenti i server TLD più comuni, implicando che il root server venga interrogato raramente.

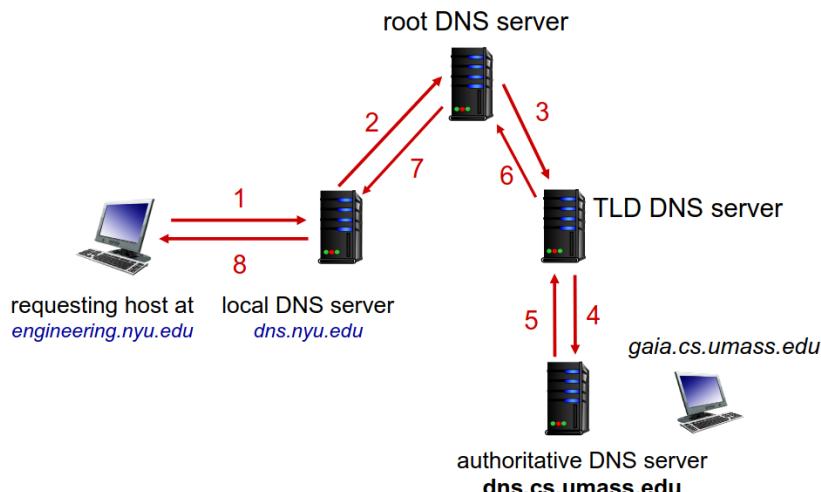
Tuttavia, è necessario notare che i record nella cache **potrebbero non essere aggiornati**: se viene cambiato l'indirizzo IP associato ad un nome presente nella cache, esso potrebbe non essere noto all'interno di Internet fino alla scadenza di tutti i TTL di tutti i server, poiché quest'ultimi risolverebbero la richiesta restituendo l'indirizzo IP precedente.

La **risoluzione dei nomi**, ossia la restituzione dell'indirizzo IP ad esso legato, può avvenire in due modalità:

- **Risoluzione a query iterativa**, dove il server contattato dal client risponde con il nome del prossimo server da contattare, il quale (probabilmente) sarà in grado di risolvere il nome



- **Risoluzione a query ricorsiva**, dove l'onere della risoluzione del nome viene affidato al server contattato, ricorsivamente



Ogni mappatura nome-indirizzo viene inserita all'interno di un **resource record (RR)**, il quale assume la struttura (`name, value, type, ttl`), dove a seconda del valore del campo **type** si ha che:

- **type = A**, indica che il campo `name` contiene il nome di un host interno ad un dominio (hostname) e il campo `value` contiene l'indirizzo IP di tale host  
(es: `name = relay1.bar.foo.com, value = 45.37.93.126`)
- **type = NS**, indica che il campo `name` contiene il nome di un dominio e il campo `value` contiene l'hostname del server autoritativo associato a tale dominio  
(es: `name = foo.com, value = dns.foo.com`)

- **type = CNAME**, indica che il campo **name** contiene un alias del nome canonico e il campo **value** contiene il nome canonico stesso

(es: name = www.ibm.com, value = servereast.backup2.ibm.com)

- **type = MX**, indica che il campo **name** contiene il nome di un mail server interno ad un dominio e il campo **value** contiene l'hostname di tale mail server

#### Esempio:

- Un server autoritativo per un hostname contiene un record di tipo A per l'hostname stesso, ad esempio

(corsi.di.uniroma1.it, 131.111.45.68, A)

- Un server non autoritativo per un dato hostname contiene un record di tipo NS per il dominio che include l'hostname e un record di tipo A che fornisce l'indirizzo IP del server DNS nel campo **value** del record NS.

Ad esempio, un server TLD .it che non è autoritativo per l'host corsi.di.uniroma1.it, contiene i due record

(uniroma1.it, dns.uniroma1.it, NS)

(dns.uniroma1.it, 128.119.40.111, A)

## 2.4.2 Protocollo DNS

### Definition 27. Protocollo DNS

Il **protocollo DNS** è un protocollo a livello di applicazione utilizzato per la risoluzione di hostname e nomi di dominio. La sua porta di riferimento comune all'interno dei socket è la **porta 53**.

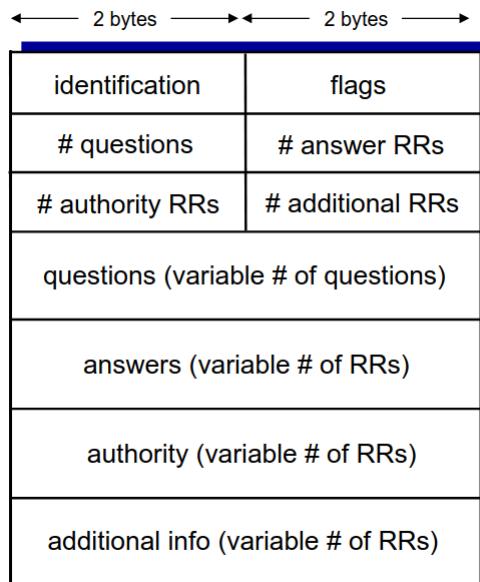
Al fine di rendere il trasferimento il più rapido possibile, il protocollo DNS utilizza il **protocollo UDP**, richiedendo l'invio di un singolo messaggio, evitando necessità della creazione del collegamento. Se un messaggio non giunge a destinazione dopo un determinato timeout, esso viene semplicemente rinvia.

Inoltre, il protocollo DNS è un protocollo **stateless**, (semplicemente poiché non è necessario salvare alcuno stato)

La **richieste** e le **risposte** DNS assumono la stessa struttura:

- Un **header** lungo 32 bit, composto da due campi da 16 bit:
  - **Identification**, contenente informazioni del richiedente
  - **Flags**, contenente flag di stato indicanti se il messaggio sia di richiesta o risposta, se la risoluzione ricorsiva sia preferita o disponibile e se la risposta sia di un server autoritativo

- Un campo **questions** di dimensione variabile contenente le informazioni per una richiesta
- Un campo **answers** di dimensione variabile contenente i RR da inviare come risposta
- Un campo **authority** di dimensione variabile contenente i RR autoritativi da inviare come risposta
- Un campo per le **informazioni aggiuntive**



## 2.5 Trasferimento di file

### 2.5.1 Protocollo FTP

#### Definition 28. Protocollo FTP

Il **protocollo FTP (File Transfer Protocol)** è un protocollo a livello di applicazione utilizzato per il trasferimento di file basato sul **paradigma client-server**.

Per gestire il trasferimento dei file, il protocollo FTP utilizza **due connessioni TCP**:

- Una **connessione di controllo** (porta 21), utilizzata per trasferire le informazioni per il controllo del trasferimento (es: nome utente, password, comandi per cambiare directory e per il trasferimento)
- Una **connessione dati** (porta 20), la quale viene aperta ogni qualvolta sia necessario trasferire un file, per poi chiuderla successivamente

Inoltre, il protocollo FTP è un protocollo **stateful**, conservando la directory corrente e l'autenticazione della sessione precedente

Nel protocollo FTP, il **client** corrisponde al dispositivo avviante il trasferimento verso un dispositivo remoto, mentre il **server** corrisponde al dispositivo remoto stesso.

Quando l'utente fornisce al proprio client il nome del server a cui connettersi tramite il comando `ftp <nome host>`, il processo client FTP stabilisce la **connessione di controllo** sulla porta 21.

Successivamente, il client trasferisce nome utente e password sulla porta 21, autenticandosi. Una volta ottenuta l'autorizzazione dal server, il client può **trasferire uno o più file** memorizzati nel file system locale verso quello remoto (o viceversa), aprendo e chiudendo la connessione dati sulla porta 20 ad ogni trasferimento.



I principali comandi del protocollo FTP sono:

Comando e Argomenti	Descrizione
ABOR	Interrompe il comando precedente
CDUP	Torna alla directory del livello precedente
CWD «nome directory»	Cambia directory corrente
DELE «nome file»	Elimina il file
LIST «nome directory»	Elenca i file nella directory
MDK «nome directory»	Crea una directory
PASS «password»	Invia la password dell'utente
PASV	Il server sceglie la porta della connessione
PORT «porta»	Il client sceglie la porta della connessione
PWD	Mostra nome directory corrente
QUIT	Termina la comunicazione
RETR «nomi dei file»	Trasferisce uno o più file dal server al client
RMD «nome directory»	Elimina la directory
RNTO «vecchio nome» «nuovo nome»	Rinomina il file specificato dal vecchio nome
STOR «nomi dei file»	Trasferisce uno o più file dal client al server
USER «nome utente»	Invia il nome dell'utente

## 2.5.2 Protocollo BitTorrent

### Definition 29. Protocollo BitTorrent

Il **protocollo BitTorrent** è un protocollo a livello di applicazione utilizzato per il trasferimento di file basato sul **paradigma peer-to-peer (P2P)**. Nonostante non abbia una porta standard, solitamente vengono utilizzate le **porte nel range 6881-6889** assieme al **protocollo TCP**.

Ogni peer entra a far parte di un **torrent**, ossia un gruppo di peer scambianti frammenti di file tra loro, registrandosi su un **tracker**, ossia un dispositivo che tiene traccia dei peer partecipanti al torrent, per poi connettersi ad un sottoinsieme di peer "vicini".

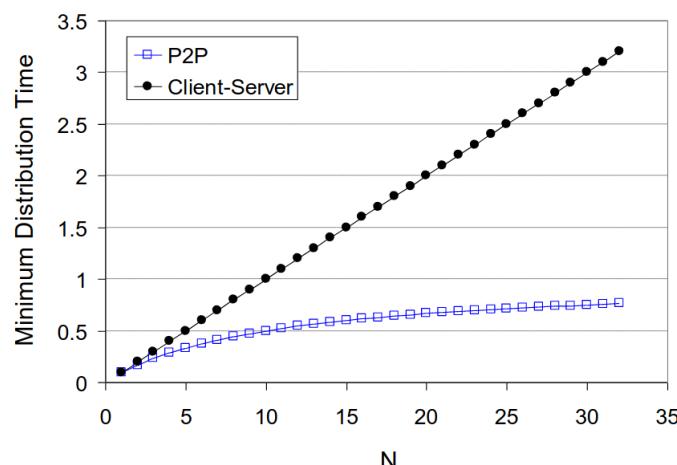
Durante il download di file, il peer svolge anche la funzione di uploader (**seeder**) di blocchi verso altri peer. Una volta ricevuto il file, il peer può scegliere se uscire dal torrent o rimanerne all'interno, continuando a svolgere la funzione di seeder.

In un dato momento, peer diversi possiedono diversi sottoinsiemi di blocchi componenti un file. Per richiedere tali blocchi, un peer chiede periodicamente agli altri l'**elenco dei blocchi** attualmente posseduti. Successivamente, il peer richiede i blocchi mancanti, dando precedenza ai più rari.

Per favorire l'altruismo tra i peer e sfavorire la presenza di **leecher**, ossia dispositivi che egoisticamente escono dal torrent una volta scaricato un file, il protocollo BitTorrent usa un approccio **tit-for-tat** (traduzione più vicina: *do ut des*, "io ti do e tu mi dai" ):

- Ogni peer seeder invia blocchi agli ulteriori quattro peer seeder che attualmente stanno uploadando i blocchi richiesti alla velocità maggiore
- Gli altri peer non appartenenti alla top 4 vengono "strozzati" (**choked**) dal peer seeder, bloccando l'invio dei blocchi ad essi.
- Ogni 10 secondi, tale top 4 viene rivalutata. Inoltre, ogni 30 secondi viene sbloccato casualmente un peer strozzato (**optimistic un-choking**), il quale può entrare o meno a far parte della top 4

Per via di tale approccio, il trasferimento di un file ad  $N$  dispositivi risulta più ottimale nel caso dell'applicazione del paradigma P2P



# Capitolo 3

## Livello di Trasporto

I servizi e protocolli situati nel **livello di trasporto** forniscono **comunicazione logica** tra processi applicativi in esecuzione su dispositivi diversi, a differenza del **livello di rete**, il quale si occupa della comunicazione logica direttamente tra i dispositivi stessi.

In particolare, il dispositivo mittente suddivide i messaggi dell'applicazione in segmenti, passandoli al livello di rete, mentre il dispositivo destinatario riassembra i segmenti in messaggi, passandoli al livello di applicazione.

### 3.1 Multiplexing e Demultiplexing

Per implementare le funzionalità di **multiplexing** e **demultiplexing** al livello di trasporto, ogni host utilizza **indirizzi IP** e **numeri di porta** per indirizzare correttamente un segmento al socket appropriato del destinatario:

- L'header di ogni segmento possiede un numero di porta per l'origine e la destinazione
- Ogni datagramma del livello di rete trasporta un segmento del livello di trasporto
- L'header di ogni datagramma possiede l'indirizzo IP dell'origine e l'indirizzo IP della destinazione

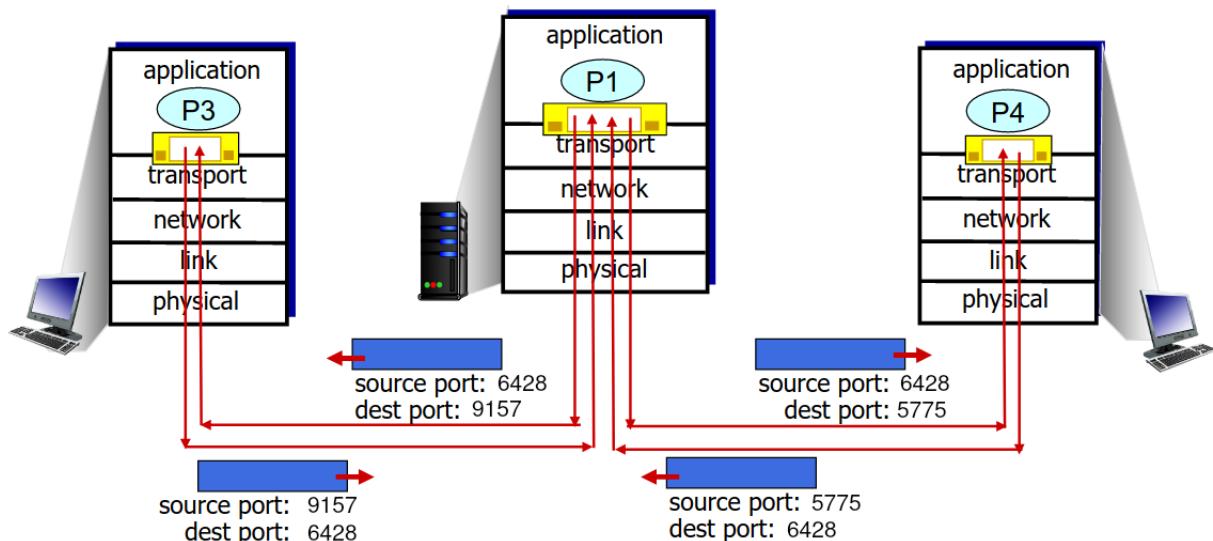


Nel caso di un **demultiplexing senza connessione** (es: protocollo UDP), durante la creazione di un socket all'interno di un processo è necessario specificare la porta locale dell'**host** con cui identificare tale socket.

(es: DatagramSocket d\_soc = new DatagramSocket(12534);)

Successivamente, qualsiasi dispositivo che voglia comunicare con tale host invierà un datagramma al cui interno sia specificata la coppia **indirizzo IP di destinazione** e la **porta di destinazione**. Una volta giunto alla destinazione, verrà letto il numero di porta di destinazione presente nell'header del segmento contenuto all'interno del datagramma ricevuto, indirizzando il segmento al **socket con tale numero di porta**.

In particolare, è necessario sottolineare che, in tal modo, il socket su tale host per la comunicazione con più mittenti sia **unico**. Di conseguenza, qualsiasi datagramma inviato su tale porta apparterrà allo **stesso stream dati**. Tuttavia, essi saranno comunque distinti univocamente dal numero di porta e l'indirizzo IP del mittente presenti nel datagramma.

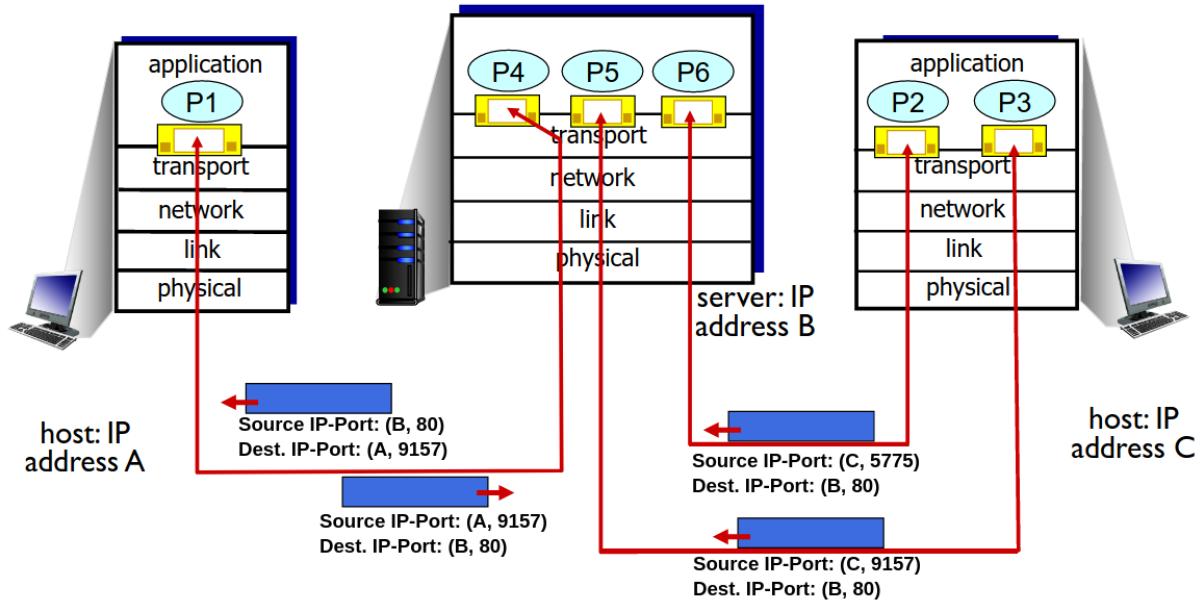


Nel caso del **demultiplexing con connessione** (es: protocollo TCP), invece, **ogni socket viene identificato univocamente come una quadrupla**

(IP\_Orig., Porta\_Orig., IP\_Dest., Porta\_Dest.)

Una volta ricevuto il datagramma, vengono utilizzati tutti e quattro i valori per indirizzare il segmento al socket appropriato. In tal modo, ogni **connessione** è identificata in modo univoco da una **coppia di socket** (una sul primo host ed una sul secondo host), permettendo di implementare le garanzie previste dai protocolli.

Inoltre, per via dell'identificazione univoca dei socket, un host può avere **più socket legati alla stessa porta** con una comunicazione diversa: se due host A e C avviano una connessione avente come destinazione la porta 80 dell'host B, su quest'ultimo verranno creati **due socket diversi**.



## 3.2 Protocollo UDP

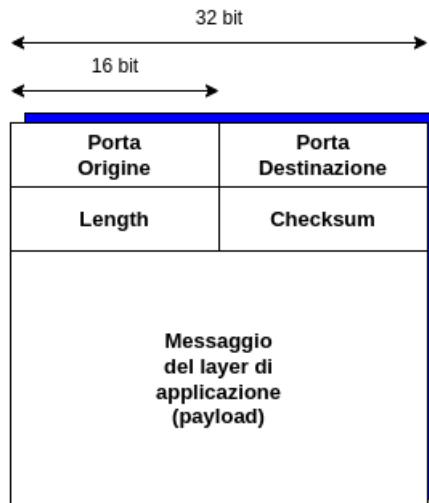
Come già accennato, il **protocollo UDP** è un protocollo di trasporto "senza fronzoli" (**bare bone**) e **senza connessione**. Pertanto, non avviene alcun handshake tra mittente e destinatario, implicando che ogni segmento UDP venga gestito indipendentemente dagli altri. Inoltre, il protocollo UDP svolge un servizio **best-effort**, dunque i segmenti UDP possono essere persi o consegnati in modo non ordinato.

Tuttavia, tali caratteristiche rendono UDP **vantaggioso** in alcune casistiche:

- Poiché non vi è alcuna connessione, il protocollo risulta semplice, oltre all'**assenza del ritardo RTT** necessario per l'handshake richiesto
- La dimensione dell'header è minima, rendendo il **pacchetto più leggero**
- L'**assenza di controllo della congestione** permette al protocollo UDP di tentare la trasmissione senza alcun limite di velocità e il funzionamento anche in casi di congestione dovuti ad un carico elevato sui nodi della rete
- Se si vuole rendere il trasferimento affidabile anche utilizzando UDP, basta implementare l'affidabilità necessaria al livello di applicazione (es: HTTP/3 tramite il protocollo QUIC), piuttosto che al livello di trasporto

In particolare, l'header utilizzato dal protocollo UDP, oltre a contenere le porte di origine e di destinazione, contiene solamente due campi aggiuntivi:

- Un campo **length** (16 bit), indicante la lunghezza del contenuto
- Un campo **checksum** (16 bit), utilizzato per rilevare errori nel segmento trasmesso



Il valore di **checksum** viene calcolato tramite una **somma in complemento ad uno con wrap-around**:

1. Il mittente considera il contenuto del segmento (compresi gli altri campi dell'header e gli indirizzi IP) come una sequenza di numeri interi a 16 bit
2. Il mittente calcola il checksum sommando in **complemento ad 1** (ossia sommando e poi invertendo tutti i bit) i numeri interi della sequenza.

In particolare, se è presente un riporto finale generato dalla somma del bit più significativo, viene sommato anche tale riporto (**wrap-around**)

3. Il valore del checksum viene inserito nel campo dell'header e il pacchetto continua il processo di trasmissione
4. Una volta giunto a destinazione, l'host ricevente **calcola nuovamente il checksum**, verificando che sia uguale a quello inserito nell'header del segmento.

Se il checksum è differente, viene rilevato un **errore** nella trasmissione

Tuttavia, è necessario notare che se il **checksum è uguale non è detto** che la trasmissione non abbia generato alcun errore:

- Consideriamo il calcolo del checksum tra i seguenti numeri interi a 16 bit:

$$\begin{array}{r}
 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ + \\
 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 = \\
 \hline
 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1
 \end{array}$$

- Poiché è presente un riporto, viene effettuato il **wrap-around** sommando tale riporto ai restanti 16 bit:

$$\begin{array}{r}
 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ + \\
 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 = \\
 \hline
 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \\
 \quad \downarrow \quad \downarrow \quad \downarrow \\
 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0
 \end{array}$$

- Infine, vengono **invertiti i bit** del risultato per ottenere la somma in complemento ad 1

$$\begin{array}{cccccccccccccccccc}
 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
 & & & & & & \downarrow & \downarrow & \downarrow & & & & & & & & \\
 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1
 \end{array}$$

- Tuttavia, nel caso in cui i due bit meno significativi di entrambi i numeri fossero stati invertiti (per qualche motivo sconosciuto) durante la trasmissione, il **checksum calcolato sarebbe identico**

$$\begin{array}{cccccccccccccccccc}
 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & + \\
 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & = \\
 \hline
 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1
 \end{array}$$

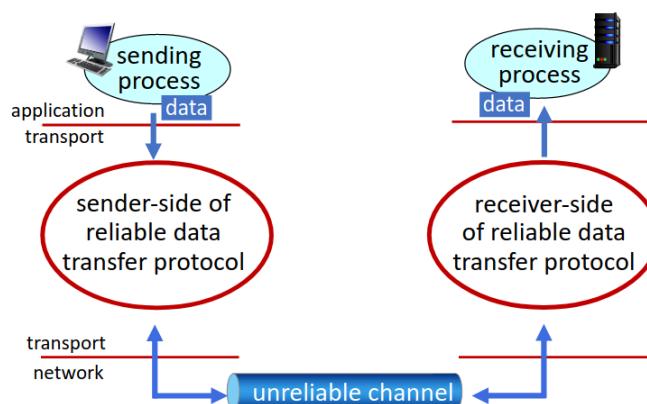
$$\begin{array}{cccccccccccccccccc}
 & & & & & & \downarrow & \downarrow & \downarrow & & & & & & & & \\
 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
 & & & & & & \downarrow & \downarrow & \downarrow & & & & & & & & \\
 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1
 \end{array}$$

### 3.3 Trasferimento affidabile dei dati

Per realizzare un trasferimento affidabile dei dati, è necessario implementare un **canale sicuro** al cui interno non vengano perse o corrotte informazioni.



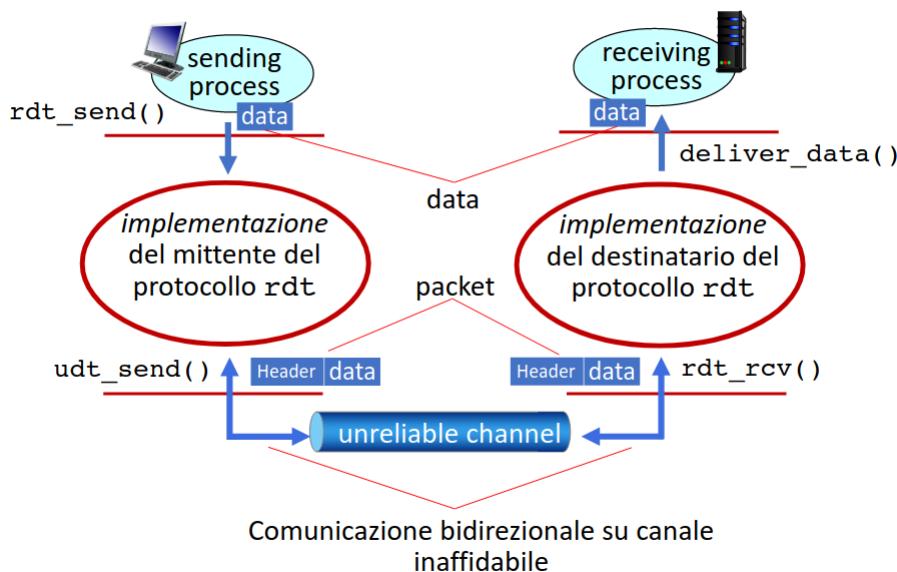
Tuttavia, un canale fisico che possa svolgere tale funzione risulta essere irrealizzabile. Per tale motivo, la complessità del **protocollo di trasferimento dati affidabile (RDT - Reliable Data Transfer)** dipende fortemente dalle caratteristiche del canale inaffidabile utilizzato.



Inoltre, è necessario puntualizzare che il mittente e il destinatario **non conoscono lo stato l'uno dell'altro** (es: se la ricezione sia andata a buon fine), a meno che non gli venga comunicato tramite un ulteriore messaggio.

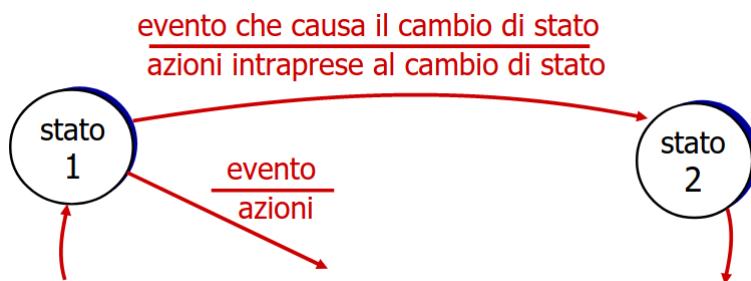
Il protocollo RDT presenta delle **interfacce** per il suo utilizzo:

- **rdt\_sent(data)**, il quale viene chiamato dal livello di applicazione e il cui argomento corrisponde ai dati da inoltrare al destinatario
- **udt\_send()**, dove UDT è acronimo di Unreliable Data Transfer, il quale viene chiamato dal protocollo RDT sul mittente per trasferire il pacchetto sul canale inaffidabile
- **rdt\_rcv()**, il quale viene chiamato alla ricezione del pacchetto dal destinatario
- **deliver\_data()**, il quale viene chiamato dal protocollo RDT sul destinatario per inoltrare al livello di applicazione i dati ricevuti



Poiché i dispositivi comunicanti non sono a conoscenza dello stato altrui, il protocollo RDT si basa su un **trasferimento dei dati unidirezionale**, dunque come se uno solo dei due sia il mittente ed uno solo sia il destinatario (sebbene in realtà sia bidirezionale).

Per rappresentare le operazioni e le decisioni effettuate dal protocollo, utilizzeremo le **macchine a stati finiti** (FSM - Finite State Machine) e in particolare la seguente notazione:



### 3.3.1 Protocollo RDT 1.0 e 2.0

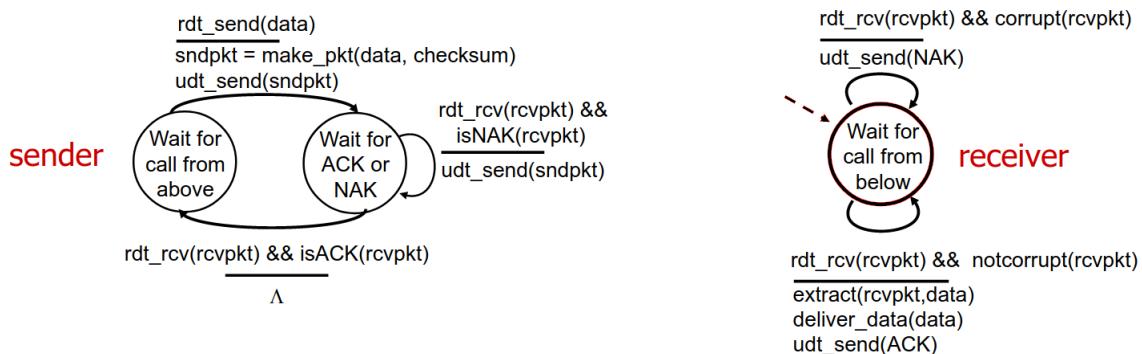
All'interno del **protocollo RDT 1.0**, viene assunto che il canale sottostante utilizzato per il trasferimento sia **perfettamente affidabile**, implicando che il mittente invii i dati nel canale e il ricevitore li legga direttamente, senza alcuna operazione aggiuntiva



Nel **protocollo RDT 2.0**, invece, viene assunto che il canale sottostante possa invertire alcuni bit nel pacchetto inviato. Analogamente al protocollo UDP, viene utilizzato un **checksum** per rilevare la presenza di errori. Nel caso in cui venga rilevato uno di quest'ultimi, il destinatario comunicherà al mittente l'esito dell'operazione:

- **Acknowledgements (ACK)**, dove il destinatario dice esplicitamente al mittente che il pacchetto è stato ricevuto senza problemi
- **Negative acknowledgements (NAK)**, dove il destinatario dice esplicitamente al mittente che il pacchetto ricevuto presenta degli errori

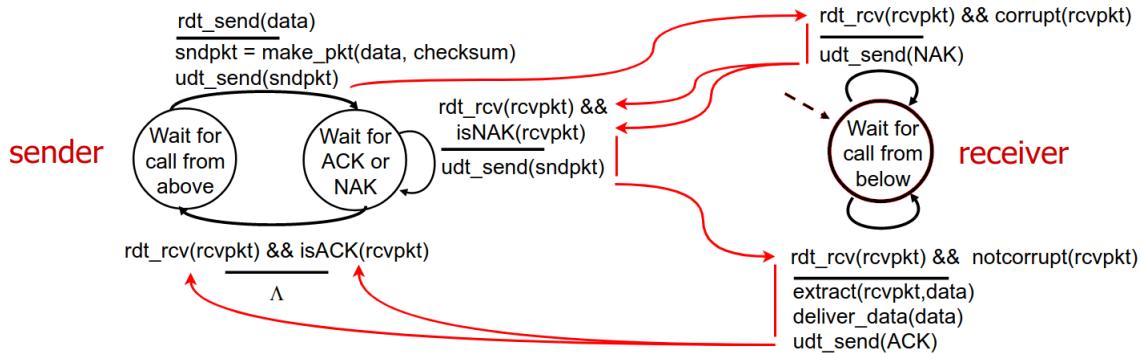
Successivamente all'invio di un pacchetto, il mittente rimane in attesa della risposta del destinatario (meccanismo **stop and wait**)



Se la risposta ricevuta è un **ACK**, il mittente torna il stato di attesa del prossimo pacchetto da parte del livello applicativo.



Se invece la risposta è un **NAK**, il mittente rinvia il pacchetto generante l'errore e rimane in attesa della risposta del destinatario, ripetendo nuovamente tale processo nel caso in cui si riceva nuovamente un NAK.



Tuttavia, la versione 2.0 del protocollo RDT presenta un **difetto fatale**: se la risposta ACK/NAK è corrotta, il mittente non è più a conoscenza di cosa sia accaduto al destinatario. Inoltre, non è sufficiente ritrasmettere il pacchetto per risolvere tale difetto, poiché il destinatario potrebbe ricevere due pacchetti duplicati ed inoltrarli al livello di applicazione.

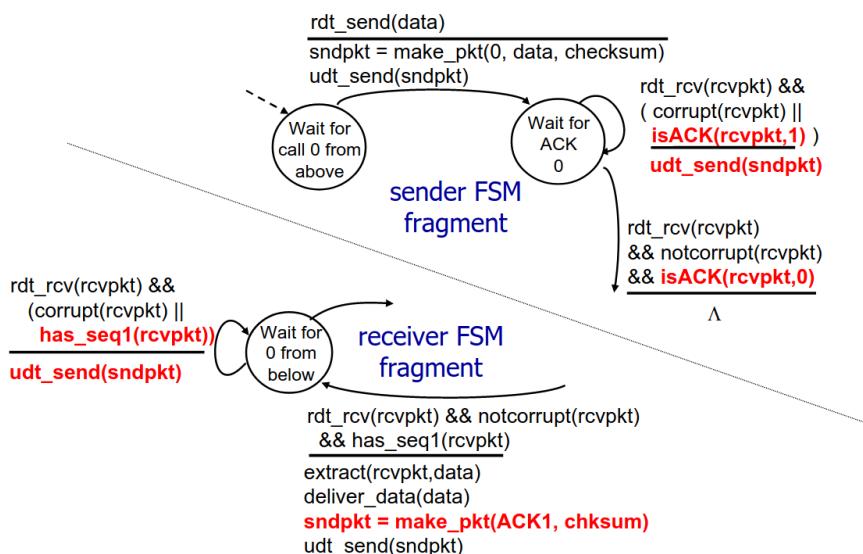
### 3.3.2 Protocollo RDT 2.1 e 2.2

Per risolvere il difetto fatale della versione 2.0, il **protocollo RDT 2.1**:

- Viene controllato se la risposta ACK/NAK sia **corrotta**. Nel caso in cui lo sia, il pacchetto viene rinvia.
- Il destinatario non è a conoscenza della possibile corruzione del pacchetto ACK/-NAK
- Viene aggiunto un **numero di sequenza** al pacchetto inviato. In particolare, sono necessari i numeri di sequenza 0 ed 1 affinché il protocollo stop and wait possa funzionare correttamente:
  - Assieme alla risposta di ACK, il destinatario invia un **numero di riscontro**, il quale, per convenzione, indica sempre il numero di sequenza del prossimo pacchetto atteso dal destinatario
  - Se il destinatario ha ricevuto correttamente il pacchetto 0, invia un riscontro con valore 1 (dunque il prossimo pacchetto atteso è il pacchetto 1)
  - Analogamente, se il destinatario ha ricevuto correttamente il pacchetto 1, invia un riscontro con valore 0 (dunque il prossimo pacchetto atteso è il pacchetto 0)
- Se il pacchetto ricevuto dal destinatario è un duplicato, esso viene automaticamente scartato senza essere inviato al livello di applicazione



In aggiunta alle modifiche della versione 2.1, il protocollo RDT 2.2 **elimina** la necessità di una risposta **NAK**: il ricevitore invia come numero di riscontro il numero di sequenza dell'**ultimo pacchetto correttamente**. In tal modo, un ACK duplicato al mittente comporta la stessa azione di un NAK, ossia la ritrasmissione del pacchetto corrente.



### 3.3.3 Protocollo RDT 3.0

Oltre all'assunzione di possibili bit invertiti, il **protocollo RDT 3.0** assume la possibilità di una **perdita di pacchetti**, sia dati che ACK. Per risolvere tale problematica, il mittente **attende un lasso di tempo**:

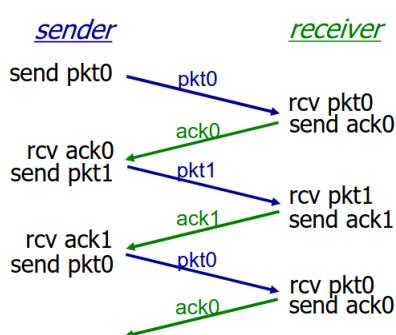
- Il destinatario deve specificare il **numero di sequenza del pacchetto** per il quale sta inviando un ACK
- Se non viene ricevuto alcun ACK allo scadere del lasso di tempo, il pacchetto dati (che indicheremo con pkt) viene ritrasmesso
- Se pkt o ACK arrivano successivamente allo scadere del tempo, il pacchetto verrà ritrasmesso, implicando che la trasmissione verrà duplicata (problema già gestito dai numeri di sequenza)

La FSM associata al mittente corrisponde a:

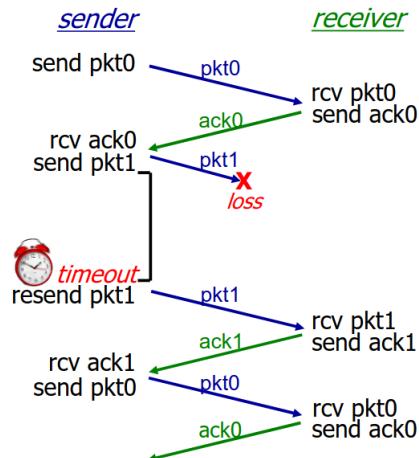


Di seguito, vengono mostrati alcuni esempi di gestione tramite protocollo RDT 3.0:

Nessuna perdita



Perdita di pkt





Tuttavia, in cambio dei notevoli benefici del meccanismo stop and wait, le **prestazioni** del protocollo RDT 3.0 risultano essere **infime**, limitando le prestazioni dell'infrastruttura sottostante, ossia il canale.

In particolare, la **percentuale di utilizzo**  $U_{mit}$  della comunicazione da parte del mittente, ossia la frazione di tempo in cui il mittente è impegnato nell'invio corrisponde a:

$$U_{mit} = \frac{D_t}{RTT + D_t}$$

dove  $D_t$  è il delay di trasmissione (dunque  $D_t = \frac{L}{R}$  con  $L$  la lunghezza del pacchetto e  $R$  il transmission rate del link)



### Esempio:

- Considerando un link avente un rate pari a  $R = 1 \text{ Gb/s}$ , una lunghezza di pacchetto pari a  $L = 8000 \text{ b}$  e un ritardo di propagazione sia pari a 15 ms, la percentuale di utilizzo del mittente corrisponde a:

$$D_t = \frac{8 \cdot 10^3 \text{ b}}{10^9 \text{ b/s}} = 8 \mu\text{s}$$

$$U_{mit} = \frac{8 \mu\text{s}}{30 \text{ ms} + 8 \mu\text{s}} = 27 \cdot 10^{-5} = 0.027\%$$

### 3.3.4 Go-back-N e Selective repeat

Per migliorare le prestazioni del protocollo RDT 3.0, viene utilizzato il **pipelining**, dove il mittente consente la presenza di molteplici trasferiti senza aver ricevuto un ACK precedente.

Per realizzare il pipelining, l'**intervallo di numeri di sequenza** deve essere **aumentato**, poiché è necessario tener traccia di più pacchetti simultaneamente, richiedendo inoltre la presenza di un **buffer** interno al mittente e al destinatario.

Poiche i pacchetti successivi al primo vengono inviati durante contemporaneamente al RTT del primo pacchetto, è sufficiente considerare un solo RTT, incrementando notevolmente la percentuale di utilizzo del mittente:

**Esempio:**

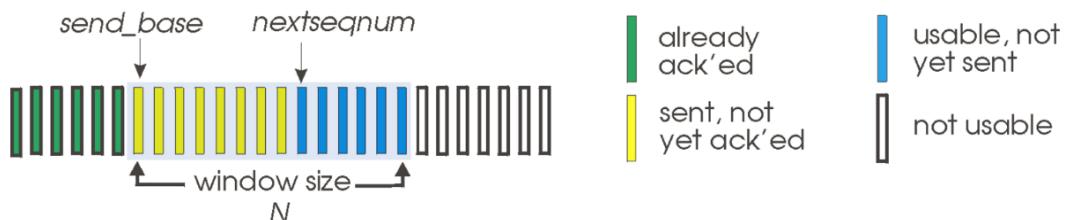
- Riprendendo i dati dell'esempio precedente, effettuando il pipelining con 3 pacchetti si ha che

$$U_{mit} = \frac{3 \cdot D_t}{RTT + D_t} = 3 \cdot \frac{8 \mu s}{30 ms + 8 \mu s} = 81 \cdot 10^{-5} = 0.081\%$$



Una delle metodologie con cui viene implementato il pipelining è il **Go-back-N**:

- Il mittente ha una "finestra" di  $N$  pacchetti consecutivi trasmessi senza ACK (**ACK cumulativo**). La ricezione del pacchetto **ACK(n)** viene interpretato dal mittente come un ACK per ognuno dei singoli  $N$  pacchetti, implicando che alla sua ricezione la finestra venga spostata in avanti in modo che essa abbia il pacchetto  $N + 1$  come primo pacchetto



- Viene mantenuto attivo un **timer** per il pacchetto della finestra inviato e senza ACK **più vecchio**. Una volta scaduto tale timeout, viene ritrasmesso il pacchetto e tutti i pacchetti con numero di sequenza maggiore presenti all'interno della finestra

- Il destinatario invia sempre l'**ACK con numero di sequenza maggiore** (in ordine) per i pacchetti attualmente ricevuti **correttamente**, implicando che non vi siano pacchetti con numero di sequenza minore mancanti.

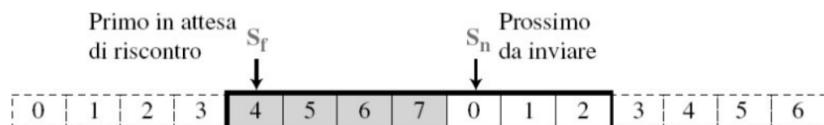
Tale procedura potrebbe generare ACK duplicati e richiede di ricordare solamente un **valore `rcv_base`** (a differenza della finestra del mittente), corrispondente al numero di sequenza del pacchetto di cui si è in attesa

- Se il destinatario riceve un pacchetto fuori ordine, può, a seconda dell'implementazione, scartare tale pacchetto (**politica don't buffer**) o conservarlo (**politica buffer**), inviando in entrambi i casi un ACK con il più alto numero di sequenza che si trovi nell'ordine corretto, richiedendo quindi la trasmissione di tutti i pacchetti con numero di sequenza maggiore.

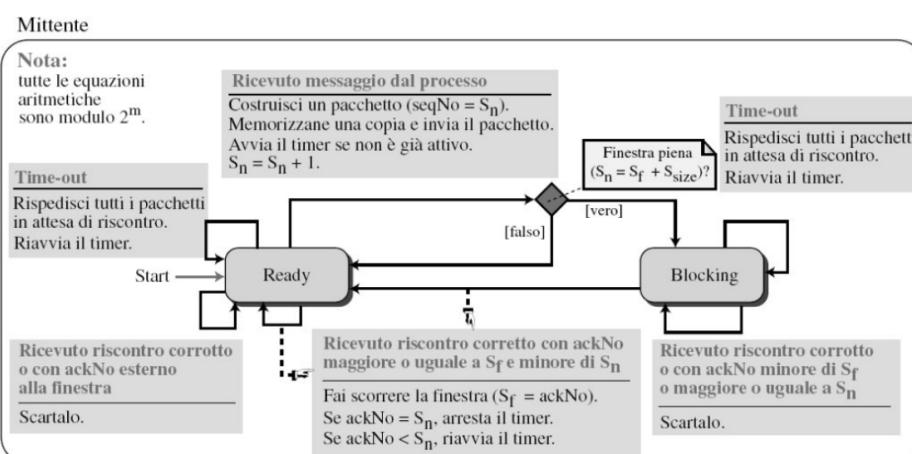
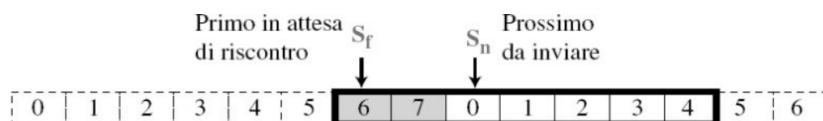


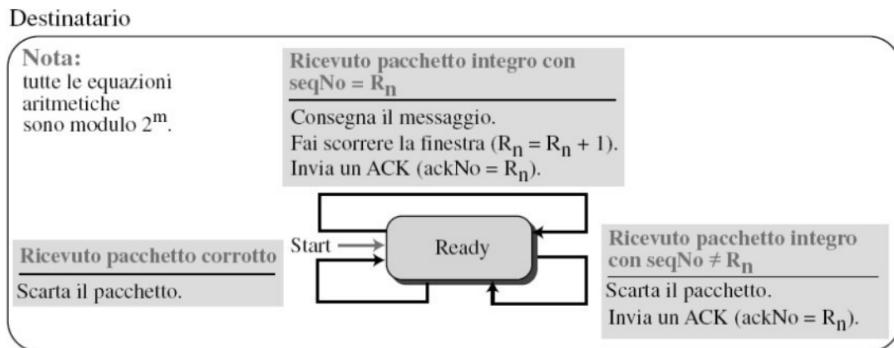
### Esempio:

- Consideriamo la seguente finestra di 7 pacchetti

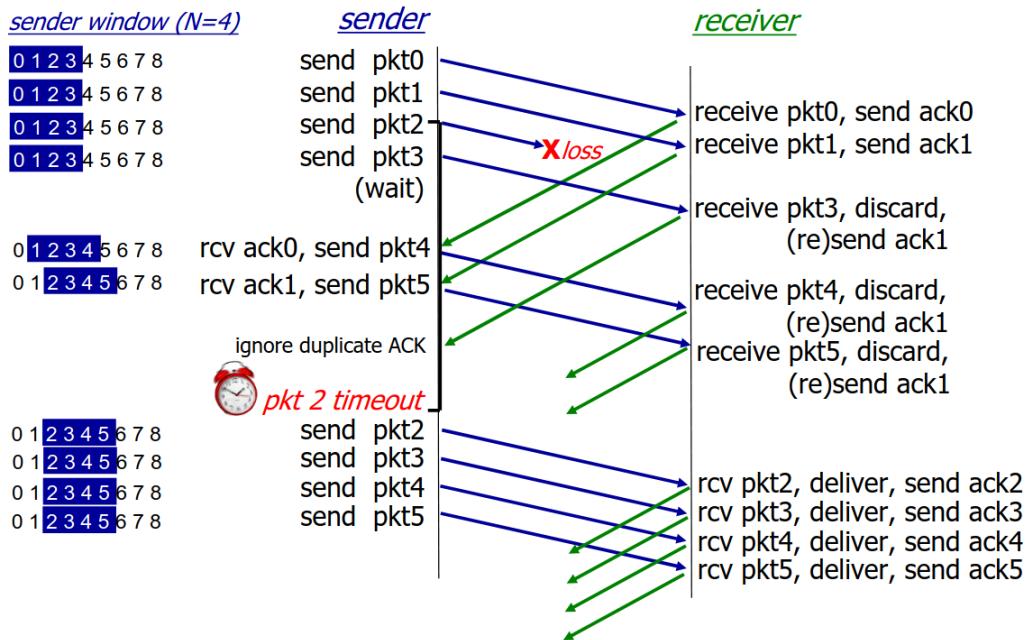


- Una volta ricevuto ACK(5), i pacchetti 4 e 5 vengono considerati come arrivati a destinazione, scorrendo la finestra in avanti





Esempio (protocollo Go-back-N con politica don't buffer):



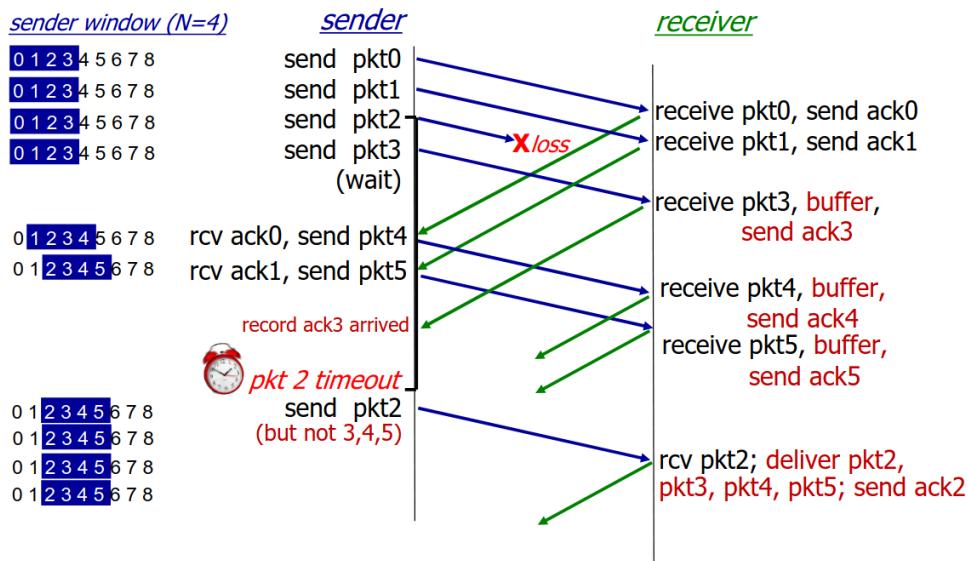
Poiché nel caso in cui un singolo pacchetto venga perso o corrotto è necessario rinviare tutti i pacchetti successivi già inviati nella pipeline, il protocollo Go-back-N può **peggiорare la congestione della rete**.

Contrariamente, il **protocollo Selective Repeat** è in grado di gestire tale problematica:

- Oltre al mittente, anche il destinatario è dotato di una **finestra di  $N$  pacchetti**
- Il destinatario conferma **individualmente** tutti i pacchetti ricevuti correttamente, anche nel caso in cui essi siano fuori sequenza, **bufferizzandoli** per l'eventuale consegna in ordine al livello superiore
- Il mittente mantiene un **timer per ogni pacchetto** inviato senza ACK, rinvia ogni pacchetto individualmente alla scadenza del suo timeout
- La finestra del mittente scorre a partire dal **pacchetto più alto confermato in ordine** (senza pacchetti non confermati prima di esso). Alla ricezione dell'ACK di un pacchetto, dunque, se tale pacchetto era il più piccolo pacchetto non ancora confermato, la finestra avanza fino al prossimo pacchetto non confermato

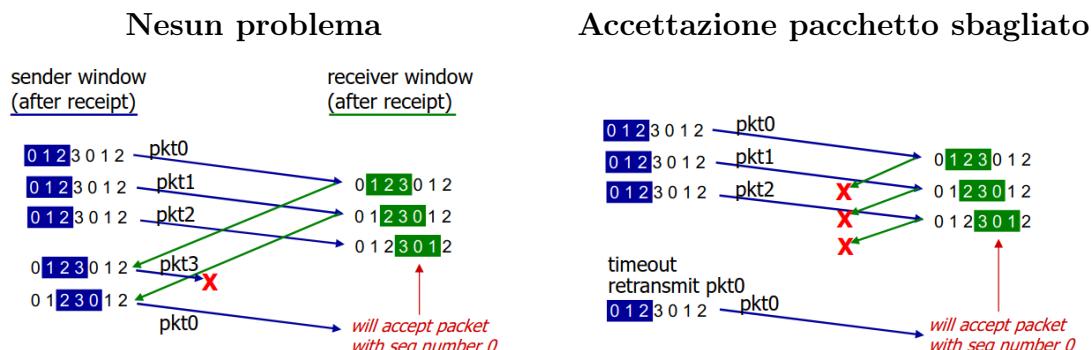


Esempio:



Tuttavia, anche il protocollo Selective Repeat non è privo di problematiche. In particolare, se la dimensione della finestra è troppo piccola, si può andare in contro a casi sfavorevoli (**dilemma della finestra**).

Ad esempio, con un range di numeri di sequenza pari a 0, 1, 2, 3 e una finestra di dimensione 3, si ha che:



**Esempio:**

- In una rete con un valore fisso  $m > 1$  (numero di bit della sequenza), è possibile utilizzare entrambi i meccanismi Go-Back-N e Selective Repeat, si indichino i vantaggi e gli svantaggi dell'impiego di ciascuno di essi. Quali altre considerazioni si devono fare per decidere quale meccanismo utilizzare?

- **Go-back-N**

- Ritrasmette tutti i frame inviati dopo il frame che si sospetta essere danneggiato o perso
- Se il tasso di errore è alto, spreca molta larghezza di banda
- Meno complicato
- Window size  $N - 1 = 2^m - 1$
- Riordinamento non è richiesto né lato mittente né lato destinatario
- Il destinatario non memorizza i frame ricevuti dopo il frame corrotto finché esso non viene ritrasmesso (dipende dall'implementazione)
- Non è richiesta alcuna ricerca di frame né lato mittente né destinatario

- **Selective Repeat**

- Ritrasmette solo i frame sospettati di essere persi o danneggiati
- Comparativamente meno larghezza di banda viene sprecata nella ritrasmissione
- Più complesso in quanto richiede l'applicazione di logica aggiuntiva, ordinamento e archiviazione, lato mittente e destinatario
- Window size  $\frac{N+1}{2} = 2^{m-1}$
- Il destinatario deve essere in grado di ordinare in quanto deve mantenere la sequenza dei frame
- Il destinatario memorizza i frame ricevuti dopo il frame danneggiato nel buffer finché il frame danneggiato non viene sostituito
- Il mittente deve essere in grado di cercare e selezionare il frame richiesto

Un'idea aggiuntiva implementata nei **trasferimenti bidirezionali** (dunque dove entrambi i dispositivi sono sia mittente sia destinatario, coincidenti con la vita reale) è il **piggybacking**, dove nel momento in cui un pacchetto stia trasportando dati dal dispositivo A al dispositivo B, vengono trasportati anche i riscontri ricevuti da A inerenti ai pacchetti ricevuti da B, in modo che entrambi i dispositivi ne siano a conoscenza, gestendo efficientemente il rinvio dei pacchetti.

## 3.4 Protocollo TCP

Il **protocollo TCP** è un protocollo **end-to-end**, ossia con un solo mittente ed un solo destinatario, offrendo un **byte stream affidabile e in ordine**, dove i messaggi del livello di applicazione vengono concatenati in un unico stream, a differenza dell'UDP, dove ogni messaggio è un segmento diverso.

Come già discusso, il protocollo TCP è **orientato alla connessione**, dove l'**handshaking** inizializza lo stato del mittente e del destinatario prima dello scambio dei dati.

Il flusso dati, inoltre è **full duplex**, ossia bidirezionale all'interno della stessa connessione (dati full duplex), limitati tuttavia da un **Maximum Segment Size (MSS)**. Tuttavia, è necessario sottolineare che si tratta di un paradigma diverso dalla commutazione di circuito, poiché la rete non è a conoscenza dello stabilimento della connessione.



Per gestire il trasporto affidabile, il protocollo TCP utilizza:

- **ACK cumulativi** e **pipelining**, dove il window size dipende dal **flow control**, ossia una garanzia sul non sovraccarico del destinatario da parte del mittente, e dal **congestion control**, ossia una garanzia sol non sovraccarico della rete da parte del mittente
- Il **numero di sequenza** dei segmenti del protocollo TCP corrisponde al numero di sequenza del **primo byte del settore data** del segmento stesso. Per quanto riguarda l'**ACK**, viene utilizzato il numero di sequenza del **byte successivo aspettato**.
- Nel momento in cui il mittente riceve dati dal livello di applicazione, viene creato il segmento e il suo numero di sequenza, avviando il timer a meno che esso non sia già in esecuzione. Inoltre, il **timer** utilizzato è **singolo** e collegato al **segmento non confermato più vecchio**. Allo scadere del **TimeoutInterval**, viene ritrasmesso il segmento che ha causato il timeout, riavviando il timer.

- Alla **ricezione di un ACK**, invece, se quest'ultimo copre segmenti precedentemente non confermati, vengono aggiornate le informazioni di tali pacchetti, avviando il timer se vi sono ancora segmenti non confermati, il quale sarà collegato al nuovo segmento più vecchio (ibrido tra Go-back-N e Selective Repeat)



Per quanto riguarda il destinatario, invece, si hanno quattro scenari:

- All'arrivo di un **segmento in ordine**, con **numero di sequenza atteso** e tutti i segmenti **precedenti già confermati**, viene inviato un **delayed ACK**: dopo aver atteso 500 ms per il prossimo segmento, se quest'ultimo non è stato ricevuto viene inviato l'ACK
- All'arrivo di un **segmento in ordine**, con **numero di sequenza atteso** e ma con un segmento precedente **non ancora confermato**, viene immediatamente inviato un ACK cumulativo confermando entrambi i segmenti
- All'arrivo di un **segmento fuori ordine** e con numero di sequenza maggiore di quello atteso (dunque vi è un **gap**), viene inviato immediatamente un ACK duplicato
- All'arrivo di un segmento che in parte o totalmente **riempie in ordine un gap**, viene immediatamente inviato l'ACK



### 3.4.1 Gestione del timeout e stima del RTT

Il valore di timeout impostato deve essere **più lungo di un RTT**. Tuttavia, poiché il RTT è variabile, è necessario **stimarlo**.

Se il timeout scelto è **troppo corto**, si verificheranno troppi timeout prematuri, creando una serie di ritrasmissioni non necessarie. Se invece è **tropo lungo**, vi è una reazione troppo lenta a seguito della perdita di un pacchetto.

Per stimare il RTT, viene campionato un valore **SampleRTT**, ossia il tempo misurato dalla trasmissione del segmento fino alla ricezione dell'ACK (ignorando le ritrasmissioni). Poiché SampleRTT varia, viene utilizzata una **media delle misurazioni recenti** e non solo dell'ultimo SampleRTT (EWMA - Exponential Weighted Moving Average):

$$\text{EstimatedRTT} = (1 - \alpha) \cdot \text{PreviousEstimatedRTT} + \alpha \cdot \text{SampleRTT}$$

dove tipicamente si ha  $\alpha = 0.125$  e dove l'influenza del campione passato diminuisce in modo esponenziale



Il valore del **TimeoutInterval**, dunque, corrisponderà al valore attuale dell'EstimatedRTT sommato ad un **margine di sicurezza**

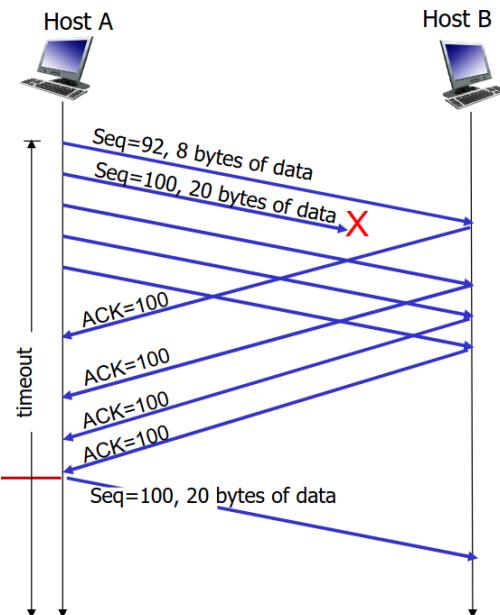
$$\text{TimeoutInterval} = \text{EstimatedRTT} + 4 \cdot \text{DevRTT}$$

dove DevRTT è l'EWMA della deviazione di SampleRTT da EstimatedRTT

$$\text{DevRTT} = (1 - \beta) \cdot \text{PreviousDevRTT} + \beta |\text{SampleRTT} - \text{EstimatedRTT}|$$

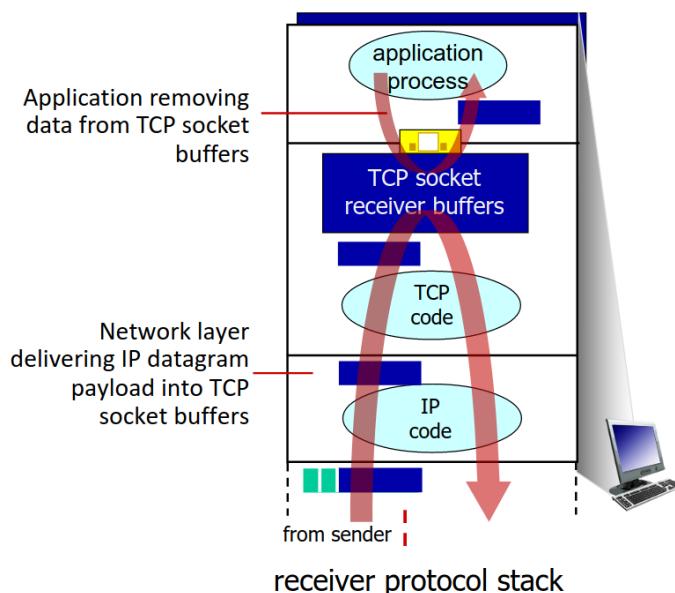
con un valore tipico  $\beta = 0.25$

Un'ottimizzazione ulteriore del protocollo TCP prevede l'implementazione del **fast retransmit**: se il mittente riceve 3 ACK aggiuntivi per gli stessi dati (dunque **tre ACK duplicati**), viene nuovamente inviato il segmento non confermato con numero di sequenza più piccolo poiché probabilmente tale segmento è andato perso, dunque non è necessario aspettare il timeout



### 3.4.2 Controllo del flusso

Per poter funzionare correttamente, il protocollo TCP necessita di un **controllo del flusso**. Ad esempio, se la velocità con cui il livello di rete del destinatario fornisce i dati è maggiore rispetto a quella con cui il suo livello di applicazione rimuove i dati dal buffer del socket, il buffer andrà in **overflow**, implicando che i dati in eccesso vengano necessariamente **scartati**, risultando tuttavia come ricevuti correttamente dal destinatario.



Di conseguenza, è necessario che il **destinatario controlli il mittente**, impedendo che quest'ultimo possa riempire il buffer del destinatario trasmettendo troppi dati velocemente. Per gestire il flusso, quindi, viene utilizzata un campo **rwnd** (**receive window**) all'interno del segmento TCP:

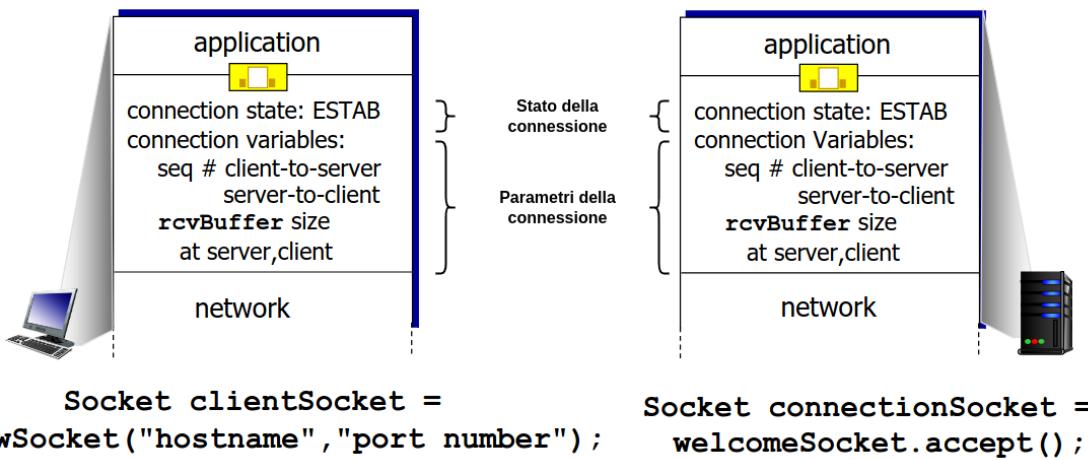
- Il destinatario inserisce in **rwnd** il numero di byte che è disposto ad accettare (dunque lo spazio rimanente nel buffer del socket)
- La dimensione del **RcvBuffer** impostata tramite le opzioni socket (predefinito a 4096 byte) o gestita automaticamente dal sistema operativo
- Il mittente limita la quantità di dati inviati senza ACK al valore di **rwnd**, garantendo che il buffer di ricezione non vada in overflow



Buffering lato destinatario TCP

### 3.4.3 Gestione della connessione

Prima di effettuare lo scambio di dati, il mittente e il destinatario effettuano un **handshake**, dove viene determinata la disponibilità dell'un e dell'altro ad accettare di stabilire una connessione, concordando i parametri di quest'ultima (es: l'inizio del numero di sequenza)



Una prima implementazione dell'handshake è l'**handshake a 2 vie**, dove il mittente invia la richiesta di connessione al destinatario, il quale invia successivamente l'accettazione di tale richiesta, assumendo lo stato di connessione **ESTAB** (established).

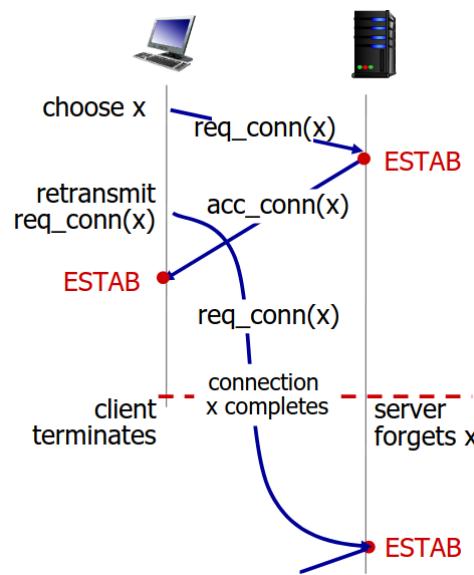
Una volta ricevuta l'accettazione, anche il mittente assumerà lo stato ESTAB, per poi procedere con l'invio effettivo dei dati.



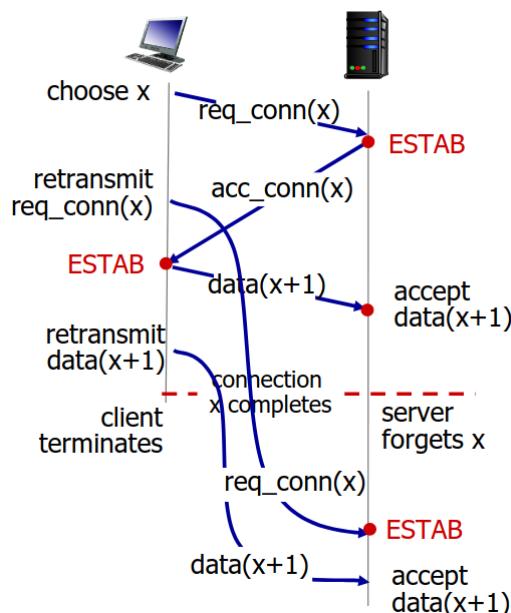
Tuttavia, in tale implementazione il destinatario **non è a conoscenza** della **ricezione** da parte del mittente del pacchetto di **accettazione** della connessione, presentando quindi **due problematiche fondamentali**:

- Nel caso in cui il mittente **rinvii la richiesta** di connessione allo scadere del timer TCP e l'accettazione del destinatario inerente alla prima richiesta giunge comunque dopo lo scadere del timer, il mittente suppone che la connessione sia andata a buon fine (nonostante il RTT sia estremamente basso), stabilendo quindi una **prima connessione**.

- Se tale connessione viene **terminata** prima che la seconda richiesta del mittente sia giunta al destinatario, quest'ultimo interpreterà la richiesta come una richiesta appartenente ad un'**seconda connessione**.
- Tuttavia, poiché tale richiesta era solo un rinvio della prima richiesta connessione, il client ignorerà la seconda richiesta di accettazione del server, creando quindi una **connessione fantasma senza client**



- Inoltre, nel caso in cui venga stabilita una connessione fantasma, si potrebbe andare incontro ad accettazioni di pacchetti dati duplicati

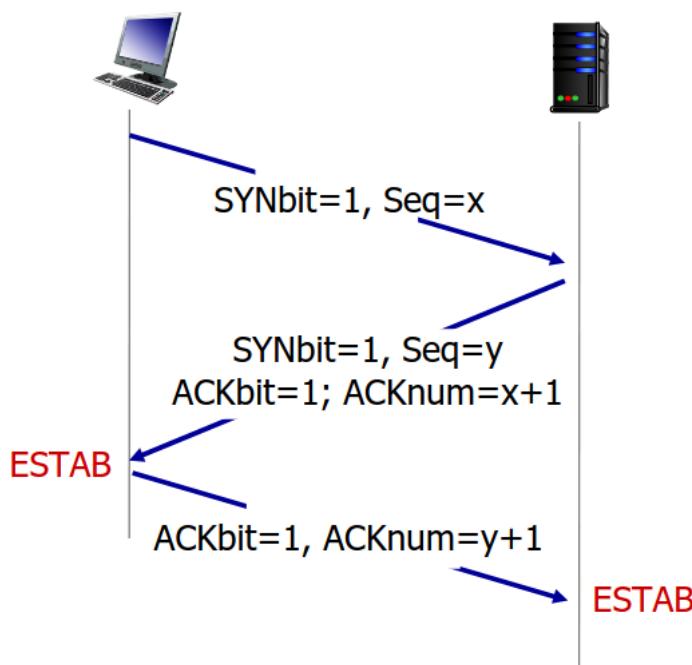


Di conseguenza, l'handshake TCP viene implementato attraverso uno scambio di 3 messaggi (**handshake a 3 vie**):

- Il mittente sceglie un numero di sequenza iniziale  $x$  e invia un pacchetto di tipo **SYN (synchronize)** al destinatario, richiedendo di stabilire una connessione.

Per inviare un pacchetto di tipo SYN, è sufficiente impostare il campo **SYN = 1** all'interno dell'header

- Una volta ricevuto il pacchetto SYN, il destinatario sceglie un numero di sequenza iniziale  $y$  e invia un pacchetto di tipo **SYN/ACK (synchronize and ACK)** al mittente, impostando i campi **SYN = 1** e **ACK = 1** nell'header
- Una volta ricevuto il pacchetto SYN/ACK, il mittente invia un pacchetto di tipo ACK (dunque con solo **ACK = 1**), passando in stato **ESTAB**
- Infine, una volta ricevuto il pacchetto ACK, anche il destinatario passerà in stato **ESTAB**



In questo modo, il destinatario sarà a conoscenza dello stato finale del mittente, risolvendo le due problematiche.

Per effettuare la **chiusura di una connessione**, il primo dispositivo (mittente o destinatario che sia) invia al secondo dispositivo un pacchetto di tipo **FIN (finished)**. Una volta ricevuto il pacchetto FIN, il secondo dispositivo risponderà con un pacchetto FIN/ACK, per poi inviare, dopo un breve lasso di tempo, un secondo pacchetto FIN. Analogamente, anche il primo dispositivo una volta ricevuto il pacchetto FIN invierà un pacchetto FIN/ACK.

Utilizzando tale **handshake a 4 vie**, entrambi i dispositivi riescono accertarsi il corretto termine della connessione. Inoltre, in tal modo entrambi i dispositivi possono terminare la connessione simultaneamente (creando una sorta di doppio handshake a 2 vie)

## 3.5 Controllo della congestione

A differenza del **controllo del flusso**, il quale si occupa di gestire un mittente troppo veloce per un destinatario, il **controllo della congestione** si occupa di gestire situazioni in cui vi sono troppe fonti che inviano una grande quantità di dati troppo velocemente per poter essere gestiti correttamente dalla rete.

In presenza di congestione della rete, si manifestano **lunghi ritardi**, dovuti all'accodamento di troppi pacchetti nel buffer dei router, e **perdita di pacchetti**, dovuti agli overflow dei buffer dei vari router.

### 3.5.1 Cause e costi della congestione

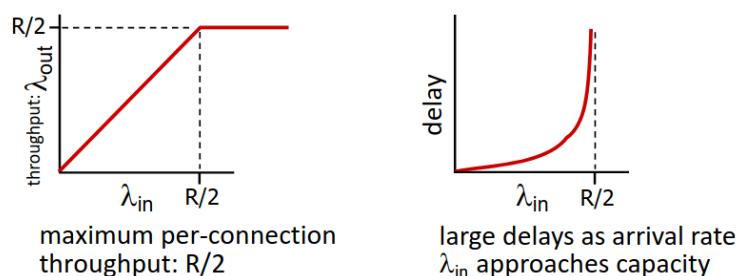
Consideriamo il seguente scenario:

- Vi sono due connessioni aperte passanti per un router con **buffer di dimensione infinita** e il transmission rate dei link è  $R$
- $\lambda_{in}$  è l'**arrival rate del router**, la quantità di dati inviati da un host della prima rete al router
- $\lambda_{out}$  è il **throughput del router**, la quantità di dati inviati dal router ad un host della seconda rete



In tal caso, poiché il buffer è infinito ci troviamo in una situazione in cui non sono necessarie ritrasmissioni dovute alla perdita del pacchetto. Di conseguenza, l'**arrival rate** riesce ad essere equivalente al **throughput**, corrispondente alla quantità di dati in uscita dal router.

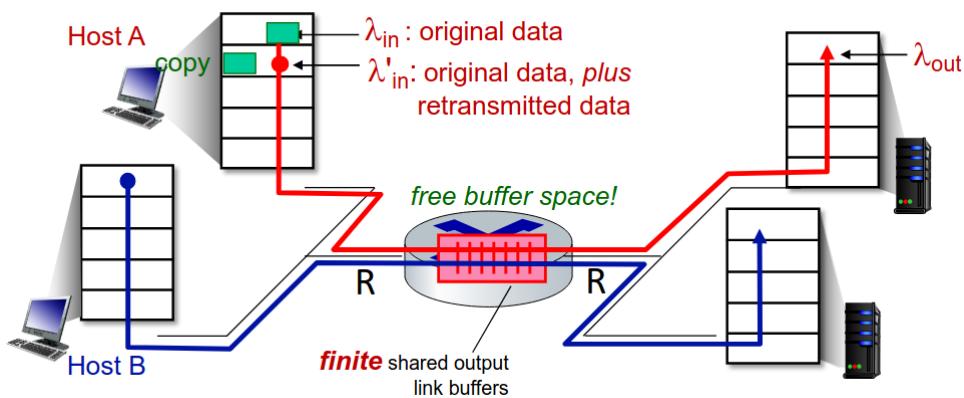
Tuttavia, poiché sono aperte due connessioni passanti per il router, il throughput massimo di ognuna di esse corrisponde a  $\frac{R}{2}$ . Inoltre, anche in tale scenario perfetto, man mano che  $\lambda_{in}$  si avvicina a  $\frac{R}{2}$ , il **delay cresce notevolmente**, per via carico eccessivo sui link stessi della rete.



Nella vita reale, ovviamente, la dimensione dei buffer è **finita**, implicando che alcuni pacchetti possano andar persi, venendo ritrasmessi dal mittente a seguito dello scadere del timeout.

Dato l'arrival rate  $\lambda'_{in}$  dei **dati originali sommati ai dati ritrasmessi**, è necessario sottolineare che:

- Al livello di applicazione, la quantità di dati inviati è equivalente a quella dei dati ricevuti, dunque si ha che  $\lambda_{in} = \lambda_{out}$
- Al livello di trasporto, tuttavia, l'input contiene anche i dati ritrasmessi, implicando che  $\lambda'_{in} \geq \lambda_{in}$



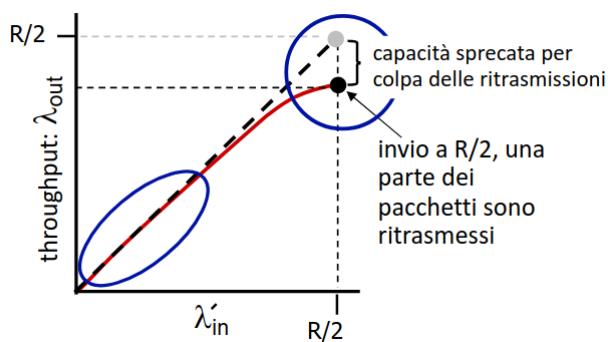
A questo punto, procediamo per **assunzioni** per studiare come la congestione influenzi l'infrastruttura:

- Idealmente, possiamo assumere che il mittente vada ad inviare i dati **solamente** nel caso in cui esso sappia che i buffer dei router abbiano abbastanza spazio per ricevere il pacchetto (assunzione **perfect knowledge**)

In tal caso, ci troveremmo in una situazione identica allo scenario perfetto, poiché la rete sarebbe in grado di gestire il carico senza problemi, inviando i dati da un router all'altro al loro arrivo.

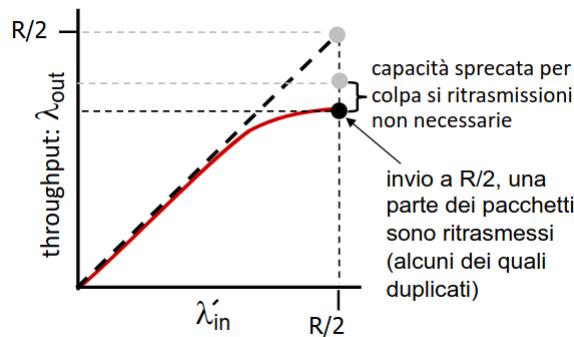
- In uno scenario più realistico, assumiamo che i pacchetti possano essere scartati a seguito di un **overflow** di un buffer e che il mittente sia a conoscenza perfetta di quali pacchetti siano andati persi, ritrasmettendoli (**perfect knowledge parziale**).

In tal caso, parte della capacità dei link verrebbe sprecata per via delle ritrasmissioni, **diminuendo il throughput**

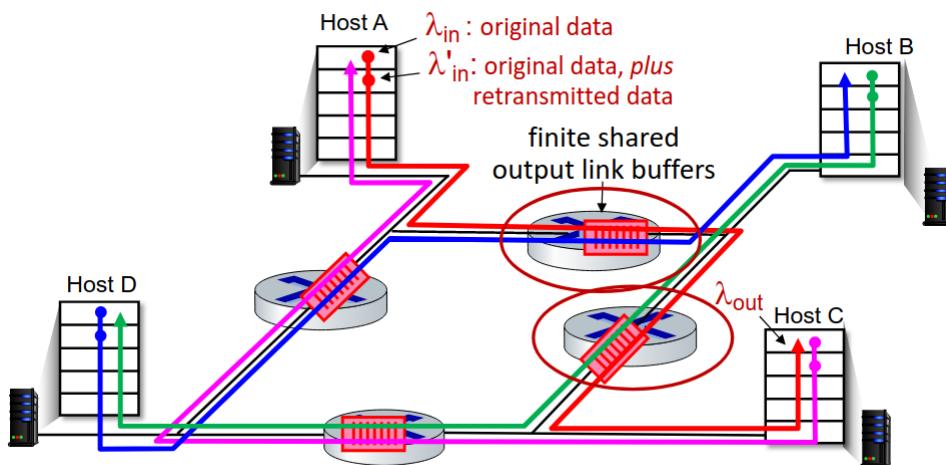


- In uno scenario reale, oltre alla perdita di pacchetti dovuta ad un overflow dei buffer, il **timer** del mittente può scadere prematuramente, inviando due copie dello stesso pacchetto ritrasmesso (**duplicati non necessari**)

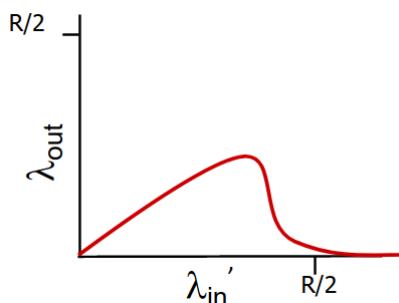
In tal caso, ulteriore parte della capacità dei link verrebbe sprecata per via delle ritrasmissioni non necessarie, **diminuendo il throughput ulteriormente**



Consideriamo invece ora una rete più realistica in cui tutti e quattro i dispositivi sono mittenti e vi siano più router colleganti le loro reti (rete multi-hop).



All'aumentare dei valori  $\lambda_{in}^{red}$  e  $\lambda_{in}^{red'}$  del collegamento rosso mostrato in figura, **tutti i pacchetti del collegamento blu vengono scartati**, poiché il buffer del router viene riempito dai pacchetti del collegamento rosso rinviati, portando il valore  $\lambda_{out}^{blue}$  a tendere a 0, diminuendo il throughput generale della rete



Possiamo quindi riassumere il comportamento della rete nei seguenti punti:

- Il throughput non può mai superare la capacità
- Il ritardo aumenta con l'avvicinarsi alla capacità
- La perdita e ritrasmissione riduce il throughput effettivo
- I duplicati non necessari riducono ulteriormente il throughput effettivo
- Viene sprecata capacità di trasmissione e buffering upstream per i pacchetti persi downstream

Infine, utilizziamo tali punti per definire i **costi della congestione**:

- È necessario un **lavoro** (numero di ritrasmissioni) **maggiori** per un dato throughput durante la congestione
- Il collegamento trasporta **più copie** dello stesso pacchetto **non necessarie**, riducendo il throughput massimo ottenibile
- Quando un pacchetto viene scartato, tutta la capacità di trasmissione upstream e la porzione di buffer utilizzata per esso viene **sprecata**

### 3.5.2 Controllo della congestione nel TCP

Per tentare di gestire la congestione, vengono principalmente utilizzati due approcci:

- **Controllo della congestione end-to-end**, dove non viene ricevuto alcun feedback esplicito dalla rete e la congestione viene **dedotta** dalle perdite e ritardi osservati dal mittente e il destinatario.

Tale approccio è adottato dal protocollo TCP

- **Controllo della congestione assistito dalla rete**, dove i router forniscono un feedback **diretto** agli host di invio/ricezione con flussi che passano attraverso router congestionati, indicando, in alcuni casi, direttamente il livello di congestione o la velocità di invio impostata

#### Definition 30. Algoritmo AIMD

L'algoritmo **AIMD** (**Additive Increase, Multiplicative Decrease**) è un algoritmo utilizzato da alcune versioni del protocollo TCP per **prevenire la congestione**, dove i mittenti possono **aumentare la velocità di invio** fino a quando si verifica una **perdita di pacchetti**, per poi diminuirla:

- **Additive Increase**: il rate viene aumentato di 1 MSS (Maximum Segment Size) ad ogni RTT fino a quando una perdita non viene osservata
- **Multiplicative Decrease**: ad ogni perdita osservata, il rate di invio viene dimezzato



### Definition 31. Congestion avoidance e Congestion window

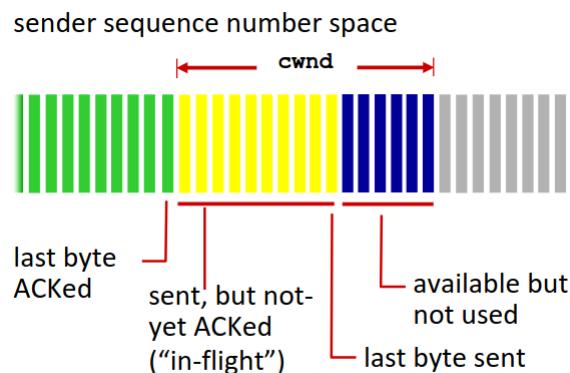
Approssimativamente, il protocollo TCP utilizza la seguente procedura di **prevenzione della congestione (congestion avoidance)**:

- Viene utilizzato un valore **cwnd** (**congestion window**), corrispondente alla quantità di byte inviata ad ogni RTT, da cui ne segue che

$$\text{Rate di invio} \approx \frac{\text{cwnd}}{\text{RTT}} \text{ B/s}$$

- Il mittente limita la trasmissione a  $\text{LastByteSent} - \text{LastByteAcked} \leq \text{cwnd}$
- Il valore cwnd varia dinamicamente reagendo alla congestione osservata. In particolare, utilizzando l'**Additive Increase** ad ogni ACK ricevuto si ha che:

$$\text{cwnd} \approx \text{prev\_cwnd} + \left( \text{MSS} \cdot \frac{\text{MSS}}{\text{prev\_cwnd}} \right)$$



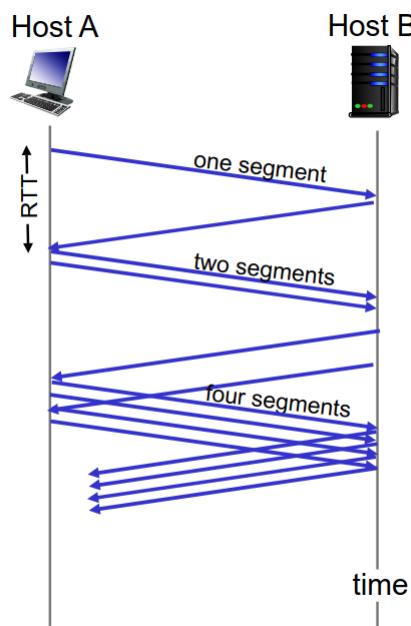
**Definition 32. Fast recovery**

Il **fast recovery** è una procedura utilizzata da alcune versioni del protocollo TCP per **prevenire la congestione**, dove ad ogni perdita rilevata a seguito di un **triplo ACK** duplicato viene **dimezzato il rate di invio** (ottenuto circa dimezzando il valore cwnd)

**Definition 33. Slow start**

Lo **slow start** è una procedura utilizzata da alcune versioni del protocollo TCP **prevenire la congestione**, dove:

- Il valore cwnd viene **impostato ad 1 MSS** all'inizio della connessione o a seguito di un **timeout**
- Successivamente, il valore di cwnd viene **raddoppiato ad ogni RTT**, fino al rilevamento della prima perdita di pacchetto (**incremento esponenziale**)



*Nota: l'immagine superiore è un'approssimazione del vero comportamento, poiché raddoppiare cwnd non implica che venga raddoppiata la quantità di segmenti inviati, bensì che raddoppi la quantità di segmenti di dimensione massima inviati*

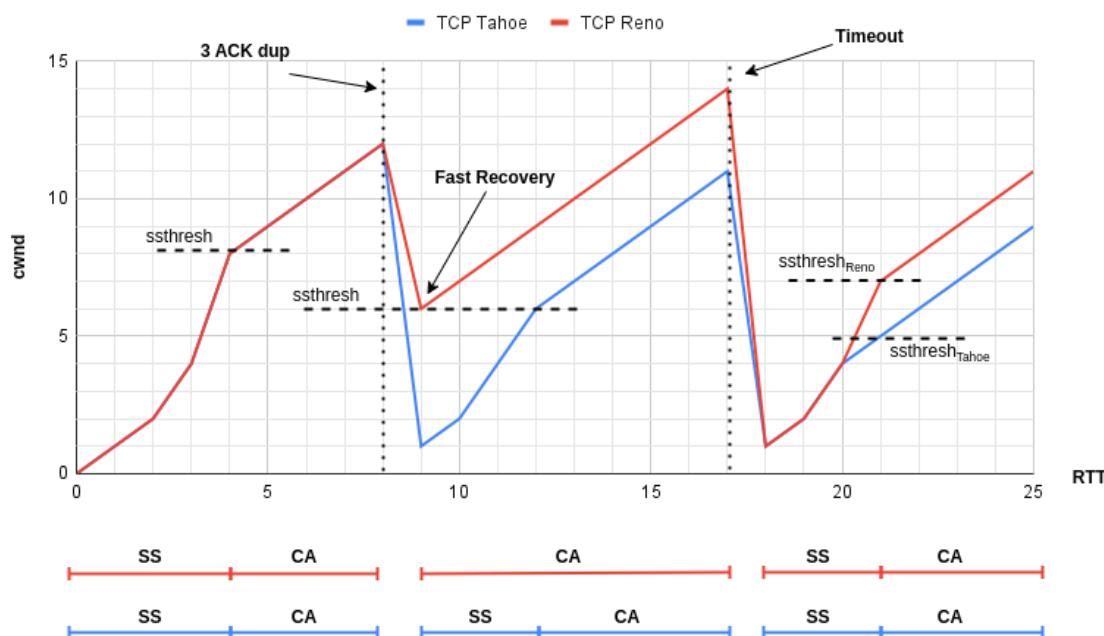
Tali meccanismi di prevenzione della congestione di rete vengono utilizzati principalmente da due versioni del protocollo TCP:

- **TCP Tahoe**: composto da un'algoritmo di **congestion avoidance** (tramite l'**Additive Increase**), l'algoritmo **slow start** e il **fast retransmit**
- **TCP Reno**: analogo al TCP Tahoe, ma con l'utilizzo aggiuntivo del **fast recovery** (FSM riportata in seguito)



In particolare, per effettuare il passaggio tra **slow start** e **congestion avoidance**, viene utilizzato un valore **ssthresh** (slow start threshold).

- A seguito del rilevamento di una perdita di pacchetto, il valore **ssthresh** viene impostato a  $\frac{cwnd}{2}$  (con il valore di **cwnd** precedente alla perdita). Se al prossimo RTT si verificasse che  $cwnd \geq ssthresh$ , viene posto  $cwnd = ssthresh$  e si passa dallo slow start al congestion avoidance
- Nel caso particolare del TCP Reno, se si verifica un triplo ACK duplicato, il valore **cwnd** viene dimezzato dal fast recovery, dunque si ha direttamente  $cwnd = ssthresh$



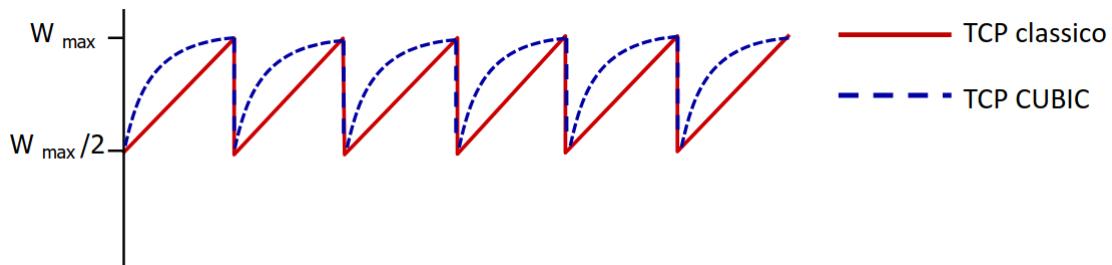
### Definition 34. TCP CUBIC

Il **TCP CUBIC** è una versione di TCP utilizzante l'algoritmo **CUBIC** per **prevenire la congestione**, il quale è definito dalla seguente logica:

- Viene utilizzato un valore  $W$ , corrispondente alla **velocità di invio** (o alla quantità di dati inviati dal mittente, ossia  $cwnd$ ). Ad ogni perdita rilevata, viene **dimezzato** tale valore.
- Il limite superiore  $W_{max}$  corrisponde alla **velocità di invio** nel momento in cui è stata rilevata una **perdita di pacchetto** (viene assunto che a seguito della perdita lo stato di congestione della rete non sia variato di molto)
- Viene utilizzato un valore  $K$  corrispondente al **momento di tempo stimato** in cui il valore  $W$  raggiungerà il limite superiore  $W_{max}$  (la modalità di stima viene definita dallo standard RFC 8312)
- Il valore  $W$  viene **incrementato in funzione del cubo della distanza tra il tempo corrente e  $K$** .

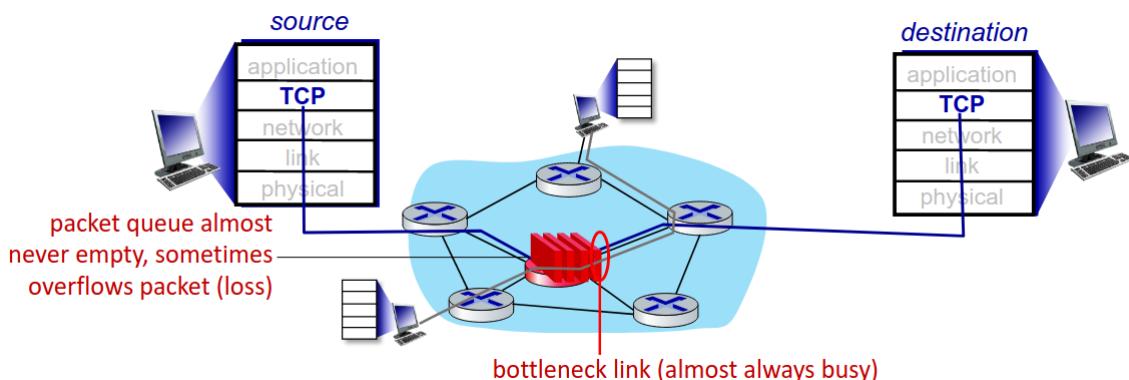
Di conseguenza, il valore  $W$  **crescerà molto rapidamente** quando il tempo corrente è lontano dal valore  $K$ , mentre **crescerà lentamente** al suo avvicinarsi.

Supponendo, ad esempio, che il valore di  $W_{max}$  rimanga sempre lo stesso nel tempo, il throughput del TCP CUBIC rispetto a quello standard risulta più elevato:

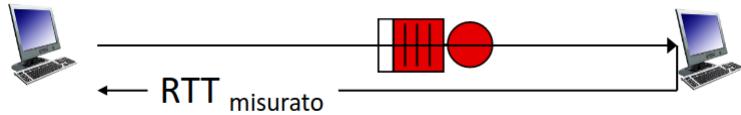


In particolare, essendo predefinito sul sistema operativo Linux, il TCP CUBIC è la versione del protocollo TCP più diffusa nei web server.

Una volta aver visto algoritmi e tecniche per prevenire la congestione, possiamo concentrarci sul link di uscita del stesso in cui si verifica la perdita (**bottleneck link**)



In presenza di un bottleneck link, **aumentando il rate di invio** non aumenterà il throughput per via del bottleneck link ma **aumenterà il RTT misurato**.



Una soluzione ottimale, dunque, è quella di mantenere il percorso end-to-end **quasi pieno**, ma senza superare la soglia stabilità, utilizzando un approccio **delay-based**:

- Il valore  $RTT_{min}$  è il RTT minimo osservato dal mittente, corrispondente quindi al RTT osservato quando il percorso **non è congestionato**
- Approssimativamente, il **throughput misurato** ad ogni RTT corrisponde a:

$$\text{Throughput}_{\text{misurato}} = \frac{\text{Byte}_{\text{RTT}}}{\text{RTT}_{\text{misurato}}}$$

dove  $\text{Byte}_{\text{RTT}}$  è il numero di byte inviati nell'ultimo RTT, mentre il **throughput non congestionato** è pari a:

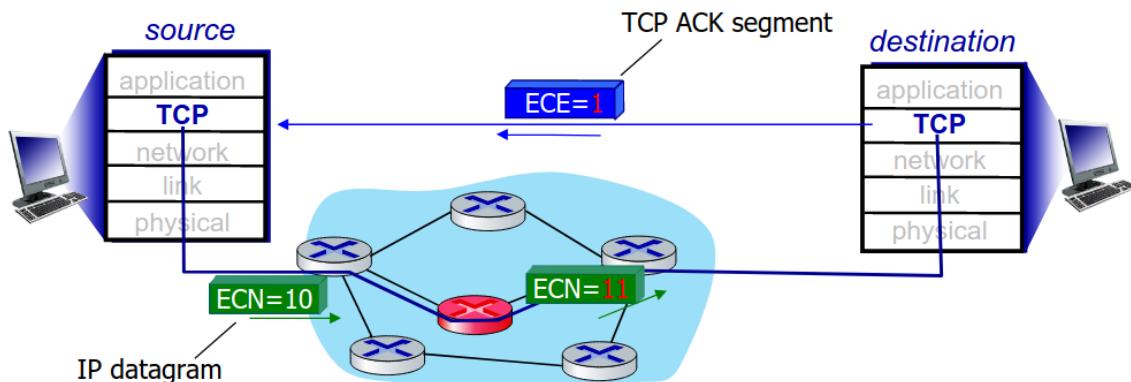
$$\text{Throughput}_{\text{non cong}} = \frac{\text{cwnd}}{\text{RTT}_{\text{min}}}$$

- Se il valore del throughput misurato è **molto vicino** a quello non congestionato, il valore di **cwnd** viene **incrementato** in modo lineare (dunque +1 MSS ad ogni RTT), mentre se è **molto inferiore** viene **decrementato** in modo lineare

Tramite tale approccio, alcune versioni di TCP (es: protocollo BBR) riescono ad indurre un controllo della congestione senza forzare delle perdite di pacchetto, massimizzando il throughput ma mantenendo basso il ritardo.

Altre versioni di TCP (es: TCP ECN), invece, implementano anche la seconda modalità di controllo della congestione, ossia il **controllo della congestione assistito dalla rete**, dove:

- Due bit dell'**header del livello di rete** vengono contrassegnati dal **router** per indicare lo stato della congestione
- Una volta raggiunto il destinatario, quest'ultimo imposterà il bit ECE sul segmento ACK per notificare al mittente lo **stato della congestione**



## 3.6 Equità nei protocolli di trasporto

### Proposition 2. Equità nelle connessioni

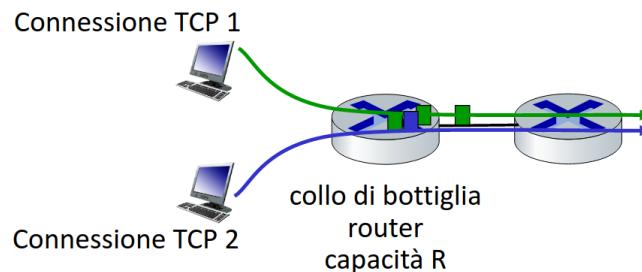
Affinché un protocollo di trasporto sia definibile **equo**, se  $K$  sessioni di tale protocollo condividono lo stesso **bottleneck link** con larghezza di banda  $R$ , ciascuna delle  $K$  sessioni deve avere una velocità media pari a  $\frac{R}{K}$

Notiamo con facilità che il **protocollo UDP** sia un protocollo **non equo** per via dell'assenza di un controllo della congestione e di limiti sulla banda utilizzabile.

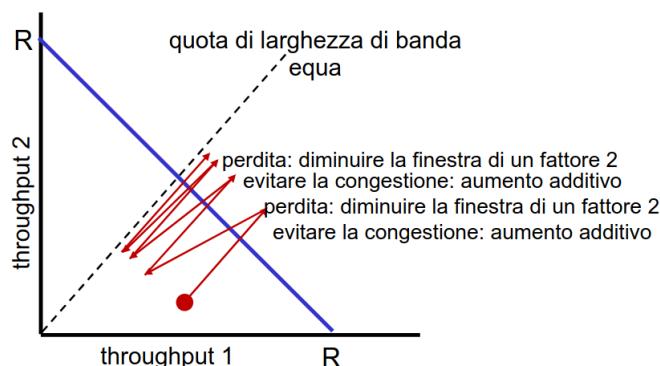
Per tale motivo, spesso applicazioni multimediali utilizzanti il protocollo UDP (es: i servizi streaming) "rubano" velocità di connessione ad altre applicazioni.

Per quanto riguarda il protocollo TCP, invece, è necessario effettuare uno studio:

- Consideriamo il seguente scenario con due sessioni TCP con algoritmo AIMD concorrenti sullo stesso bottleneck link



- Tramite l'**additive increase** viene generata una pendenza pari ad 1
- Tramite il **multiplicative decrease** viene ridotto proporzionalmente il throughput



Sotto **ipotesi idealizzate**, dunque, il **protocollo TCP** risulta essere **equo** (es: stesso RTT, numero fisso di sessioni, ...).

Tuttavia, molte applicazioni moderne utilizzano **più di una connessione TCP parallela** tra due host (es: un web browser). Di conseguenza, anche se la larghezza di banda fosse equamente distribuita tra tutte le connessioni possibili tra i due host, tale applicazione otterrebbe comunque una quantità di banda superiore alle altre applicazioni.

# Capitolo 4

## Livello di Rete

### 4.1 Panoramica del livello di rete

Come già accennato, a differenza del livello di trasporto, il **livello di rete** si occupa della comunicazione logica tra i dispositivi stessi tramite il trasporto di segmenti dall'host di invio a quello di ricezione.

In particolare, ogni **router** della rete si occupa di esaminare i campi header di tutti i **datagrammi** IP che lo attraversano, spostandoli dalle porte di ingresso alle porte di uscita per trasferirli lungo il percorso end-to-end

#### Definition 35. Forwarding e Routing

All'interno del livello di rete distinguiamo **due funzionalità fondamentali**:

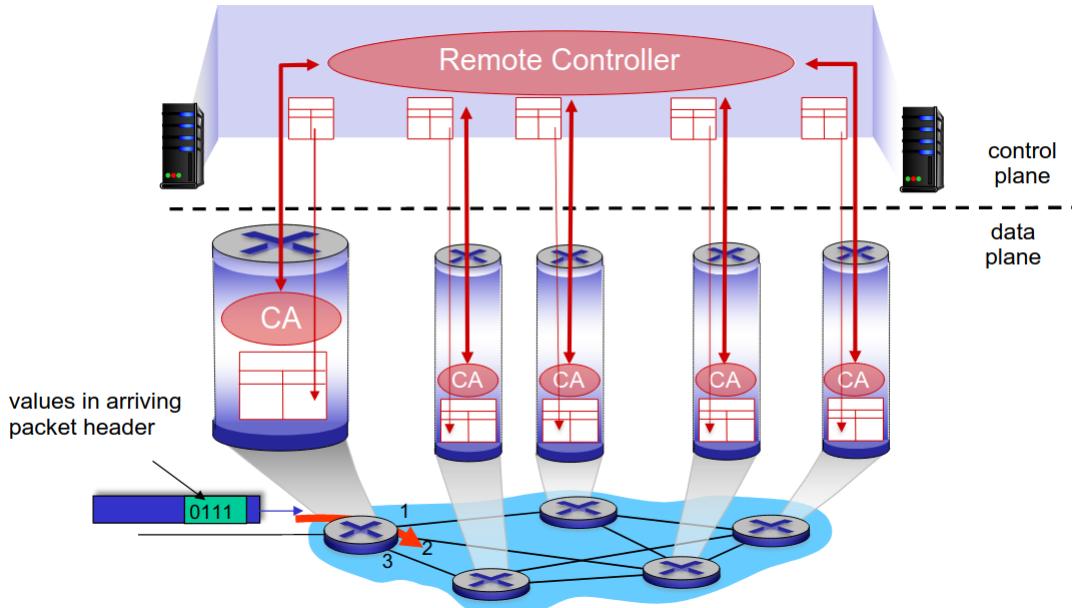
- **Forwarding (inoltro)**, ossia il trasferimento dei pacchetti dal link di ingresso di un router al link appropriato di uscita tramite la **gestione delle porte**
- **Routing (instradamento)**, ossia la determinazione (solitamente tramite **algoritmi** di routing) del percorso seguito dai pacchetti dalla sorgente alla destinazione

Per poter realizzare correttamente il servizio di trasferimento dei datagrammi, il livello di rete deve essere in grado di realizzare entrambe tali funzioni fondamentali. Distinguiamo quindi il servizio di rete in **due strati**:

- **Data plane**, dove viene determinato come il datagramma in arrivo sulla porta di ingresso di un router venga inoltrato alla porta di uscita del router (**lavoro in locale**)
- **Control plane**, dove viene determinato come il datagramma venga instradato tra i router lungo il percorso end-to-end dall'host di origine all'host di destinazione (**logica a livello di rete**)



Oltre agli **algoritmi di routing** implementati all'interno dei singoli router, per il control plane può essere utilizzato anche il **Software-Defined Networking (SDN)**, dove un server remoto, detto **controller remoto**, calcola preventivamente tutte le **forwarding table** dei router, ossia le tabelle contenenti le regole di inoltro, i quali poi si connetteranno con il controller stesso per ottenere ed installare la propria tabella



Nella gestione dei "canali" di trasporto dei datagrammi dal mittente al destinatario viene utilizzato un modello **best effort**:

- Non vi è garanzia sull'effettiva **consegna** del datagramma a destinazione
- Non vi è garanzia sulle **tempistiche** o sull'**ordine** di consegna dei datagrammi
- Non vi è garanzia sulla **larghezza di banda** disponibile per il flusso end-to-end

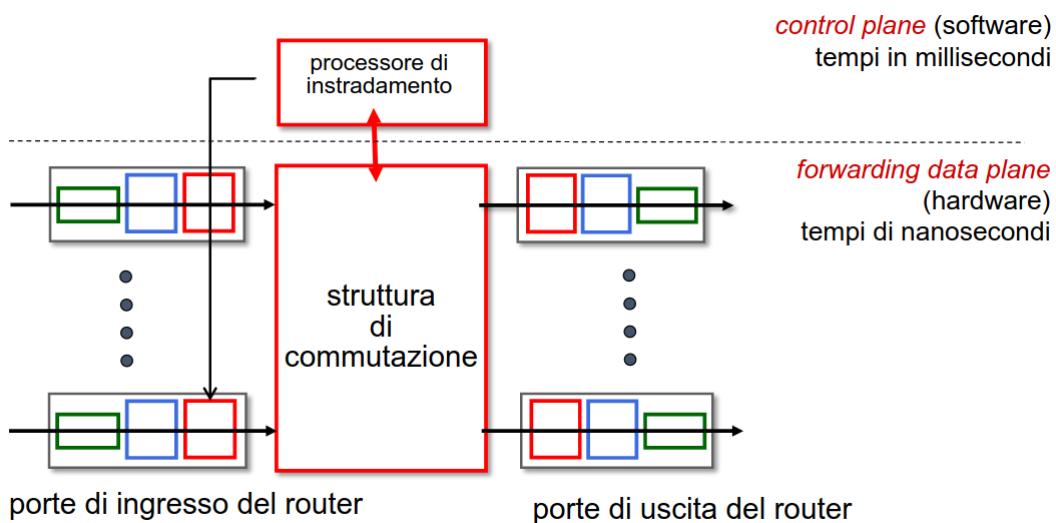
Nonostante i difetti, il modello best effort ha raggiunto un ottimo **successo**:

- La sua **semplicità** ha permesso ad Internet di essere ampiamente adottato ed implementato
- Una **larghezza di banda sufficiente** consente alle prestazioni delle applicazioni in tempo reale di essere per lo più sufficientemente ottime
- I **servizi distribuiti replicati a livello di applicazione** che si connettono vicino alle reti dei clienti (data center, reti di distribuzione di contenuti, ...) consentono di fornire servizi da più posizioni

## 4.2 Architettura e funzionalità dei router

L'architettura interna di un router può essere riassunta in:

- Una serie di **porte di ingresso e di uscita** connesse a dei link
- Una **struttura di commutazione (switching fabric)** interposta tra le porte di entrata ed uscita
- Un **processore di instradamento**, il quale si occupa di effettuare i calcoli necessari per il routing



Le **porte di ingresso e di uscita** sono dotate di:

- Una propria **memoria** contenente le **forwarding table**
- Una **terminazione di linea** (ossia il termine/inizio del link ad esse associate)
- Un'interfaccia con il **livello di collegamento** tramite cui viene gestito il protocollo utilizzato (es: Ethernet)
- Una **coda di ingresso/uscita** in cui vengono inseriti temporaneamente i pacchetti appena vengono ricevuti o prima di essere spediti.



In particolare, all'interno della coda della porta di ingresso viene effettuata una **commutazione decentralizzata**, dove per ogni datagramma al suo interno viene cercata la porta di uscita utilizzando i valori del campo di intestazione e della forwarding table nella memoria della porta di input stessa (**match plus action**).

Per realizzare tale commutazione, vengono utilizzati il **destination-based forwarding**, dove l'inoltro è basato solo sull'indirizzo IP di destinazione presente negli header, e il **generalized forwarding**, dove l'inoltro è basato su un insieme di valori dell'header dei datagrammi.

#### Definition 36. Longest prefix matching

Il **longest prefix matching** è un algoritmo di forwarding basato sul destination-based forwarding: durante la ricerca della voce della forwarding table per un indirizzo di destinazione, viene selezionata l'entrata il cui indirizzo ha il **prefisso più lungo corrispondente** a quello dell'indirizzo di destinazione

**Esempio:**

- Consideriamo la seguente forwarding table, dove gli asterischi, detti **wildcard**, indicano che un qualsiasi valore tra 0 o 1 possa occupare tale posizione (**intervalli di indirizzi IP**)

Intervallo di indirizzi di destinazione	Porta di uscita
11001000 00010111 00010*** *****	0
11001000 00010111 00011000 *****	1
11001000 00010111 00011*** *****	2
altrimenti	3

- Utilizzando il longest prefix matching, il datagramma contenente l'indirizzo di destinazione 11001000 00010111 00010110 10100001 verrà inoltrato alla porta di uscita 0, poiché l'intervallo 11001000 00010111 00010\*\*\* \*\*\*\*\* possiede il prefisso corrispondente più lungo tra le tutte le entrate

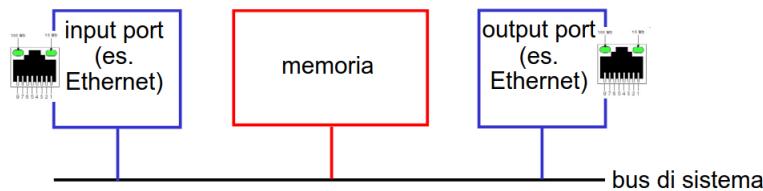
- Analogamente, il datagramma contenente l'indirizzo di destinazione `11001000 00010111 00011000 10101010` verrà inoltrato alla porta di uscita 1, poiché l'intervallo `11001000 00010111 00011000 *****` possiede il prefisso corrispondente più lungo tra le tutte le entrate (24 cifre rispetto alle 21 della porta 2)

Per quanto riguarda gli **switching fabric**, essi si occupano di effettuare il vero e proprio inoltro, trasferendo ogni pacchetto dai link di input al link di output appropriato.

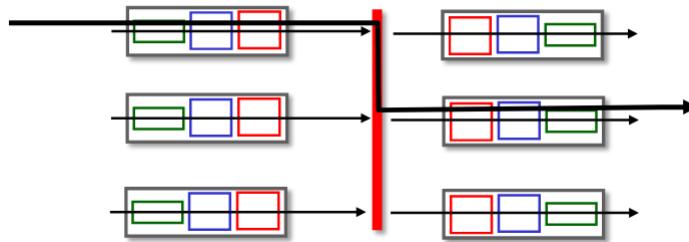
In particolare, lo **switching rate** dello switching fabric corrisponde alla velocità con cui i pacchetti possono essere trasferiti dagli ingressi alle porte (idealmente pari a  $N \cdot R$ , dove  $N$  è il numero di porte di ingresso/uscita ed  $R$  è il transmission rate dei link connessi alla porta, supponendo che esso sia uguale per tutti i link)

Le principali tre modalità di implementazione degli switching fabric prevedono:

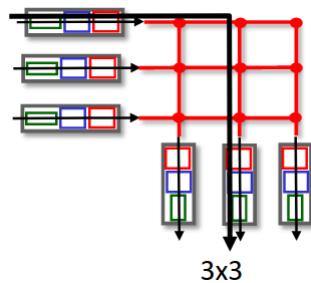
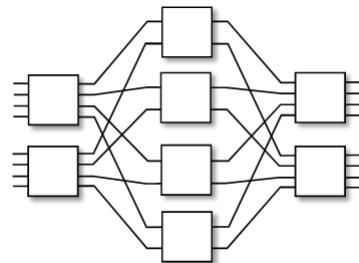
- Commutazione tramite memoria**, dove la commutazione è sotto diretto controllo della CPU, copiando i pacchetti in arrivo nella **memoria del sistema**, per poi inviarli sulle porte di uscita, implicando che lo switching rate sia limitato dalla larghezza di banda della memoria.



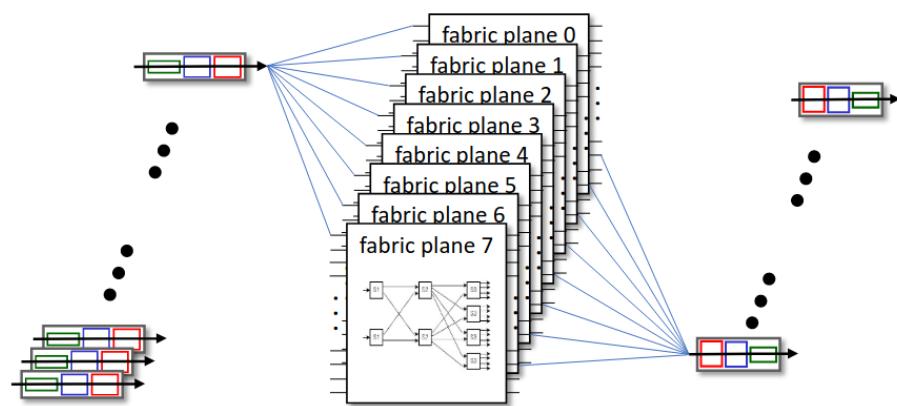
- Commutazione tramite bus**, dove i datagrammi vengono trasferiti dalla memoria della porta di ingresso alla memoria della porta di uscita tramite un **singolo bus** condiviso, implicando che lo switching rate sia limitato dalla larghezza di banda del bus e che vi sia una contesa tra le porte per l'utilizzo del bus



- Commutazione tramite reti di interconnessione**, dove vengono utilizzate reti di interconnessione (es: Crossbar, reti Clos) inizialmente sviluppate per connettere processori tra di loro. In particolare, vengono utilizzati **interruttori multistadio**, ossia interruttori  $N \times N$  formati da più stadi di interruttori più piccoli, e il **parallelismo**, frammentando i diagrammi in celle di lunghezza fissa all'ingresso per poi commutarle attraverso la rete di interconnessione e riassemblarle una volta raggiunta la porta di uscita

**Interruttore  $3 \times 3$** **Interruttore multistadio  $8 \times 8$   
formato interruttori più piccoli**

Inoltre, l'uso di reti di interconnessione permette un maggiore **scaling** utilizzando più "piani" di commutazione in parallelo



### 4.2.1 Accodamento nelle porte

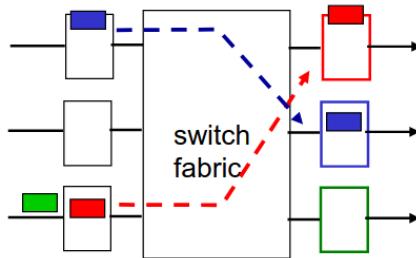
Nel caso in cui lo switch fabric sia più lento delle porte di input combinate, dunque se lo switching rate è minore del transmission rate dei link di entrata, potrebbe verificarsi dell'**accodamento** nei buffer di coda delle **porte di input**, generando un **queueing delay** e una possibile **perdita** dovuta all'overflow del buffer.

In particolare, possono verificarsi due situazioni sfavorevoli che possano generare accodamento nella porta di input:

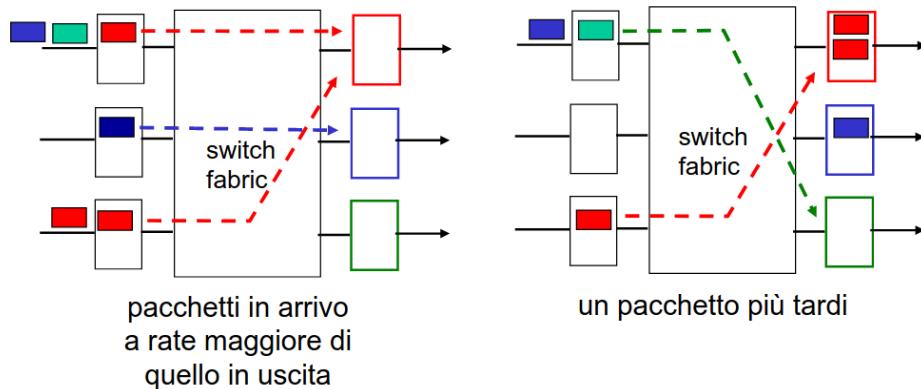
- **Contesa della porta di uscita:** in ogni istante può essere commutato un solo pacchetto verso una determinata porta di uscita, impedendo agli altri pacchetti di proseguire, bloccando di conseguenza la loro coda



- **Blocco HOL (Head-of-Line):** all'interno di ogni coda il datagramma nella parte anteriore della coda impedisce agli altri datagrammi in coda di poter proseguire



Analogamente, può verificarsi dell'**accodamento** all'interno nei buffer di coda delle **porte di output** nel caso in cui lo switch rate superi il transmission rate del link di uscita, generando ritardo e perdite di pacchetti.



Per gestire tali accodamenti, dunque, è necessario gestire minuziosamente i **buffer**. In particolare, lo standard più recente prevede un buffer di dimensione pari a:

$$\text{Buffer} = \frac{\text{RTT} \cdot C}{\sqrt{N}}$$

dove  $N$  è il numero di flussi e  $C$  è la capacità dei collegamenti.

Tuttavia, un buffering eccessivo può **aumentare i ritardi** (in particolare all'interno dei router domestici):

- Con RTT lunghi si ottengono scarse prestazioni per le app in tempo reale ed una risposta TCP troppo lenta
- I buffer dovrebbero solo assorbire le fluttuazioni statistiche di occupazione in mancanza di congestione, senza creare un collo di bottiglia troppo pieno

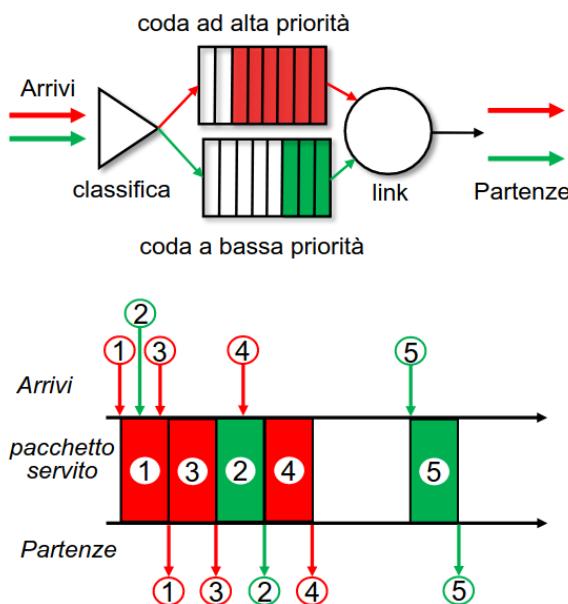
Di conseguenza, è necessario utilizzare un **protocollo di scarto** per scegliere quale pacchetti inserire nella coda e quali scartare quando il buffer è pieno. In particolare, vengono utilizzati principalmente il **tail drop**, dove viene scartato l'ultimo pacchetto in arrivo, e il **priority drop**, dove i pacchetti vengono scartati selettivamente in base alla priorità.

### 4.2.2 Scheduling dei pacchetti

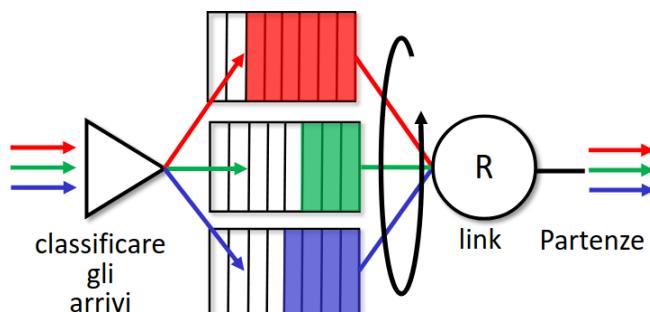
Per decidere quale sia il prossimo pacchetto da inviare, le porte di uscita vengono gestite tramite **politiche di scheduling**, cercando di ottenere le **migliori prestazioni** possibili mantenendo una **neutralità della rete**, ossia la modalità con cui un ISP dovrebbe allocare le proprie risorse.

In particolare, vengono principalmente utilizzate quattro politiche:

- **First come, First served (FCFS)**, dove i pacchetti vengono trasmessi in ordine di arrivo alla porta di uscita
- **Priority scheduling**, dove il traffico in arrivo viene classificato ed inserito in una classe di coda in base alla sua priorità, inviando il pacchetto della coda con la priorità più alta contenente pacchetti nel buffer (FCFS all'interno delle classi di priorità). La priorità viene determinata utilizzando un insieme di campi presenti nell'intestazione del pacchetto.



- **Round Robin (RR)**, dove il traffico in arrivo viene sempre classificato in code di classe utilizzando più code e l'invio dei pacchetti viene effettuato ciclicamente: viene ciclicamente eseguita una scansione delle code di classe, inviando a turno un pacchetto completo da ciascuna classe (se disponibile)

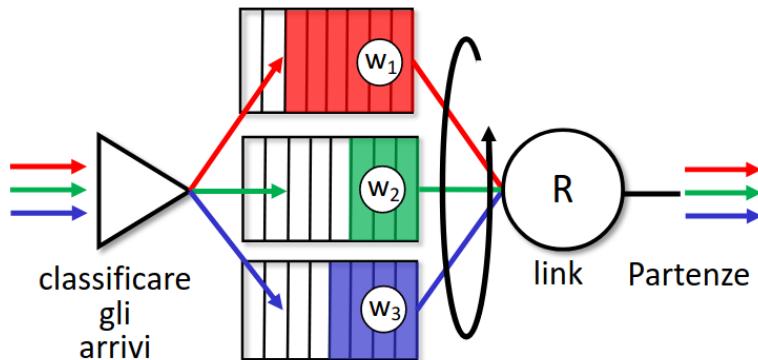


- **Weighted fair queueing (WFQ)**, dove il traffico in arrivo viene sempre classificato in code di classe utilizzando più code e l'invio dei pacchetti viene effettuato in base al peso delle classi: ogni classe  $i$  ha un peso  $w_i$  e riceve una quantità ponderata di servizio ad ogni ciclo, equivalente a

$$\frac{w_i}{\sum_{j=1}^k w_j}$$

dove  $k$  è il numero di classi.

In tal modo, si ottiene una gestione pari ad un Round Robin generalizzato e viene garantita una larghezza di banda minima per ogni classe di traffico.



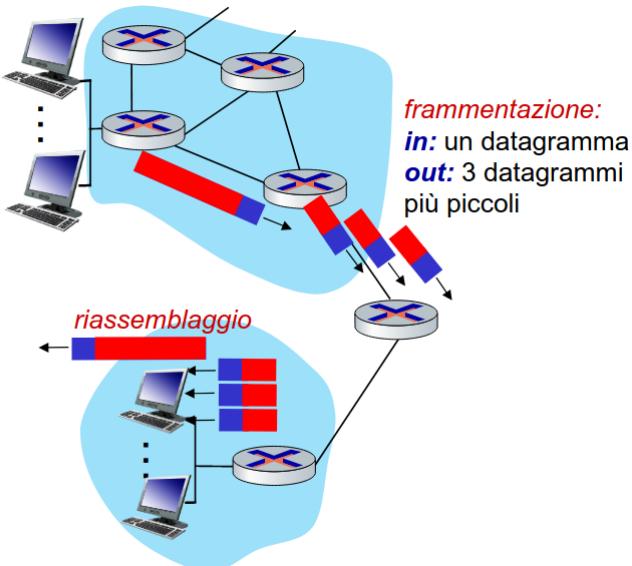
Inoltre, con la terminologia "neutralità della rete" vengono anche contrassegnati i **principi sociali/economici** e i **provvedimenti legali** atti a stabilire regole e politiche di gestione. In particolare, tale neutralità viene basata su tre principi:

- **No blocking**: non devono essere bloccati contenuti, applicazioni, servizi o dispositivi leciti e non dannosi soggetti ad una ragionevole gestione della rete
- **No throttling**: non si deve compromettere o degradare il traffico Internet legittimo sulla base di contenuti, applicazioni o servizi Internet o l'uso di un dispositivo non dannoso, soggetto a una ragionevole gestione della rete
- **No payed priority**: non deve essere prevista la prioritizzazione retribuita

### 4.2.3 Frammentazione dei datagrammi

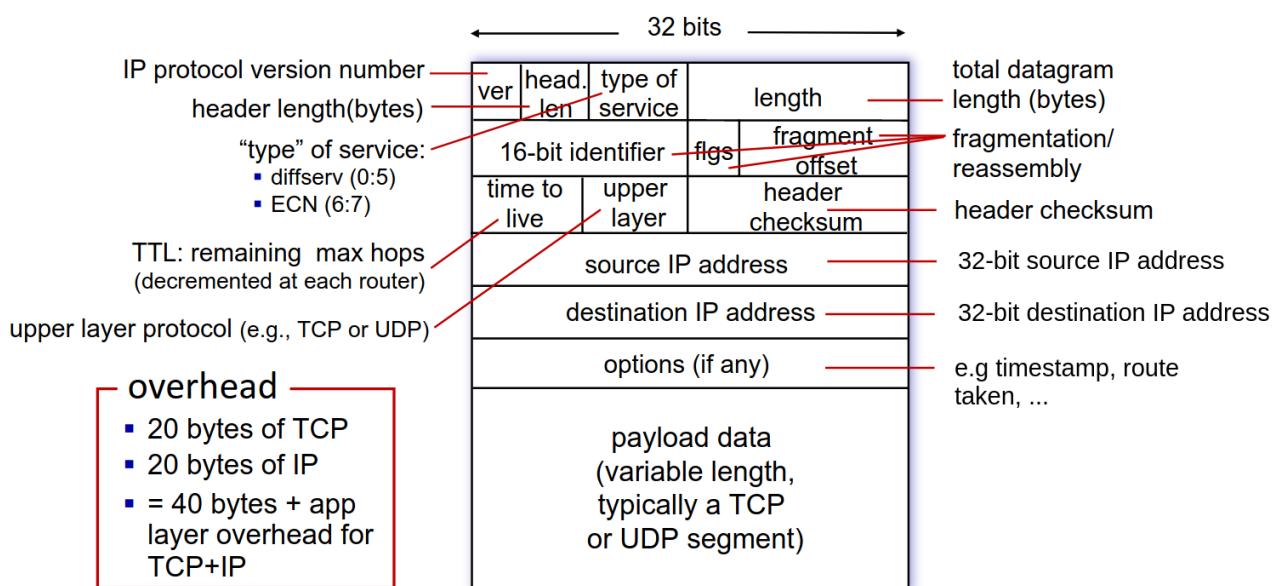
Per gestire meglio la **congestione**, i collegamenti di rete possiedono **Maximum Transmission Unit (MTU)**, ossia la dimensione massima comunicabile in una singola trasmissione del livello di rete all'interno del link stesso (dunque variabile a seconda del tipo di collegamento).

Di conseguenza, ogni datagramma di grandi dimensioni viene **frammentato** lungo la sua trasmissione a seconda dei link attraverso cui avviene il forwarding, venendo **ri-assemblato** solamente una volta raggiunta la destinazione, richiedendo quindi un campo all'interno dell'header per mantenere traccia dell'**ordine**.



### 4.3 Protocollo IP

Principalmente, all'interno del livello di rete viene utilizzato un solo protocollo standard, ossia il **protocollo IP (Internet Protocol)**.



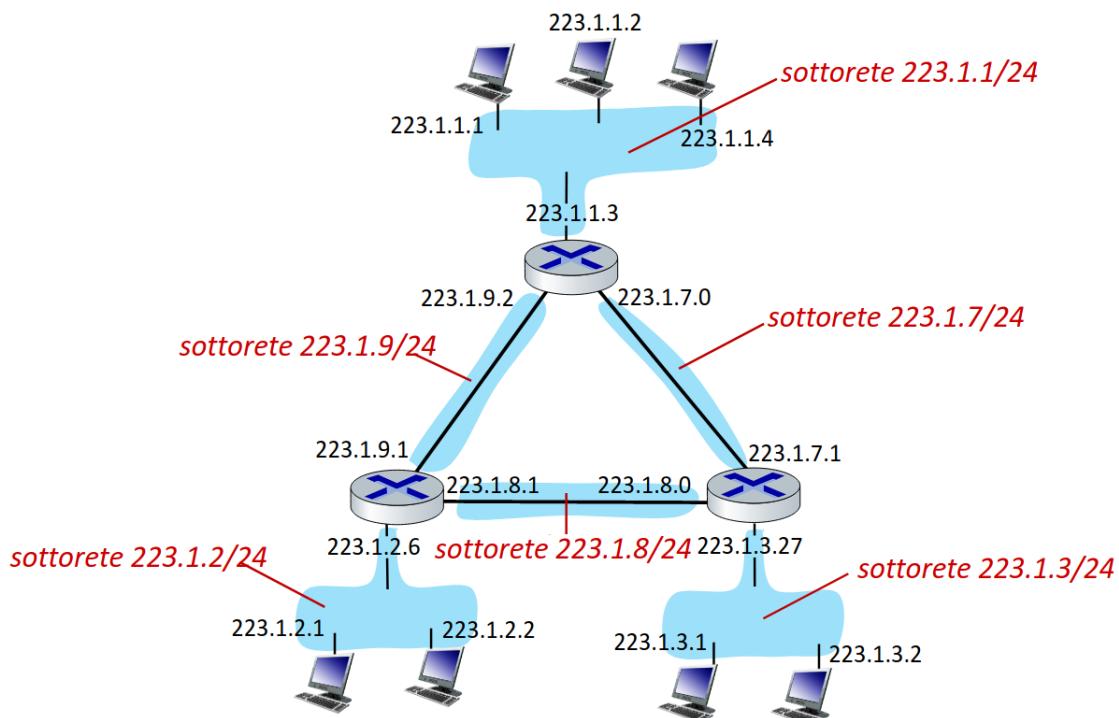
Il protocollo IP è basato su tre costrutti fondamentali:

- **Interfaccia**, ossia una **connessione** tra host e router associata ad un **collegamento fisico**. Solitamente, i router possiedono più interfacce, mentre un host possiede una o due interfacce (es: interfaccia Ethernet cablata ed interfaccia wireless Wi-Fi). Vengono gestite e determinate dal livello di collegamento.

- **Sottorete**, ossia un insieme di interfacce di dispositivi che possono raggiungersi fisicamente l'un l'altro senza passare attraverso un router intermedio (dunque tramite uno switch o altri mezzi).
- **Indirizzo IP**, ossia un identificatore a 32 bit associato ad un'interfaccia. Per facilitare la gestione agli umani, viene interpretato con una **notazione decimale puntata**, dove l'indirizzo viene suddiviso in quattro ottetti ed ogni ottetto viene interpretato come un valore decimale  
(es: l'indirizzo 11011111 00000001 00000001 00000001 viene interpretato come 223.1.1.1)

La struttura degli indirizzi IP viene definita dal **Classless Inter Domain Routing (CIDR, letto "cider")**:

- Ogni indirizzo possiede una **parte di sottorete**, condivisa tra i dispositivi della stessa sottorete e costituita da un determinato numero di bit più significativi (dunque più a sinistra). Gli  $n$  bit utilizzati per la parte di sottorete vengono definiti all'interno della **subnet mask**, i cui primi  $n$  bit più significativi sono posti ad 1 e i restanti posti a 0 (formata da 32 bit totali)
- Ogni indirizzo possiede una **parte di host**, identificante l'host stesso all'interno della sottorete e costituita dai bit meno significativi rimanenti
- Il formato degli indirizzi "ciderized" segue la struttura  $a.b.c.d/x$ , dove  $a.b.c.d$  è l'indirizzo IP e  $x$  è la quantità di bit posti ad 1 della subset mask  
(es: l'indirizzo 200.23.16.0/23 viene interpretato come 11001000 00010111 00010000 00000000, dove i primi 23 bit rappresentano la sottorete)



L'utilizzo della **subnet mask** risulta essere estremamente comodo per ottenere in modo efficiente informazioni sul **blocco di indirizzi** definito dalla sottorete:

- Il **numero di indirizzi del blocco** corrisponde al bitwise NOT della maschera sommato ad 1

$$\text{Num. indirizzi} = \text{NOT(mask)} + 1$$

- Il **primo indirizzo del blocco** corrisponde al bitwise AND tra un indirizzo qualsiasi del blocco e la maschera

$$\text{Primo indirizzo} = (\text{qualsiasi indirizzo del blocco}) \text{ AND } (\text{mask})$$

(solitamente viene utilizzato per indicare direttamente la sottorete)

- L'**ultimo indirizzo del blocco** corrisponde al bitwise OR tra un indirizzo qualsiasi del blocco e il bitwise NOT della maschera

$$\text{Ultimo indirizzo} = (\text{qualsiasi indirizzo del blocco}) \text{ OR } (\text{NOT(mask)})$$

### Proposition 3. Indirizzi IP speciali

Alcuni **indirizzi IP speciali** vengono utilizzati come scorciatoie per ottenere determinati comportamenti:

- L'indirizzo **0.0.0.0** viene utilizzato per indicare **qualsiasi indirizzo possibile**
- Gli indirizzi IP la cui parte di rete è impostata completamente a 0 si riferiscono alla **sottorete corrente**
- L'indirizzo **255.255.255.255** permette la **trasmissione broadcast**, ossia ad ogni dispositivo, sulla rete **locale**
- Gli indirizzi con parte di rete opportuna e la parte di host impostata completamente ad 1 permettono l'invio di pacchetti **broadcast a reti distanti**
- Gli indirizzi in cui il primo ottetto è impostato a 127, dunque gli indirizzi **127.x.y.z**, vengono riservati al **loopback**. Tali pacchetti non vengono trasmessi sul mezzo di trasmissione ma vengono elaborati localmente dall'host e trattati come se fossero pacchetti in arrivo.

#### 4.3.1 Protocollo DHCP e indirizzamento gerarchico

Ogni **host** può ottenere il suo indirizzo IP all'interno della sua rete, dunque la sua **parte host** da associare alla parte di sottorete, in modalità **statica** tramite una sua configurazione interna (es: il file `/etc/rc.config` sul sistema operativo Unix) o in modalità **dinamica** ottenendo tale indirizzo IP da un server addetto, non richiedendo alcuna configurazione.

### Definition 37. Protocollo DHCP

Il **protocollo Dynamic Host Configuration Protocol (DHCP)** è un protocollo a livello di applicazione in grado di assegnare dinamicamente gli indirizzi IP agli host interni ad una rete:

1. Nel momento in cui si unisce alla rete, l'host effettua una richiesta broadcast interna alla rete, cercando un server DHCP al suo interno (**DHCP discover**)
2. Il server DHCP (solitamente collocato all'interno del router stesso) risponde alla richiesta offrendo all'host un possibile indirizzo IP (**DHCP offer**)
3. L'host risponde al server accettando tale indirizzo IP, prendendolo "in prestito" fino a quando esso non si disconnetterà dalla rete (**DHCP request**)
4. Il server DHCP risponde all'host confermando la presa in prestito di tale indirizzo (**DHCP ack**)

### Observation 3. Riutilizzo di indirizzi precedenti

Se l'host appena unitosi alla rete **ricorda** e desidera **riutilizzare** il precedente indirizzo IP, verrà inviato direttamente il messaggio di DHCP request in modalità broadcast, permettendo al server DHCP di rispondere immediatamente con un DHCP ack

Oltre all'indirizzo IP, solitamente il protocollo DHCP restituisce anche altre informazioni sulla sottorete, come l'indirizzo del router di **gateway**, ossia il primo router raggiungibile dal client per comunicare in rete, il nome e l'indirizzo IP del server DNS (se ve ne è uno) e la subnet mask della sottorete.

Per quanto riguarda le **reti** invece, ognuna di esse ottiene il suo indirizzo IP, dunque la sua **parte di sottorete**, effettuando una richiesta al proprio ISP, il quale allocherà una **porzione del proprio spazio di indirizzi**.

**Esempio:**

- Un ISP possiede il blocco di indirizzi **200.23.16.0/20**
- L'ISP decide di suddividere il suo blocco in 8 blocchi, associando ciascuno di essi ad un'organizzazione richiedente un blocco di indirizzi.

Proprietario	Indirizzo IP
ISP	<u>11001000 00010111 00010000 00000000</u> 200.23.16.0/20
Organiz. 1	<u>11001000 00010111 00010000 00000000</u> 200.23.16.0/23
Organiz. 2	<u>11001000 00010111 00010010 00000000</u> 200.23.18.0/23
...	...
Organiz. 7	<u>11001000 00010111 00011110 00000000</u> 200.23.30.0/23

In tal modo, è possibile creare una struttura di **indirizzamento gerarchico**, permettendo un'instradamento più efficiente tramite la pubblicizzazione di percorsi più specifici per poter raggiungere le sottoreti.

**Esempio:**

- Nell'esempio precedente, l'ISP pubblicizza un percorso più specifico per poter raggiungere le varie organizzazioni tra cui ha diviso il suo blocco di indirizzi, richiedendo all'esterno che gli venga inviato qualsiasi pacchetto avente un'indirizzo ricadente in tali range

In particolare, l'indirizzamento gerarchico è anche uno dei motivi per cui il **longest prefix matching** risulti essere così efficiente, cercando di inviare il pacchetto seguendo l'orientamento gerarchico.

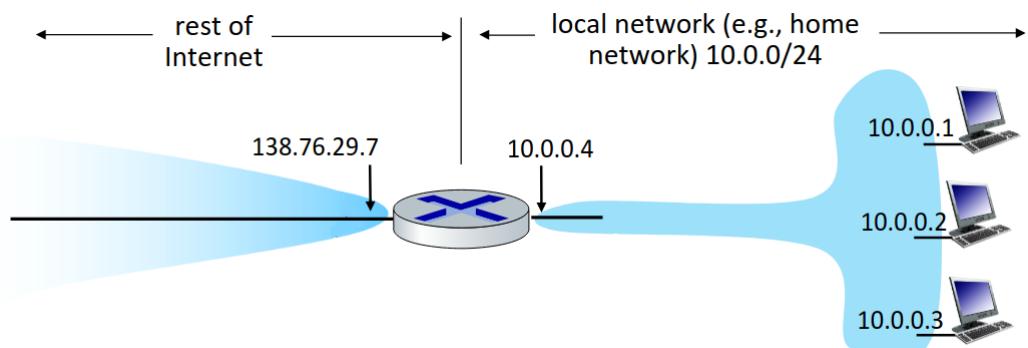
Per ottenere un blocco di indirizzi, ogni ISP deve effettuare una richiesta all'**Internet Corporation for Assigned Names and Numbers (ICANN)**, la quale alloca gli indirizzi IP attraverso **5 registri regionali** e gestisce la zona radice del DNS, inclusa la delega della gestione dei singoli TLD.

Tuttavia, nel 2011 l'ICANN ha assegnato l'ultima parte disponibile di **indirizzi IPv4** (ossia la versione trattata fino ad adesso), **esaurendo** a tutti gli effetti **gli indirizzi assegnabili**.

### 4.3.2 Servizio NAT e Protocollo IPv6

Per aggirare il problema dell'esaurimento degli indirizzi IPv4, è stato idealizzato un **escamotage** tramite l'implementazione del **Network Address Translation (NAT)**:

- Tutti i dispositivi interni ad una sottorete condividono **un solo IPv4 pubblico**, il quale viene utilizzato per identificare l'intera sottorete al mondo esterno
- Tutti i dispositivi interni ad una sottorete possiedono un proprio **indirizzo IPv4 privato**, il quale può essere utilizzato solo all'interno della sottorete stessa
- Tutti i datagrammi che escono dalla rete locale hanno lo **stesso indirizzo IPv4 pubblico di origine** ma **diversi numeri di porta di origine**, utilizzando quindi la porta del livello di trasporto come un identificatore univoco per un indirizzo IPv4 privato

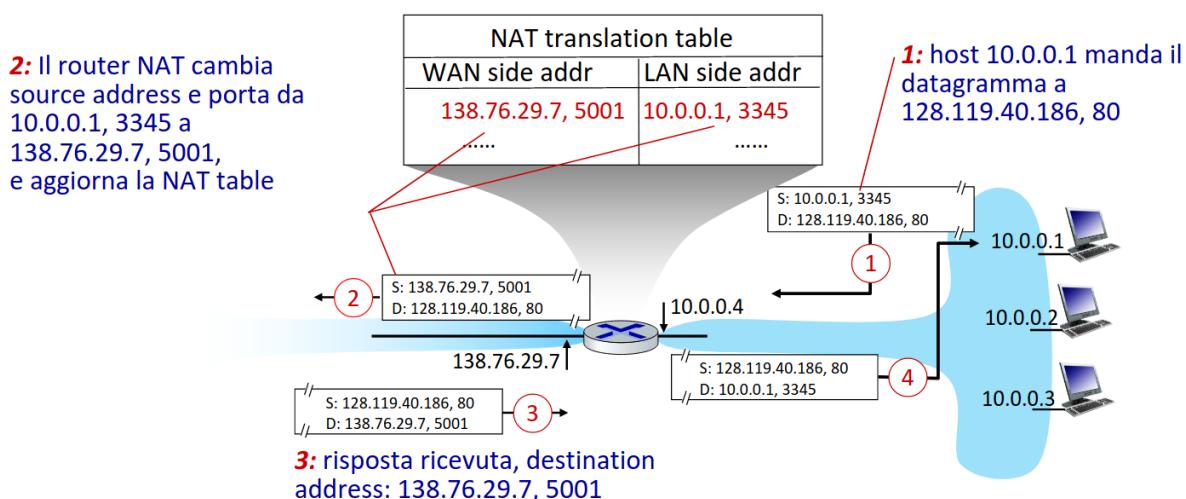


Tramite il NAT, dunque, l'ISP può utilizzare un **singolo indirizzo IPv4** per identificare ogni dispositivo interno ad una sottorete. Inoltre, gli indirizzi della rete locale possono essere gestiti separatamente, permettendo di cambiarli senza dover avvisare il mondo

esterno e fornendo una **maggior sicurezza**, poiché i dispositivi della rete locale non sono direttamente indirizzabili e visibili dall'esterno.

Per implementare il NAT, dunque, è necessario:

1. **Sostituire** la coppia <IP origine, Porta Origine> di ogni datagramma in uscita con la coppia <IP Router, Porta Random Inutilizzata>, implicando che i client/server remoti risponderanno utilizzando la nuova coppia come indirizzo di destinazione
2. **Memorizzare** all'interno di una **tavola di traduzione NAT** ogni coppia di conversione
3. **Sostituire** nuovamente la coppia di tutti i datagrammi in arrivo con la coppia originale, per poi spedire il datagramma al destinatario interno alla rete

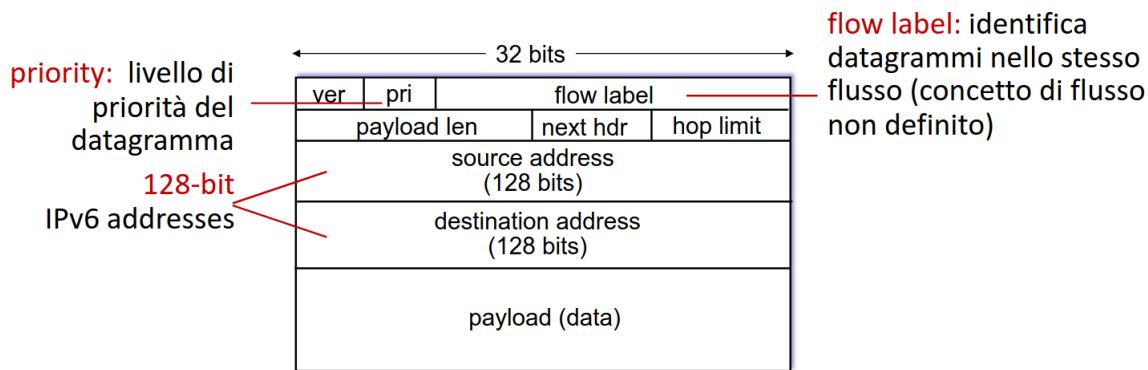


Per via della sua implementazione, l'utilizzo del NAT ha generato molte controversie:

- Per loro definizione stessa, i router dovrebbero processare i pacchetti solo **fino al livello di rete**, mentre per attuare il NAT è necessario che essi adoperino anche il livello di trasporto per modificare le porte dei datagrammi
- La **carenza di indirizzi** può essere risolta anche tramite gli **indirizzi IPv6** (che vedremo in seguito)
- Viene **violata** la modalità di trasmissione **end-to-end**, poiché è necessario manomettere il pacchetto per effettuare le traduzioni

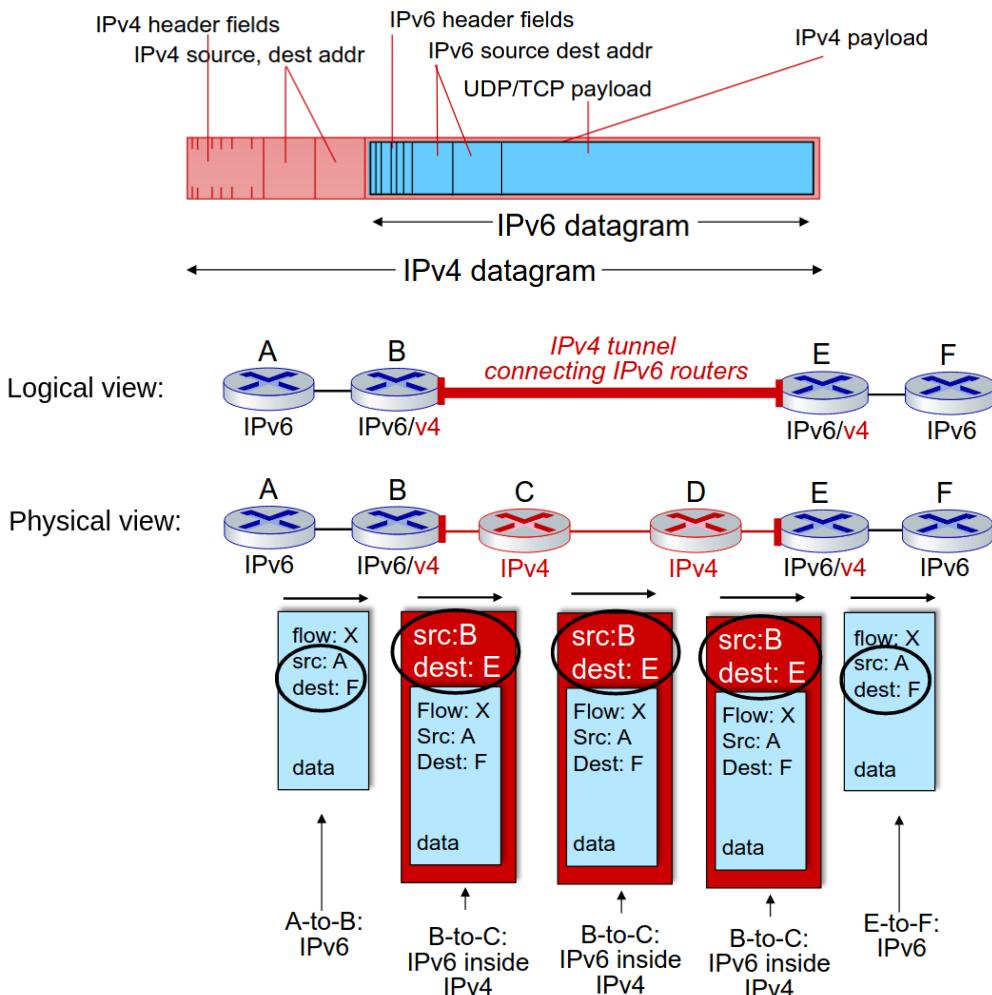
Tuttavia, il NAT risulta ormai essere attualmente ampiamente utilizzato in reti domestiche, istituzionali e cellulari, rendendo **lenta** la sua sostituzione con strumenti più moderni.

In particolare, il principale strumento che (man mano) sostituirà l'uso dell'IPv4 e il NAT è il **protocollo IPv6**, dove vengono utilizzati **128 bit** per gli indirizzi invece di 32 bit e vengono **rimossi** il **checksum** per i datagrammi (non per gli altri livelli superiori) per velocizzare l'elaborazione nei router, la **frammentazione** dei datagrammi e i **campi opzione** (implementabili tramite protocolli superiori).



Poiché non tutti i router possono essere aggiornati contemporaneamente, attualmente vengono utilizzati un **indirizzamento misto**, utilizzando sia l'IPv4 che l'IPv6:

- Per le comunicazioni tra due router IPv4 viene utilizzato direttamente il protocollo IPv4. Analogamente, per le comunicazioni tra due router IPv6 viene utilizzato direttamente il protocollo IPv6
- Per le comunicazioni tra un router IPv6 e un router IPv4 viene utilizzato il **tunneling**, dove un datagramma IPv6 viene trasportato come payload all'interno di un datagramma IPv4 ("datagramma dentro un datagramma").



## 4.4 Protocollo ICMP e Traceroute

### Definition 38. Protocollo ICMP

Il **protocollo Internet Control Message Protocol (ICMP)** è un protocollo a livello di rete utilizzato da host e router per scambiarsi informazioni a livello di rete (es: report degli errori come un host irraggiungibile).

I **messaggi ICMP** hanno un campo **tipo** e un campo **codice**, contenendo l'header e i primi 8 byte del datagramma IP che ha provocato la generazione del messaggio.

Il protocollo ICMP viene considerato "parte" del protocollo IP, nonostante quest'ultimo venga utilizzato da ICMP per inviare i suoi messaggi. Per tale motivo, esso viene considerato come "superiore" a IP all'interno dello stack TCP/IP.

<b>Tipo</b>	<b>Codice</b>	<b>Descrizione</b>
0	0	Risposta echo (a ping)
3	0	Rete destin. irraggiungibile
3	1	Host destin. irraggiungibile
3	2	Protocollo dest. irraggiungibile
3	3	Porta destin. irraggiungibile
3	6	Rete destin. sconosciuta
3	7	Host destin. sconosciuto
4	0	Riduzione (controllo di congestione)
8	0	Richiesta echo
9	0	Annuncio del router
10	0	Scoperta del router
11	0	TTL scaduto
12	0	Errata intestazione IP

Uno dei programmi utilizzante lo scambio di messaggi echo di richiesta e risposta del protocollo ICMP è il **programma ping**, presente su (quasi) ogni dispositivo, utilizzato per calcolare rapidamente il RTT.

**Esempio:**

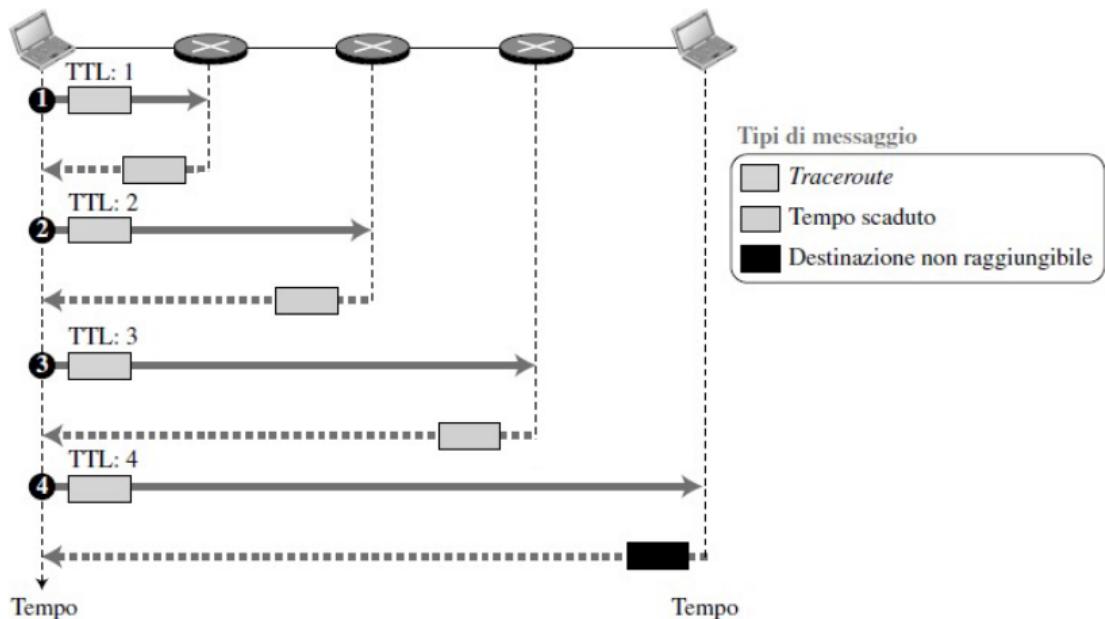
```
$ping google.it

PING google.it (142.250.180.163) 56(84) bytes of data.
64 bytes from mil04s44-in-f3.1e100.net (142.250.180.163):
icmp_seq=1 ttl=114 time=17.0 ms
64 bytes from mil04s44-in-f3.1e100.net (142.250.180.163):
icmp_seq=2 ttl=114 time=16.5 ms
64 bytes from mil04s44-in-f3.1e100.net (142.250.180.163):
icmp_seq=3 ttl=114 time=16.9 ms
--- google.it ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 16.452/16.800/17.026/0.250 ms
```

Un ulteriore programma utilizzato per vedere il percorso effettuato dal traffico per raggiungere un determinato host è il **programma traceroute**.

Il programma invia una **serie di datagrammi IP** alla destinazione, ciascuno contenente un segmento UDP con un numero di porta inutilizzato. All'interno di ogni datagramma viene inserito un **valore incrementale** (partendo da 1) nel campo header **Time-to-live (TTL)**, corrispondente al numero di router attraversabili prima che il datagramma venga considerato come **scaduto**:

- Per ogni datagramma inviato, il mittente avvia un **timer**
- Se l'*n*-esimo **datagramma** arriva all'*n*-esimo **router**, esso scarterà il datagramma, inviando al mittente un messaggio di allerta ICMP (tipo 11, codice 0), contenente inoltre il nome del router e il suo indirizzo IP. Quando il messaggio ICMP arriverà al mittente, esso calcolerà anche il RTT. Tale processo viene ripetuto per tre volte.
- Se invece il segmento UDP arriva all'**host di destinazione**, esso restituirà un messaggio ICMP segnalando che la porta sia irraggiungibile (tipo 3, codice 3), utilizzato solo come "valore simbolico". Quando l'origine riceverà tale messaggio, verrà arrestato l'invio di dei datagrammi.
- Una volta arrestato l'invio, verranno utilizzati tutti i messaggi di risposta ricevuti per ricostruire il **percorso effettuato**



## 4.5 API OpenFlow e forwarding generalizzato

Come già discusso in precedenza, ogni router è dotato di una propria **forwarding table** (anche detta **flow table**). L'uso delle forwarding table può essere astratto tramite il concetto di **match plus action**:

- Ad ogni **match** (ad esempio usando il longest prefix matching), viene eseguita un'**azione**
- Le **azioni** eseguibili consistono in **forward**, **drop**, **modify** e **send to controller**
- Per disambiguare pattern sovrapposti (ossia match multipli), vengono utilizzate **regole di priorità**
- Vengono utilizzati anche dei **contatori** per il numero di byte e il numero di pacchetti



Le **API OpenFlow** consentono l'**accesso al data plane** di un host o router attraverso la rete, venendo utilizzato per dettare le **regole** implementate all'interno delle forwarding table. Ogni regola dettata è composta da un campo **match**, un campo **action** ed un campo **statistics**



Esempi:

1. **Destination-based forwarding**: per inoltrare sulla porta di output 6 tutti i datagrammi IP destinati all'indirizzo IP 51.6.0.8 verrà utilizzata la seguente regola:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	VLAN Pri	IP Src	IP Dst	IP Prot	IP ToS	TCP s-port	TCP d-port	Action
*	*	*	*	*	*	*	*	51.6.0.8	*	*	*	port6

2. **Firewall:** per bloccare tutti i datagrammi IP la cui porta di destinazione è la porta TCP/22 (corrispondente ad un protocollo non visto, ossia il protocollo SSH) verrà utilizzata la seguente regola:

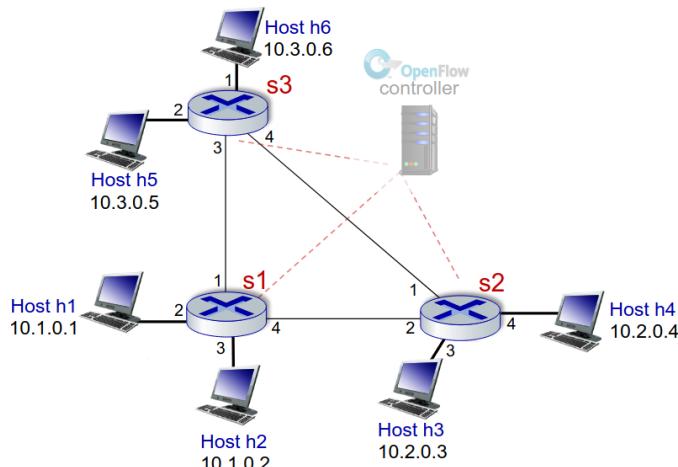
Switch Port	MAC src	MAC dst	Eth type	VLAN ID	VLAN Pri	IP Src	IP Dst	IP Prot	IP ToS	TCP s-port	TCP d-port	Action
*	*	*	*	*	*	*	*	*	*	*	*	22 drop

3. **Forwarding a livello di collegamento:** per inoltrare sulla porta di output 3 tutti i datagrammi IP destinati all'indirizzo MAC 22:A7:23:11:E1:02 (vedremo in seguito il protocollo MAC) verrà utilizzata la seguente regola:

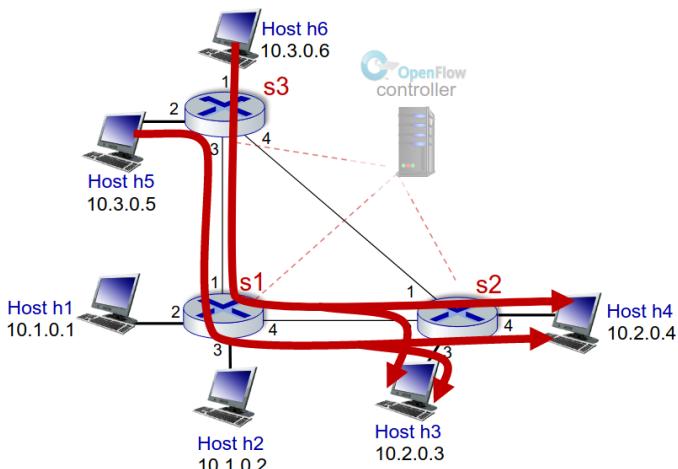
Switch Port	MAC src	MAC dst	Eth type	VLAN ID	VLAN Pri	IP Src	IP Dst	IP Prot	IP ToS	TCP s-port	TCP d-port	Action
*	*	22:A7:23: 11:E1:02	*	*	*	*	*	*	*	*	*	port3

#### 4. Gestione del flusso

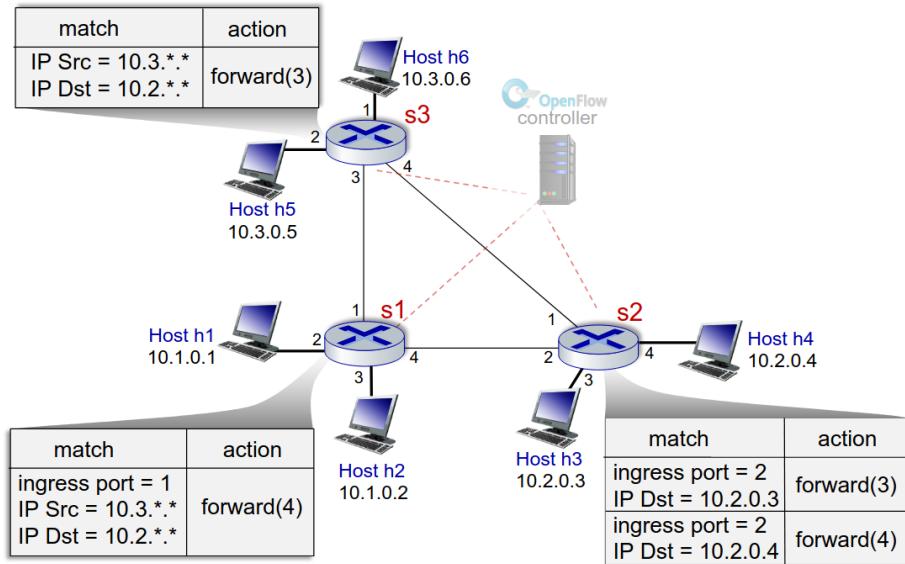
- Consideriamo la seguente rete



- Vogliamo far sì che i datagrammi dagli host h5 e h6 inviati verso gli host h3 e h4 passino prima per il router s1 e poi per il router s2



- Per ottenere tale flusso, impostiamo le seguenti flow table all'interno dei router



## 4.6 Principi architetturali di Internet

### Definition 39. Middleboxes

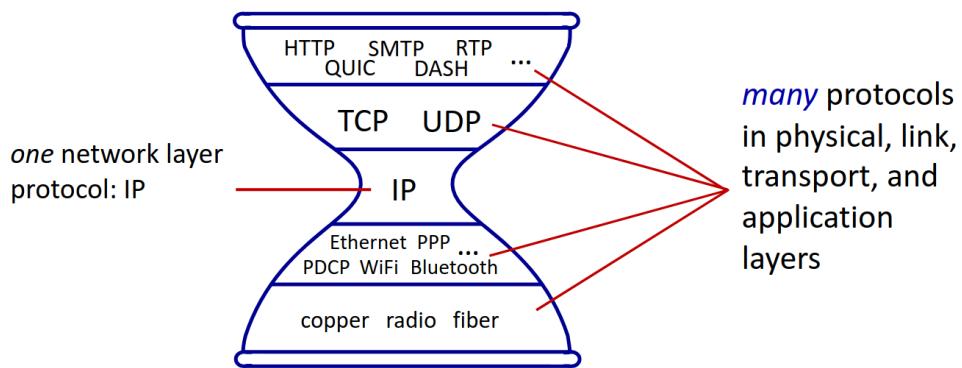
Un **middlebox** è un qualsiasi dispositivo **intermediario** tra mittente e destinatario che esegue **funzioni diverse** dalle normali funzioni standard di un router (es: NAT, Firewall, Cache servers, Load balancers, ...)

### Proposition 4. Principi architetturali di Internet

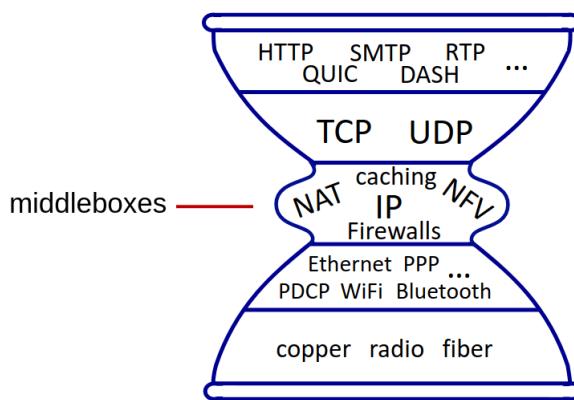
Come dettato all'interno del documento RFC 1958, non vi è una vera e propria architettura standard per Internet, bensì solamente delle "**tradizioni**". In termini generici, il servizio Internet è basato su tre principi fondamentali:

- **Connettività semplice**, rendendo il servizio facile da implementare nel maggior numero di dispositivi possibili
- Mantenere la **clessidra TCP/IP** con il **minor girovita possibile**, cercando di ridurre al minimo il numero di servizi svolti dal livello di rete, aumentando la quantità verso i livelli superiori e inferiori
- Complessità ed intelligenza (ossia lo svolgimento delle operazioni, il mantenimento dei dati, ...) deve essere implementata sulla **periferia della rete** utilizzando il **principio end-to-end**.

### Clessidra TCP/IP ottimale



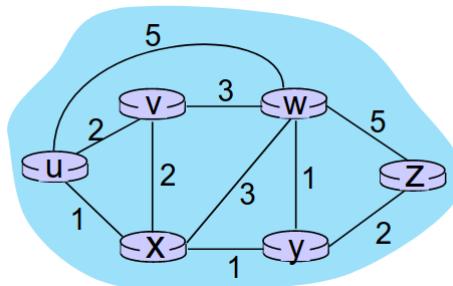
### Clessidra TCP/IP dopo 40 anni



## 4.7 Algoritmi di instradamento

Gli **algoritmi di instradamento** vengono utilizzati per determinare il **percorso migliore**, ossia una sequenza di router che i pacchetti devono attraversare, da una sorgente ad una destinazione.

Per determinare tali percorsi, la rete viene modellata come un **grafo**  $G = (N, E)$  i cui vertici  $V(G) = \{v_1, \dots, v_n\}$  corrispondono ai singoli router e/o host e gli archi  $E(G)$  corrispondono ai collegamenti tra tali dispositivi. Ad ogni arco  $(u, v) \in E(G)$  viene attribuito un **costo** (o **peso**) il quale può essere dettato da **più valori** (maggior velocità, minore congestione, ...).



Gli algoritmi di routing vengono classificati in:

- **Statici**, ossia determinanti percorsi poco soggetti al cambiamento, oppure **dinamici**, ossia determinanti percorsi soggetti ad un aggiornamento periodico in risposta a variazioni dei costi
- **Globali**, dove al termine dell'algoritmo tutti i router conoscono completamente la topologia e il costo dei link della rete, oppure **decentralizzati**, dove lo scambio di informazioni avviene tra router vicini che non conoscono l'intero stato della rete

Per le successive sezioni, utilizzeremo la seguente **notazione**:

- $c_{x,y}$  è il **costo del link diretto** tra i nodi  $x$  e  $y$ . Viene posto uguale a  $\infty$  se tale link diretto non esiste.
- $D(v)$  è la **stima corrente** del costo del percorso a minor costo dal nodo sorgente al nodo destinazione  $v$
- $p(v)$  è il **nodo predecessore** lungo il percorso dal nodo sorgente al nodo  $v$

### 4.7.1 Algoritmo link-state di Dijkstra

L'algoritmo **link-state** è un algoritmo **dinamico globale** basato sull'**algoritmo di Dijkstra**. Dato un **nodo sorgente**  $u \in V(G)$ , per ogni nodo  $u \neq v \in V(G)$  viene calcolato il percorso a **distanza minore** (ossia di minor costo) da un **nodo sorgente** a tutti gli altri nodi della rete, per poi fornire una forwarding table alla sorgente in base ai percorsi calcolati.

---

**Algorithm 1:** Algoritmo Link-State (basato su Dijkstra)

---

**Function** linkStateDijkstra( $G, u$ ):

```

 $R = \{u\};$ 
for  $v \in V(G)$  do
    if  $\exists(u, v) \in E(G)$  then
         $| D(v) = c_{u,v};$ 
    else
         $| D(v) = \infty;$ 
    end
end
while  $R \neq V(G)$  do
     $w := \arg \min_{w \in V(G) - R} [D(w)];$ 
     $R.\text{add}(w);$ 
    for  $x \in V(G) - R$  do
        if  $\exists(w, x) \in E(G)$  then
             $| D(x) = \min(D(x), D(w) + c_{w,x});$ 
             $| p(x) = w;$ 
        end
    end
end

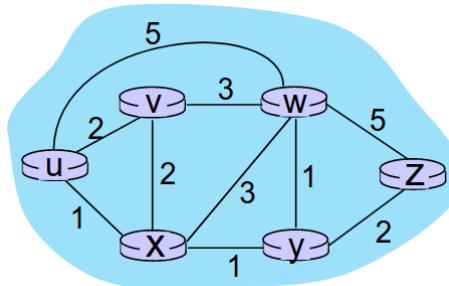
```

**end**

---

**Esempio:**

- Consideriamo la seguente rete



- Vogliamo calcolare la forwarding table del nodo sorgente  $u$ . Inizializziamo quindi la tabella delle distanze dalla sorgente  $u$  verso ogni nodo, ponendo la distanza di ogni nodo adiacente a  $u$  pari al costo del link diretto e pari a  $\infty$  per ogni altro nodo

$R$	$D(v), p(v)$	$D(w), p(w)$	$D(x), p(x)$	$D(y), p(y)$	$D(z), p(z)$
$\{u\}$	2, $u$	5, $u$	1, $u$	$\infty$	$\infty$

- A questo punto, consideriamo il nodo avente distanza minore dal nodo attualmente analizzato (ossia  $u$ ), corrispondente al nodo  $x$ . Per ogni nodo  $a$  adiacente a  $x$  non ancora analizzato (ossia non in  $R$ ), poniamo la nuova distanza calcolata pari al minimo tra la distanza dalla sorgente ad  $x$ , ossia  $D(x)$ , e la somma tra la distanza tra la sorgente ed  $a$  e il costo del link tra  $a$  ed  $x$ , ossia  $D(a) + c_{a,x}$

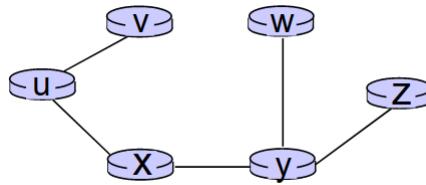
$R$	$D(v), p(v)$	$D(w), p(w)$	$D(x), p(x)$	$D(y), p(y)$	$D(z), p(z)$
$\{u\}$	2, $u$	5, $u$	1, $u$	$\infty$	$\infty$
$\{u, x\}$	2, $u$	4, $x$		2, $x$	$\infty$

- Proseguendo analogamente, le distanze finali calcolate saranno pari a:

$R$	$D(v), p(v)$	$D(w), p(w)$	$D(x), p(x)$	$D(y), p(y)$	$D(z), p(z)$
$\{u\}$	2, $u$	5, $u$	1, $u$	$\infty$	$\infty$
$\{u, x\}$	2, $u$	4, $x$		2, $x$	$\infty$
$\{u, x, y\}$	2, $u$	3, $y$			4, $y$
$\{u, x, y, v\}$		3, $y$			4, $y$
$\{u, x, y, v, w\}$					4, $y$
$\{u, x, y, v, w, z\}$					

- Una volta ottenute le distanze finali, verrà costruita la forwarding table di  $u$ :
  - I nodi  $v$  e  $x$  sono direttamente raggiungibili da  $u$  con distanza minima
  - Il nodo  $y$  è raggiungibile tramite  $x$  con distanza minima

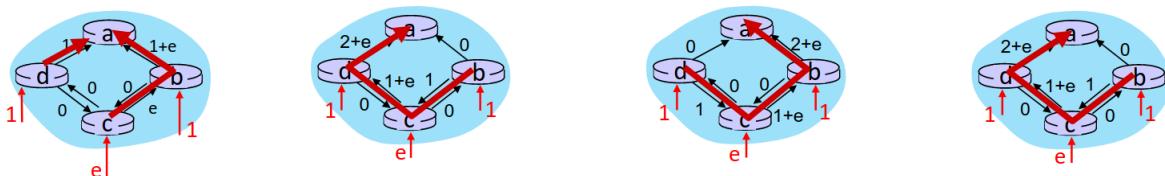
- I nodi  $w$  e  $z$  sono raggiungibili tramite  $y$  con distanza minima, necessitando dunque di passare anche per  $x$



Forwarding table di $u$	
Destinazione	Link di uscita
$v$	$(u, v)$
$x$	$(u, x)$
$y$	$(u, x)$
$w$	$(u, x)$
$z$	$(u, x)$

L'algoritmo link-state ha una **complessità computazionale** pari a  $O(n^2)$  (anche se è possibile implementarlo ottimamente in  $O(n \log n)$ ) ed una **complessità di comunicazione** pari a  $O(n^2)$ , poiché ogni router deve trasmettere in broadcast il suo stato dei costi a tutti gli altri router (richiedendo  $O(n)$  tramite algoritmi efficienti).

Inoltre, poiché i costi dei link dipendono dal volume di traffico, può verificarsi un **caso patologico** per via delle **oscillazioni del percorso**, richiedendo di essere costantemente ricalcolati.



## 4.7.2 Algoritmo Distance-vector

L'algoritmo **distance-vector** è un algoritmo **dinamico decentralizzato** basato sulla **equazione di Bellman-Ford**.

### Theorem 5. Equazione di Bellman-Ford

Dati  $x, y \in V(G)$ , sia  $D_x(y)$  la **distanza minima da  $y$  ad  $x$** .

In tal caso, si ha che:

$$D_x(y) = \min_{v \in V(G)} [c_{x,v} + D_v(y)]$$

Al verificarsi di un determinato **evento** (es: lo scadere di un timer), ogni nodo invia ai propri vicini la propria **stima del distance-vector**, ossia un vettore contenente le distanze verso tutti i nodi della rete. Quando un nodo riceve una stima da parte di un vicino, utilizza tale stima per aggiornare il proprio distance-vector tramite l'**equazione di Bellman-Ford**. Sotto determinate condizioni ottimali, la distanza stimata **converge** dopo un determinato numero di interazioni alla **distanza minima**.

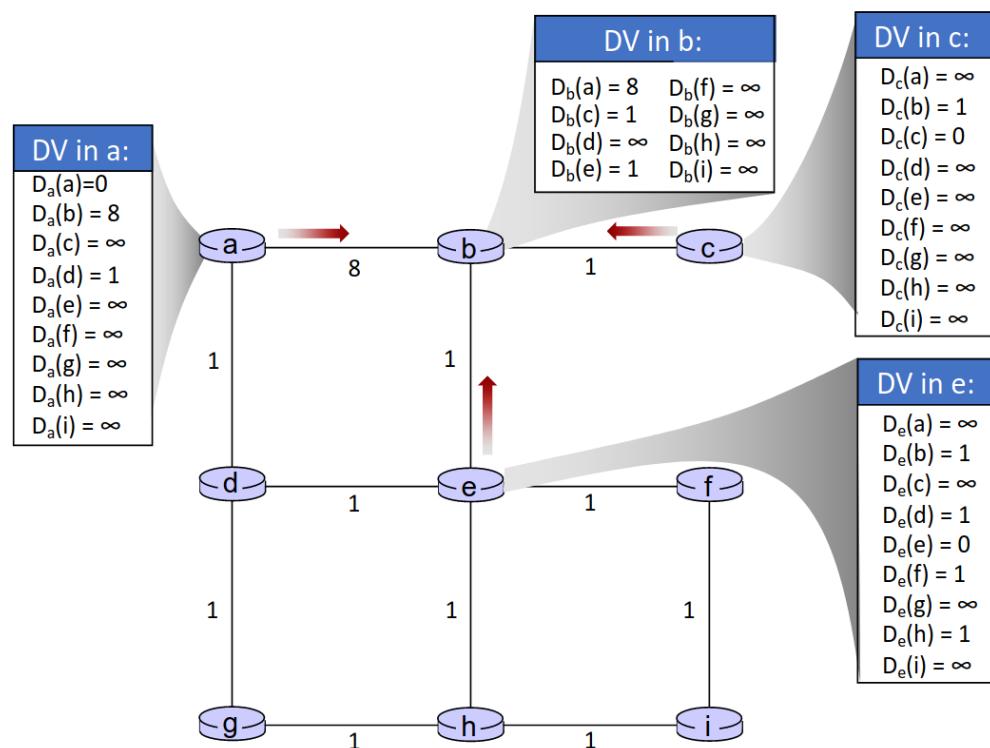
Solitamente, l'aggiornamento locale del vettore di un nodo viene effettuato solo a seguito dell'**aggiornamento** del costo di un **link diretto** da tale nodo verso un suo vicino o a seguito della **ricezione di un vettore aggiornato** inviato da un vicino (**Iterativo ed asincrono**). Inoltre, ogni nodo invia il proprio distance-vector ai vicini solo quando esso viene aggiornato (**Distribuito, self-stopping e responsive**).

Dunque, l'algoritmo è riassumibile nei seguenti passi:

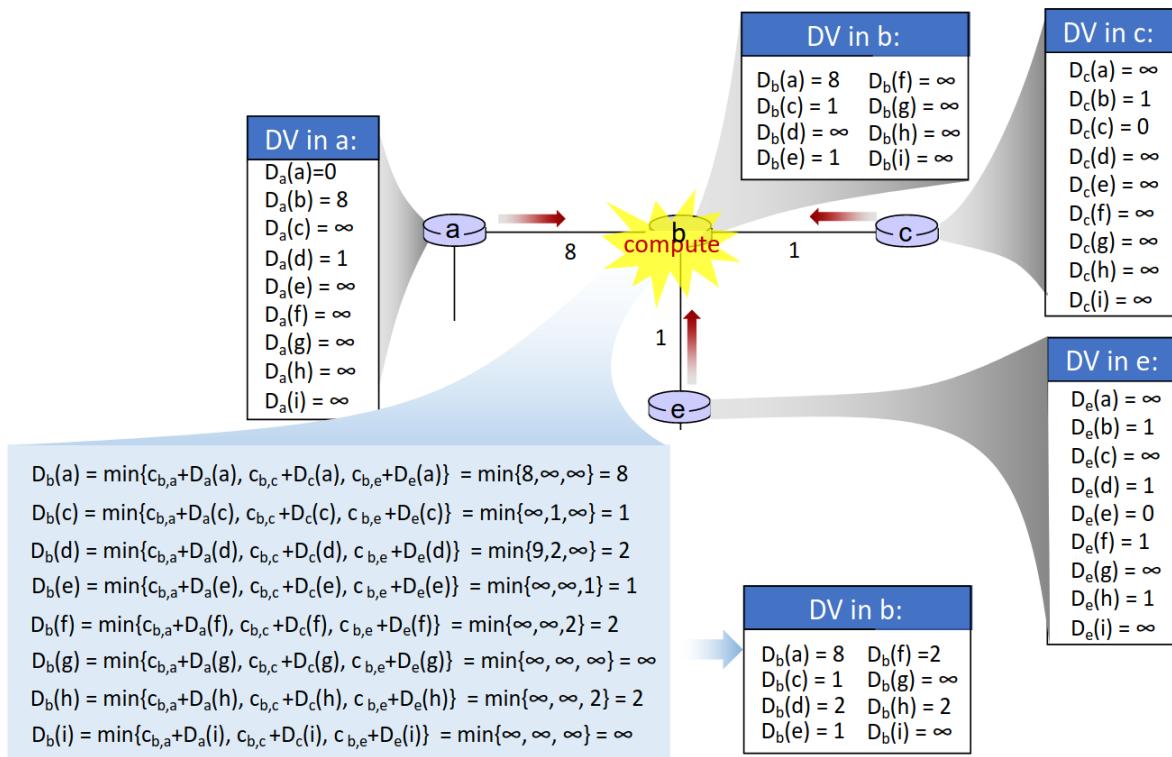
1. **Inizializzazione:** il DV di ogni nodo contiene il costo diretto verso tutti i suoi vicini e  $\infty$  per ogni altro nodo
2. **Attesa dell'evento:** ogni nodo attende il cambio di un costo diretto locale o la ricezione del vettore di un vicino
3. **Ricalcolo del DV:** se l'evento viene attivato per un nodo, esso ricalcola il proprio DV utilizzando i valori precedenti e quelli ricevuti
4. **Invio solo se modificato:** se al termine del calcolo il DV del nodo è stato aggiornato, esso viene inviato ai vicini del nodo
5. Viene ripetuto il tutto in loop tornando al passo 2

**Esempio:**

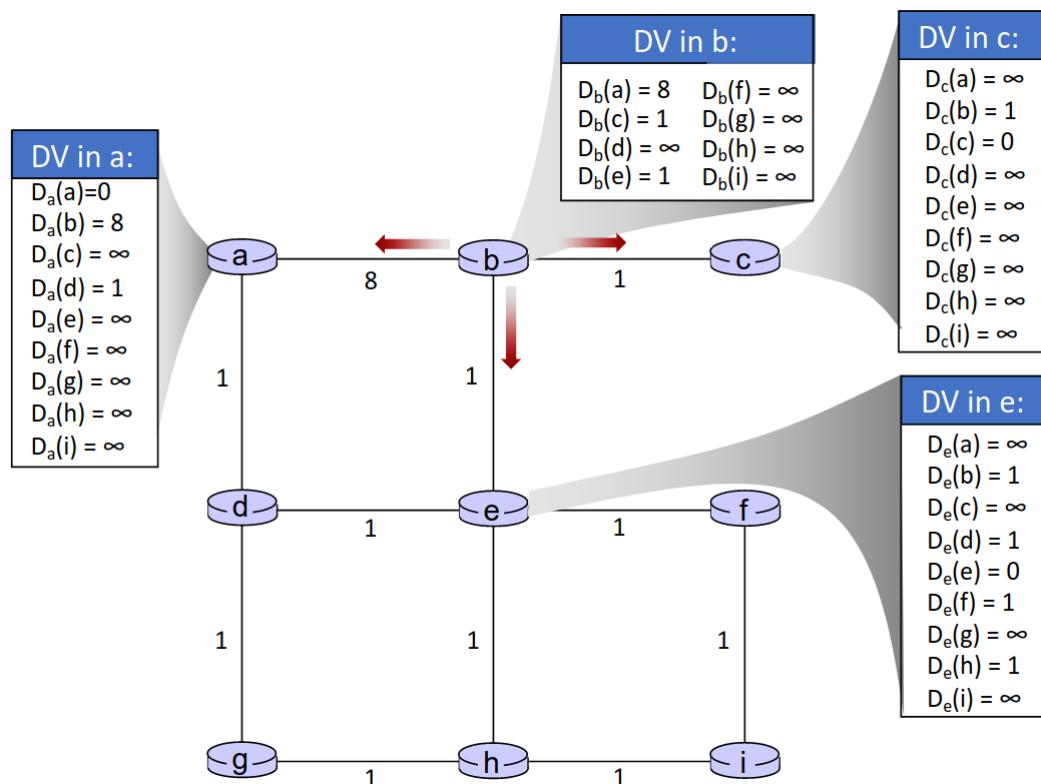
- Supponiamo che i router *a*, *c* ed *e* inviano il proprio DV al router *b*



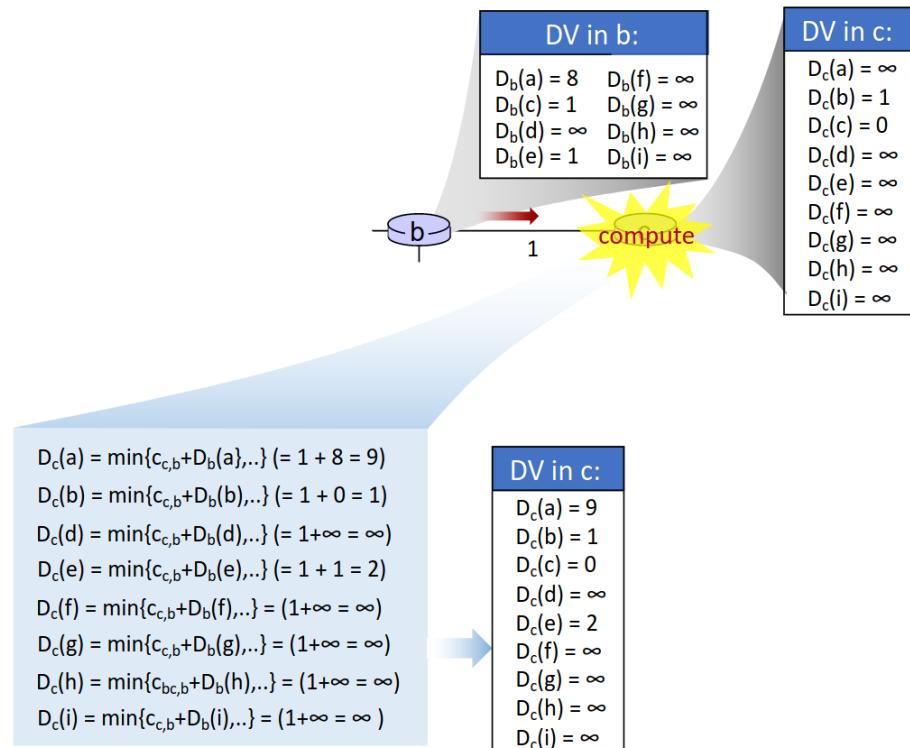
- Una volta ricevuti i vettori, il router *b* ricalcola il proprio DV utilizzando l'equazione di Bellman-Ford



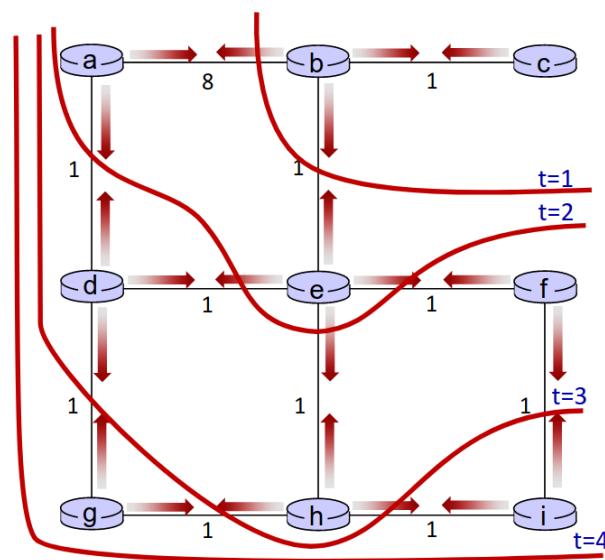
- Successivamente, il nuovo DV viene inviato ai vicini del router *b*



- Una volta ricevuto il DV di  $b$ , il router  $c$  (e anche i router  $a$  ed  $e$ ) procederà a ricalcolare il proprio DV utilizzando le nuove distanze ricevute



- Al passare degli istanti di tempo, i cambiamenti effettuati all'istante  $t = 0$  verranno propagati su tutti gli altri router della rete



Come l'algoritmo link-state, anche l'algoritmo distance-vector è soggetto a **comportamenti patologici**, in particolare il **conteggio all'infinito**:

1. Data la seguente rete, supponiamo che il costo del link  $(x, y)$  venga modificato da 4 a 60



2. Di conseguenza, il router  $y$  nota il nuovo costo del collegamento diretto verso  $x$  sia 60. Tuttavia, il nodo  $y$  ha precedentemente ricevuto il DV del router  $z$ , venendo a sapere che tramite  $z$  sia possibile raggiungere  $x$  con un costo pari a 6, aggiornando quindi il proprio DV ed inviandolo ai suoi vicini

$$D_y(x) = 4 \quad \xrightarrow{\text{diventa}} \quad D_y(x) = c_{y,z} + D_z(x) = 1 + 5 = 6$$

**(Attenzione:** è necessario ricordare che l'algoritmo distance-vector è decentralizzato dunque il vertice  $y$  non sa che il percorso da  $z$  a  $x$  passi per  $y$  stesso)

3. Successivamente, il vertice  $z$  riceverà il DV di  $y$ , notando che la distanza del percorso da  $y$  a  $x$  tramite cui  $z$  possa raggiungere  $x$  è stato modificato, aggiornando quindi il proprio DV ed inviandolo ai vicini

$$D_z(x) = 5 \quad \xrightarrow{\text{diventa}} \quad D_z(x) = c_{z,y} + D_z(y) = 1 + 6 = 7$$

4. Analogamente,  $y$  riceverà il DV di  $z$ , ricadendo nella stessa casistica

$$D_y(x) = 6 \quad \xrightarrow{\text{diventa}} \quad D_y(x) = c_{y,z} + D_z(x) = 1 + 7 = 8$$

5. ...

### Proposition 6. Soluzioni al conteggio all'infinito

Per risolvere il comportamento patologico del **conteggio all'infinito**, l'algoritmo DV adotta due politiche aggiuntive:

- **Split horizon**, dove, invece che inviare l'intera tabella attraverso ogni interfaccia, ogni nodo invia solo una porzione della propria tabella a seconda dell'interfaccia (es: se il nodo  $x$  riceve il DV del nodo  $y$ , nel DV di  $x$  aggiornato inviato verso  $y$  verranno omesse le informazioni ricevute da  $y$ )
- **Poisoned reverse**, dove, durante l'invio del proprio DV, il nodo mittente pone a  $\infty$  la distanza dei percorsi passanti attraverso il vicino a cui sta inviando il nuovo DV (es: se il nodo  $x$  deve inviare il suo DV al nodo  $y$  e un percorso per di  $x$  verso un nodo  $z$  passa per  $y$ , nel DV inviato viene posto  $D_x(z) = \infty$ )

A differenza dell'algoritmo link-state, l'algoritmo distance-vector possiede una **complessità di comunicazione** pari a  $O(n)$ . Per quanto riguarda la **velocità di convergenza**, invece, l'algoritmo LS necessita di  $O(n^2)$  computazioni (a meno di oscillazioni) mentre l'algoritmo DV richiede condizioni troppo ottimali (l'instradamento potrebbe divenire ciclico).

Inoltre, per propria natura stessa, l'algoritmo DV risulta essere **meno robusto**:

- Supponiamo che un router subisca un malfunzionamento o un attacco esterno, peggiorando notevolmente il costo dei propri link diretti
- Nell'algoritmo LS, tale router pubblicherà un **costo errato dei link diretti**. Tuttavia, poiché ogni router calcola solamente la propria tabella, gli altri router non verranno influenzati.
- Nell'algoritmo DV, invece, tale router pubblicherà un **costo errato dei percorsi (black-holing)**. Di conseguenza, poiché ogni altro router userà il DV di tale router per i calcoli, l'errore verrà **propagato sull'intera rete**

## 4.8 Instradamento intra-AS e inter-AS

Gli algoritmi di routing precedentemente visti si basano su una *concezione irrealistica* della rete, poiché viene assunto che tutti i router siano identici e che non vi sia alcuna gerarchia al suo interno, oltre all'evidente problema di scala dovuto alle miliardi di destinazioni che porterebbe ad intasare la rete con messaggi di scambio di forwarding table.

### Proposition 7. Instradamento intra-AS e inter-AS

Per risolvere tali problematiche, i router vengono **aggregati** in regioni note come **autonomous systems (AS)** o **domini**. Ogni AS costituisce una rete composta da soli router.

Distinguiamo quindi due tipologie di instradamento:

- **Instradamento intra-AS** ossia instradamento all'interno di un AS, dove tutti i router all'interno dell'AS devono eseguire lo stesso protocollo di instradamento intra-AS, implicando che router di diversi AS possano scegliere il proprio protocollo.
- **Instradamento inter-AS**, ossia instradamento tra diversi AS, dove ogni AS possiede un gateway router posto sul bordo e connesso ai gateway router degli altri AS (i gateway partecipano comunque all'instradamento intra-AS)

Le **forwarding table**, dunque, verranno configurate sia da algoritmi di instradamento intra-dominio sia da algoritmi di instradamento inter-dominio.

Di conseguenza, ogni router deve essere in grado di apprendere quali destinazioni siano raggiungibili tramite gli AS esterni e propagare tali informazioni all'interno del proprio AS.

### 4.8.1 Protocolli RIP e OSPF

#### Definition 40. Protocollo RIP

Il protocollo Routing Information Protocol (RIP) è un protocollo di **instradamento intra-AS** basato sull'**algoritmo distance-vector**.

La metrica di costo utilizzata è la **distanza misurata in hop**, ossia il numero di router necessari da attraversare per raggiungere la destinazione. Il **valore massimo** per tale metrica è **15 hop** (il valore 16 corrisponde a  $\infty$ )

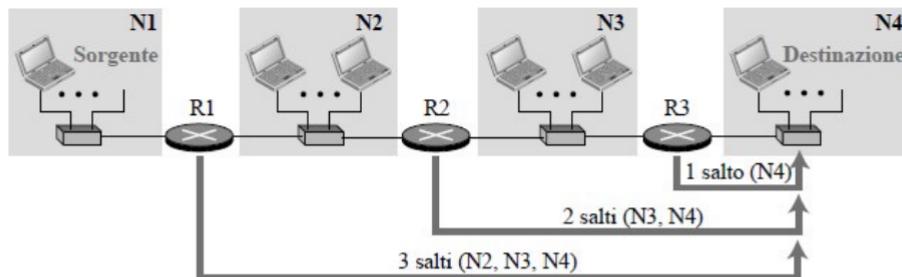


Tabella d'inoltro per R1

Rete di destinazione	Prossimo router	Costo (in hop)
N1	—	1
N2	—	1
N3	R2	2
N4	R2	3

Tabella d'inoltro per R2

Rete di destinazione	Prossimo router	Costo (in hop)
N1	R1	2
N2	—	1
N3	—	1
N4	R3	2

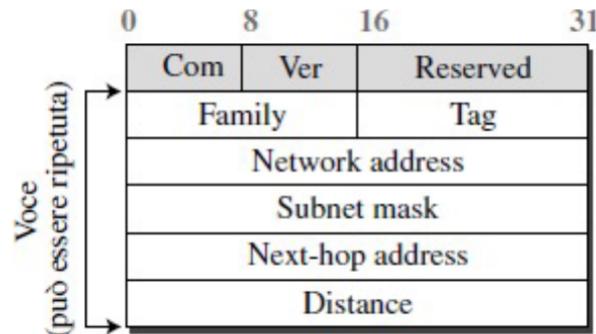
Tabella d'inoltro per R3

Rete di destinazione	Prossimo router	Costo (in hop)
N1	R2	3
N2	R2	2
N3	—	1
N4	—	1

Periodicamente, dunque dopo un **prefissato lasso di tempo**, ogni router utilizzante l'algoritmo RIP invierà il proprio distance-vector assieme ad alcune informazioni aggiuntive, fornendo agli altri router informazioni sugli host e le altre reti (ossia gli altri AS) raggiungibili.

Se all'interno del DV di un router  $x$  vi è un'entrata indicante la possibilità di raggiungere la rete  $A$  con un costo pari a  $N$  hop, ogni altro router all'**interno della rete** di  $x$  saprà di poter raggiungere la rete  $A$  con un costo pari a  $N + 1$  passando tramite  $x$ .

Ogni messaggio può contenere **più voci**, ognuna di esse corrispondenti ad un'entrata del distance-vector del router mittente.



I messaggi di **RIP request** vengono inviati dai router al momento della loro immissione all'interno di un AS oppure a fini diagnostici (es: per richiedere una voce specifica).

Per quanto riguarda i messaggi di **RIP response**, invece, essi vengono inviati in risposta ad un messaggio di richiesta (**solicited response**) o a seguito dello scadere di un timer di 25-35 secondi (**unsolicited response**). Oltre a tale timer periodico, vengono utilizzati due ulteriori timer:

- Un **timer di scadenza** (150-210 secondi), dove se allo scadere del tempo non è stato ricevuto alcun aggiornamento per un percorso, esso viene considerato come scaduto, venendo posto a 16 (dunque a  $\infty$ ).

Se un router non riceve messaggi da un suo vicino per circa 180 secondi (media tra 150 e 210), tale vicino viene considerato **spento o guasto**, impostando il costo di tale percorso a 16 e propagando l'informazione sugli altri nodi della rete.

- Un **timer per il garbage collection** (120 secondi), dove se allo scadere del tempo il router continua ad annunciare un percorso con costo pari a 16, tale percorso viene completamente rimosso

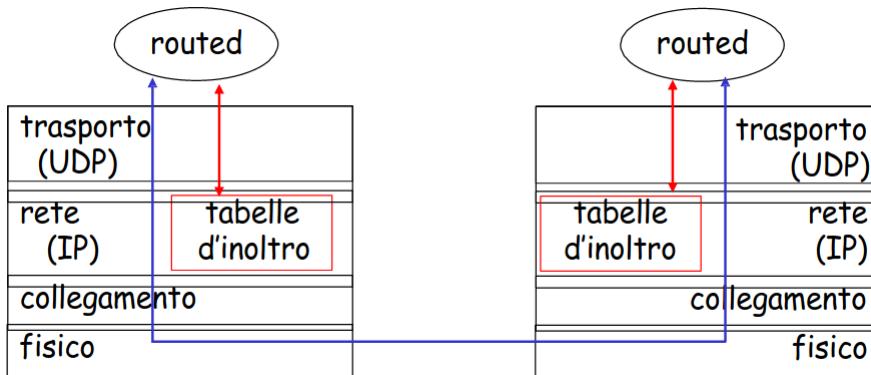
Essendo basato sull'algoritmo distance-vector, il protocollo RIP presenta gli stessi comportamenti patologici, i quali vengono mediati utilizzando sia lo **split horizon** sia il **poisoned reverse**. Inoltre, quando viene ricevuta un'informazione da una rotta non più valida (dunque posta a 16), viene avviato un timer e tutti i messaggi arrivati prima del timeout e riguardanti tale rotta vengono ignorati (**hold-down**)

#### Observation 4

Il **protocollo RIP** viene implementato tramite un processo a livello di applicazione chiamato **routed (route daemon)**, il quale utilizza **protocollo UDP** sulla **porta 520** per l'invio dei messaggi.

Per tale motivo, seppur considerato un protocollo al livello di rete, sarebbe più corretto considerare il protocollo RIP come un protocollo a livello di applicazione.

Tuttavia, è necessario sottolineare che l'utilizzo del protocollo UDP non sia necessario, bensì solo una comodità a livello di implementazione.



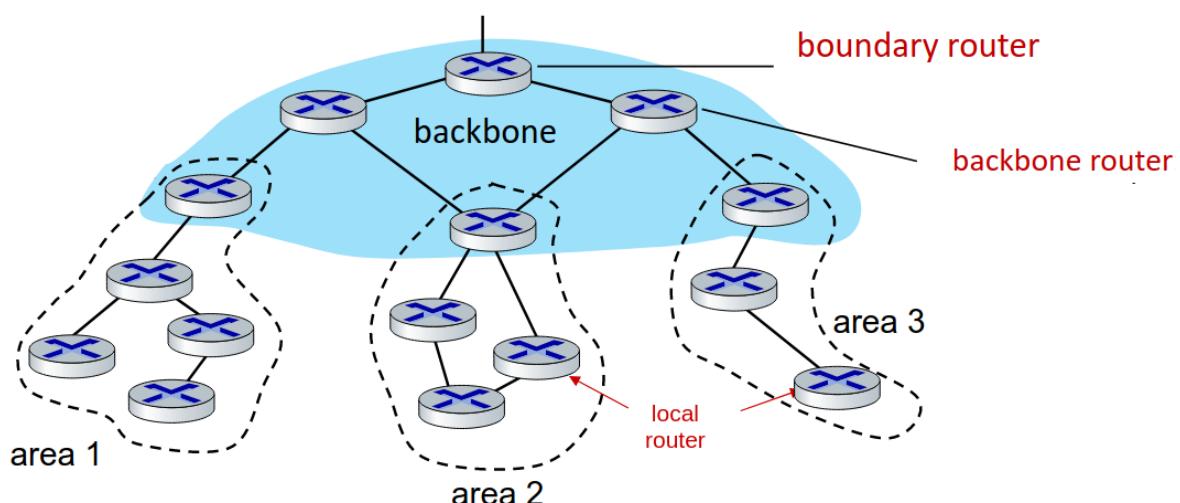
### Definition 41. Protocollo OSPF

Il protocollo Open Shortest Path First (OSPF) è un protocollo open-source di instradamento intra-AS basato sull'**algoritmo link-state**.

Per gestire il costo dei singoli link, vengono utilizzate **più metriche possibili** (es: larghezza di banda, ritardo, ...). Inoltre, tutti i messaggi OSPF sono **autenticati** per prevenire intrusioni.

Il protocollo OSPF utilizza una **gerarchia a due livelli**, composta da una **backbone** e varie **local area**:

- Gli annunci link-state vengono propagati solo nella backbone o all'interno di un'area locale, riducendo la quantità di messaggi in base alla gerarchia
- Ogni nodo conosce, a seconda di dove si trova, la **topologia dettagliata** della propria area o del backbone, mentre conosce solo la **direzione** necessaria per raggiungere le altre destinazioni
- I router vengono distinti in quattro tipologie:
  - **Backbone router**, situato all'interno del backbone, esegue la propagazione solo all'interno del backbone
  - **Local router**, situato all'interno di un'area locale, esegue la propagazione solo all'interno dell'area stessa
  - **Boundary router**, ossia il backbone router tramite cui l'intero AS si connette ad altri AS (gateway router)
  - **Area border router**, situato sia nel backbone sia all'interno di un'area locale (punto di scambio), "riepiloga" le distanze verso le altre destinazioni nella propria area e le pubblica nel backbone



## 4.8.2 Protocollo BGP

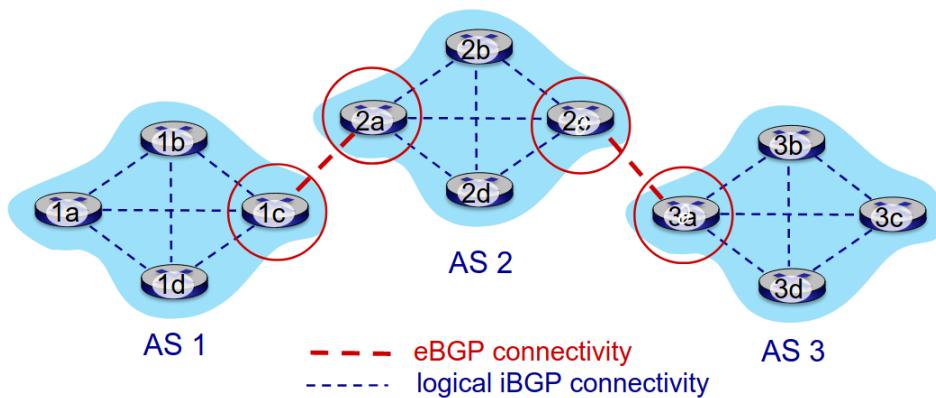
### Definition 42. Protocollo BGP

Il **protocollo Border Gateway Protocol (BGP)** è un protocollo di **istradamento inter-AS** basato sull'algoritmo path-vector (non visto precedentemente).

Consente ad un'AS di pubblicizzare alle altre AS la propria esistenza e le destinazioni che essa può raggiungere.

Il protocollo BGP fornisce due tipologie di connettività ad ogni AS:

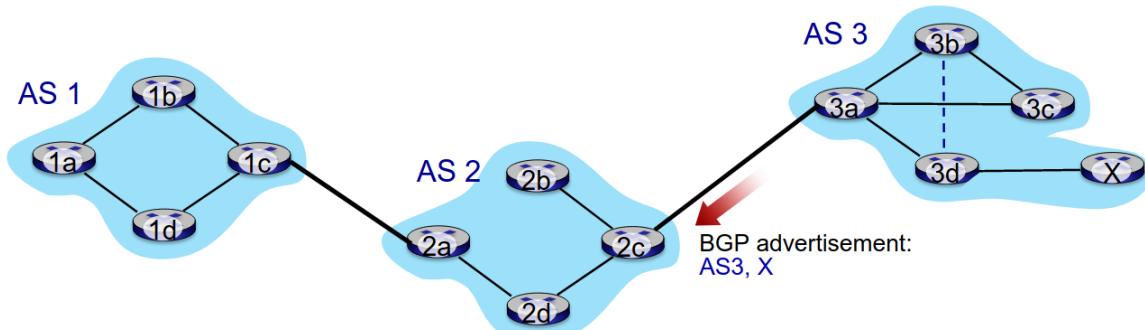
- **eBGP (external BGP)**, permettendo di ottenere informazioni sulla raggiungibilità di una sottorete tramite gli AS vicini
- **iBGP (internal BGP)**, permettendo di propagare tali informazioni sulla raggiungibilità a tutti i router interni all'AS



All'interno di una **sessione BGP**, due router BGP (detti *peer*) si scambiano messaggi BGP su una connessione TCP semipermanente, pubblicizzando i percorsi verso diversi prefissi di rete di destinazione.

Esempio:

- Quando il gateway 3a di AS3 annuncia il percorso AS3, X al gateway 2c di AS2, l'AS3 promette ad AS2 di inoltrare tutti i datagrammi diretti verso X



I messaggi BGP vengono scambiati tramite **connessioni TCP** e possono essere di quattro tipologie:

- **OPEN**, dove viene aperta una connessione TCP tra due peer BGP, autenticando prima il peer che apre la connessione
- **UPDATE**, dove viene pubblicizzato un nuovo percorso o ritirato uno precedente
- **KEEPALIVE**, dove viene richiesto di mantenere viva la connessione in assenza di messaggi UPDATE (viene utilizzato anche come ACK per il messaggio OPEN)
- **NOTIFICATION**, dove vengono segnalati errori nei messaggi precedenti (viene utilizzato anche per chiudere la sessione)

Per quanto riguarda i **percorsi BGP pubblicizzati**, essi sono composti da un prefisso ed una serie di attributi:

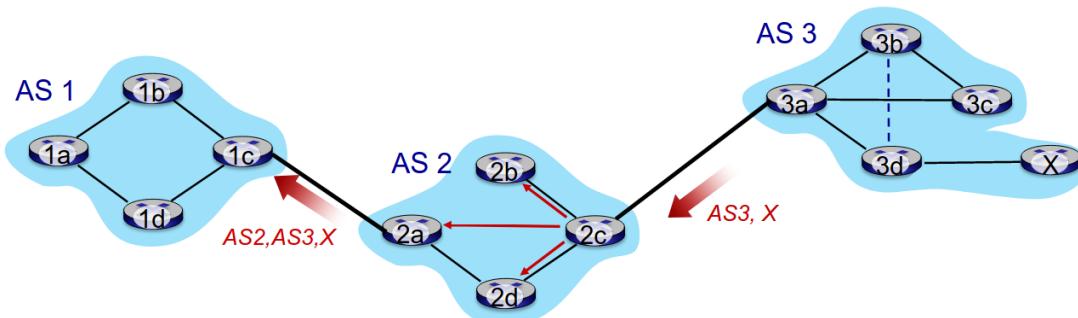
- Il **path prefix**, ossia la destinazione che viene pubblicizzata dall'AS mittente (in formato *ciderized*)
- L'attributo **AS-PATH**, contenente l'elenco di AS attraverso cui è passato l'annuncio, utilizzato dall'AS destinatario come percorso per raggiungere l'AS mittente
- L'attributo **NEXT-HOP**, contenente l'indirizzo dell'hop successivo dell'AS destinatario per poter raggiungere il gateway, ossia l'**egress router**, (es: corrispondente al router 2c nell'esempio precedente)

Alla ricezione di un percorso pubblicizzato, il router destinatario sceglie se **accettare** o **rifiutare** il percorso in base ad una propria politica (**policy-based routing**). Ad esempio, una politica di routing potrebbe essere basata sul rifiutare qualsiasi percorso passante attraverso un determinato AS o un determinato paese (ulteriore utilizzo dell'attributo AS-PATH).

Se un percorso viene accettato, esso viene **propagato** all'interno dell'AS, affinché i router interni ne siano a conoscenza, e verso le **altre AS raggiungibili**.

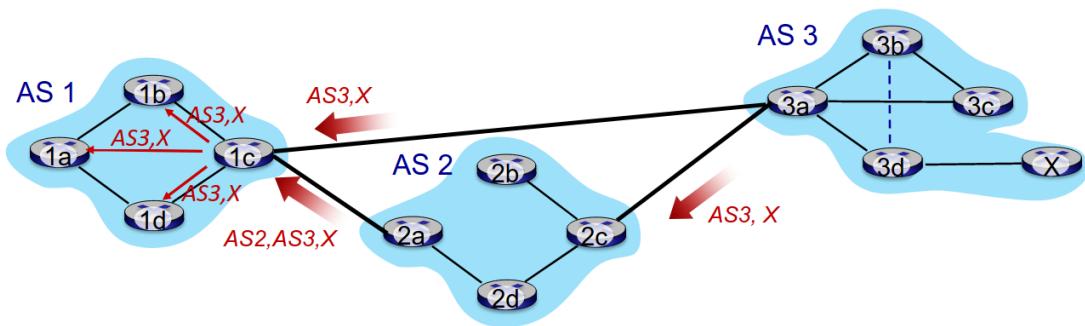
**Esempi:**

1. Consideriamo la seguente situazione:



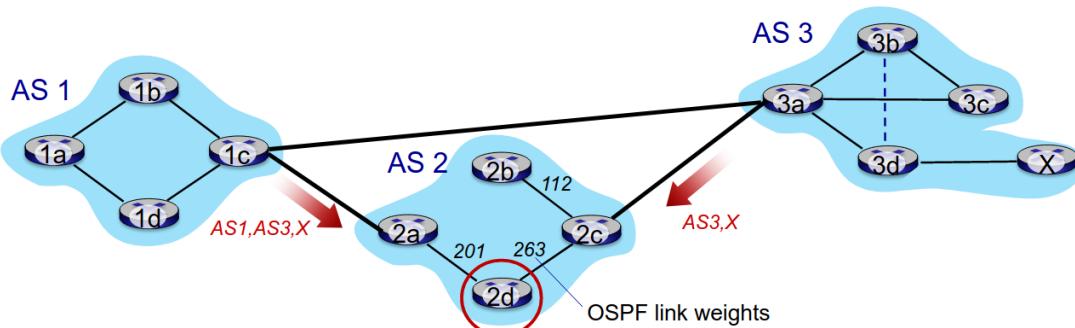
- Il router 2c di AS2 riceve (tramite eBGP) l'annuncio del percorso AS3, X dal router 3a di AS3.
- Basandosi sulla propria politica, il router 2c accetta il percorso e lo propaga (tramite iBGP) all'interno del proprio AS
- Successivamente, basandosi sempre sulla propria politica, il router 2c annuncia (tramite eBGP) il percorso AS2, AS3, X al router 1c di AS1

2. Consideriamo la seguente situazione (separata dalla precedente):



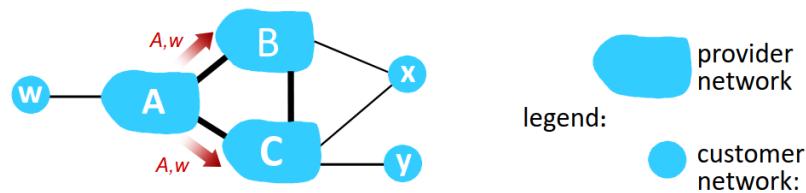
- Il router 1c di AS1 apprende il percorso AS2, AS3, X da parte del router 2a di AS2 e il percorso AS3, X da parte del router 3a di AS3
- Basandosi sulla propria politica, il router 1c decide di accettare il percorso AS3, X e rifiutare il percorso AS2, AS3, X (es: poiché necessita meno hop), propagando il percorso all'interno del suo AS

3. Consideriamo la seguente situazione (separata dalla precedente):



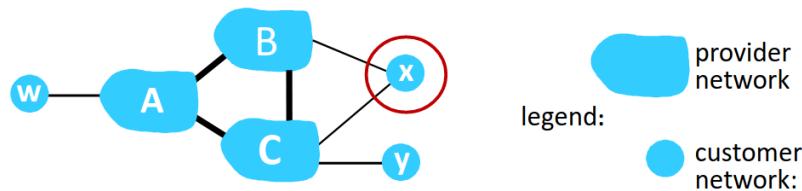
- Il router 2d di AS2 apprende (tramite iBGP) la possibilità di raggiungere il router X di AS3 sia tramite il router 2a sia tramite il router 2c (utilizzo dell'attributo NEXT-HOP)
- In tal caso, il router 2d sceglierà il gateway locale avente il minor costo intra-AS (**hot potato routing**) nonostante il percorso passante tramite 2c abbia un numero di hop inferiore, favorendo l'utilizzo di minor traffico all'interno di AS1 al prezzo di avere un minor controllo sul traffico esterno

4. Consideriamo la seguente situazione (separata dalla precedente):



- L'AS dell'ISP A pubblicizza il percorso A, w agli AS degli ISP B e C
- Poiché l'ISP B non trae alcun vantaggio per l'instradamento C, B, A, w (poiché nè C, nè A e nè w sono clienti di B), decide di non pubblicizzare tale percorso verso C (policy basata sull'*egoismo*)
- Di conseguenza, l'ISP C apprenderà solo il percorso C, A, w ricevuto da A stesso

5. Consideriamo la seguente situazione (separata dalla precedente):



- L'AS X è **dual-homed**, ossia connesso a due ISP
- Poiché B e C sono già direttamente connessi, per evitare il transito di traffico tra di essi passando attraverso l'AS x, quest'ultimo non pubblicherà il percorso C, x, B e il percorso B, x, C (policy basata sulla rimozione di intermediari tra ISP)

### Proposition 8. Scelta dei percorsi BGP

Se un router apprende più di un percorso verso la stessa destinazione, verrà selezionato il percorso in base a:

- Attributo del valore di preferenza locale
- AS-PATH più breve
- Percorso verso il NEXT-HOP con peso minore (**hot-potato routing**)
- Criteri aggiuntivi dettati dalla policy

## 4.9 Tipologie di instradamento

### 4.9.1 Unicast e Broadcast

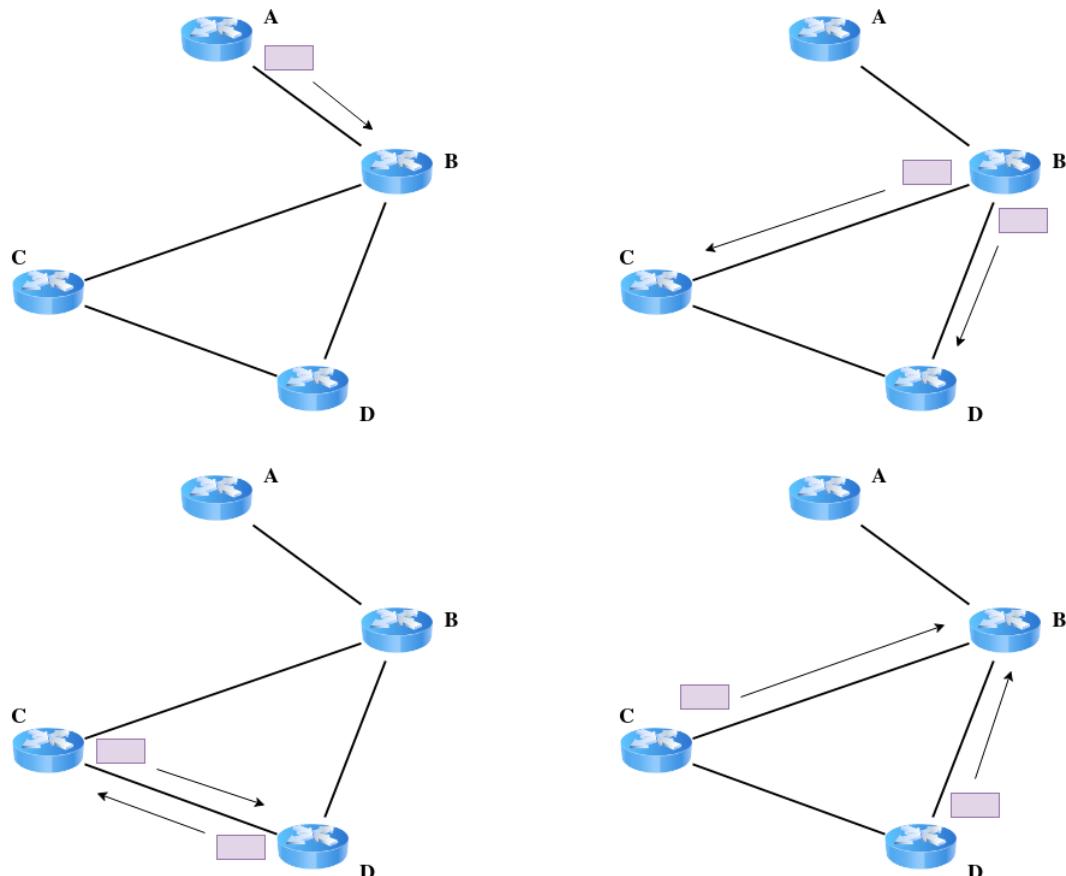
#### Definition 43. Unicast e Broadcast

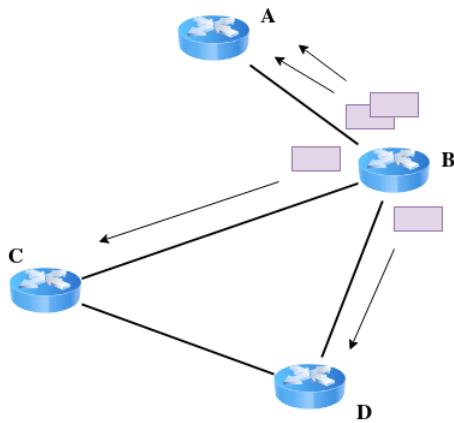
Nell'ambito delle comunicazioni in rete, definiamo come:

- **Unicast** la comunicazione tra **una sorgente ed una destinazione**, solitamente effettuata tramite la coppia <IP sorgente, IP destinazione>
- **Broadcast** la comunicazione tra **una sorgente e tutti i nodi di una rete**, solitamente effettuata tramite la coppia <IP sorgente, IP broadcast destinazione> (es: come già discusso, l'IP speciale 255.255.255.255 effettua il broadcast sulla rete locale)

Alla ricezione di un pacchetto broadcast da parte di un nodo, esso verrà **duplicato** ed inviato su tutti i nodi adiacenti al ricevente, fatta eccezione del nodo tramite cui è stato ricevuto il pacchetto. Tale tipologia di invio di messaggi viene detto **uncontrolled flooding** (tradotto *inondazione incontrollata*).

L'utilizzo dell'uncontrolled flooding può portare ad un **grave peggioramento della rete**, soprattutto nel caso in cui vi siano **cicli nel grafo**, portando il pacchetto broadcast ad essere duplicato ed inviato all'infinito.





Di conseguenza, è necessario utilizzare una strategia di **controlled flooding** affinché si possa ridurre il traffico sulla rete:

- **Sequence number controlled flooding**, dove ogni nodo contiene una lista dei pacchetti già ricevuti, duplicati ed inviati, inoltrando il pacchetto broadcast ricevuto solo se non è già stato inviato
- **Reverse path forwarding (RPF)**, dove il pacchetto broadcast ricevuto viene inoltrato solo se è stato inoltrato dal link appartenente al **percorso più breve verso la sorgente** dell'invio



Nonostante le due strategie eliminino il problema di inondare la rete di pacchetti all'infinito, esse non eliminano completamente la trasmissione di pacchetti ridondanti, poiché essi verranno comunque inviati/ricevuti più volte prima di essere scartati.

Per risolvere definitivamente la ridondanza dei pacchetti, viene utilizzato uno **spanning tree**, ossia un albero in cui ogni nodo può essere raggiunto da un solo link, propagando i pacchetti broadcast **solamente all'interno dell'albero stesso**.



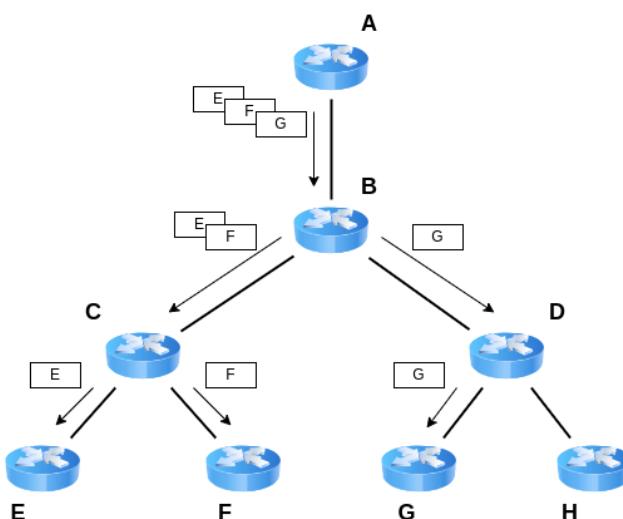
Per creare lo spanning tree, viene scelto un **nodo radice** come centro della rete. Successivamente, ogni altro nodo invierà un messaggio di **join** in modalità unicast verso la radice. Tale messaggio viene propagato finché esso non arriva ad un nodo che già appartiene all'albero o finché non arriva alla radice. Una volta "toccato" l'albero, il percorso mancante verrà aggiunto allo spanning tree.

#### 4.9.2 Multicast

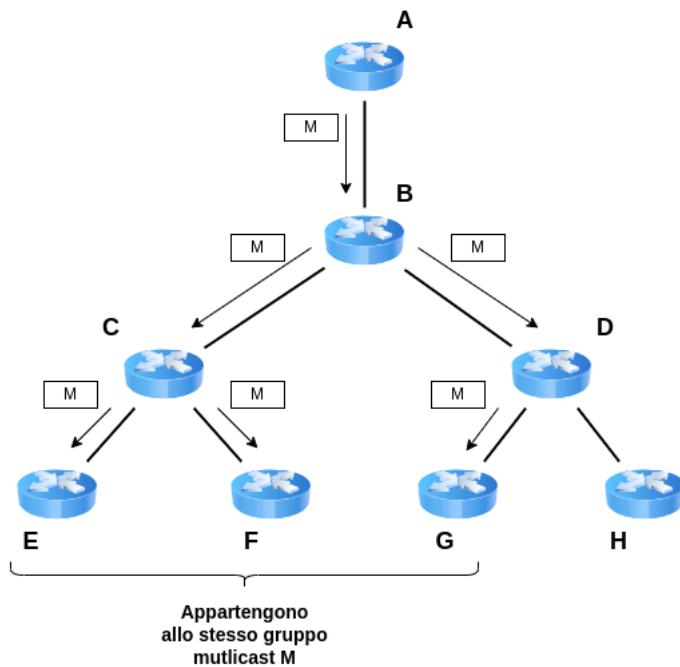
##### Definition 44. Multicast

Nell'ambito delle comunicazioni in rete, definiamo come **Multicast** la comunicazione tra **una sorgente e un gruppo di nodi della rete**

Molte applicazioni richiedono il trasferimento di pacchetti da uno o più mittenti verso un gruppo di destinatari (es: il trasferimento di un aggiornamento verso un gruppo di macchine, streaming ad un gruppo di utenti, ...). Effettuare tali trasferimenti utilizzando dei **pacchetti unicast multipli** risulta essere **estremamente inefficiente** per via dell'aggiunta di ritardi nella rete.



La soluzione più ottimale, dunque, risulta essere quella di trattare l'insieme di destinatari come un **gruppo multicast**, necessitando di un singolo pacchetto che verrà man mano sdoppiato per poter raggiungere tutte le destinazioni.



Tuttavia, poiché il protocollo IP è in grado di gestire un singolo indirizzo IP di destinazione, è necessario identificare tutti i membri del gruppo attraverso un **indirizzo multicast** (aggiuntivo rispetto al normale indirizzo IP).

In particolare, viene utilizzato un **blocco di indirizzi riservati** per il multicast. Per l'IPv4, ad esempio, il blocco di indirizzi da 224.0.0.0 a 239.255.255.255 ( $2^{28}$  gruppi possibili). Dunque, qualsiasi **indirizzo IP secondario** "appartenente alla rete" 224.0.0.0/4 viene considerato come un indirizzo multicast valido (dunque qualsiasi indirizzo nel formato 1110-**identificatore gruppo-**)



Dunque, l'appartenenza ad un gruppo multicast non ha alcuna relazione con il prefisso associato alla rete. Inoltre, l'appartenenza ad un gruppo è **variabile** (ad esempio il gruppo potrebbe avere un periodo di appartenenza limitato).

Pertanto, un router deve essere in grado di venire a conoscenza di quali gruppi siano raggiungibili su ciascuna delle sue interfacce per poter propagare l'informazione.

#### Definition 45. Protocollo IGMP

Il **protocollo Internet Group Management Protocol (IGMP)** è un protocollo di comunicazione utilizzato per offrire agli host la possibilità di comunicare al proprio router direttamente connesso la volontà di **aderire** ad uno specifico **gruppo multicast**.

I messaggi del protocollo IGMP (inviai con TTL pari a 1) si suddividono in:

- **Membership query**, inviato dal router agli host per determinare a quali gruppi multicast hanno aderito gli host (inviai periodicamente)
- **Membership request**, inviato da un host al router per informarlo dell'adesione ad un gruppo multicast
- **Leave group**, inviato da un host al router per informarlo dell'abbandono di un gruppo multicast

Ogni router multicast mantiene una **lista** per ciascuna sottorete di gruppi multicast (a patto che almeno un elemento del gruppo faccia parte della sottorete) impostando un **timer** per ogni **membership**. Se la membership non viene aggiornata (da request o leave) prima dello scadere del tempo, essa viene rimossa dalla lista.

Fra la popolazione complessiva di router, solo alcuni di essi, in particolare quelli collegati agli host del gruppo multicast, si occuperanno del traffico multicast (**multicast router**). Di conseguenza, è necessario un protocollo che coordini i vari router multicast per instradare il traffico multicast all'interno di Internet.

Per realizzare ciò, viene mantenuto un **albero** che colleghi i vari router multicast, instradando il traffico multicast solamente all'interno dell'albero stesso. Un albero può essere unico per tutto il gruppo o diverso a seconda della sorgente.

I principali protocolli per l'instradamento multicast sono:

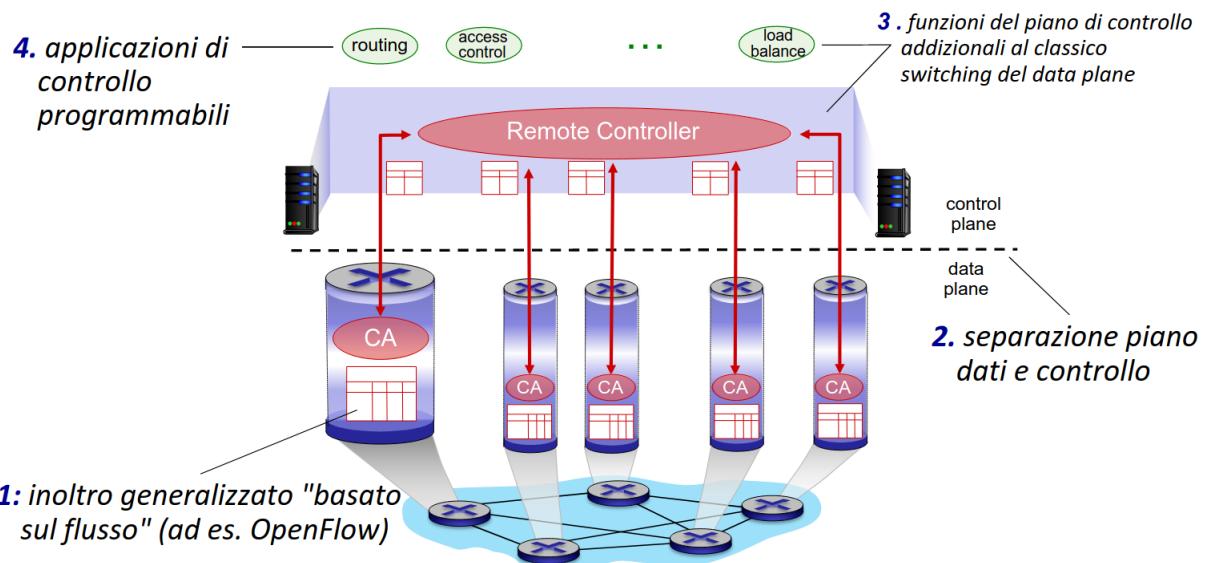
- **Instradamento multicast intra-AS:**
  - Distance-vector multicast routing protocol (DVMRP)
  - Multicast open shortest path first (MOSPF)
  - Protocol independent multicast (PIM)
- **Instradamento multicast inter-AS:**
  - Multicast border gateway protocol (MBGP)

## 4.10 Software Defined Networking (SDN)

Come precedentemente trattato, il livello di rete è stato storicamente implementato tramite un approccio di controllo distribuito sui router:

- Un **router monolitico** contiene hardware di commutazione, esegue implementazioni proprietarie dei protocolli standard Internet (es: IP, RIP, OSPF, BGP, ...) su sistemi operativi proprietari (es: Cisco IOS, ...)
- Diversi **middleboxes** per diverse funzionalità aggiuntive del livello di rete: firewall, load balancing, NAT, ...

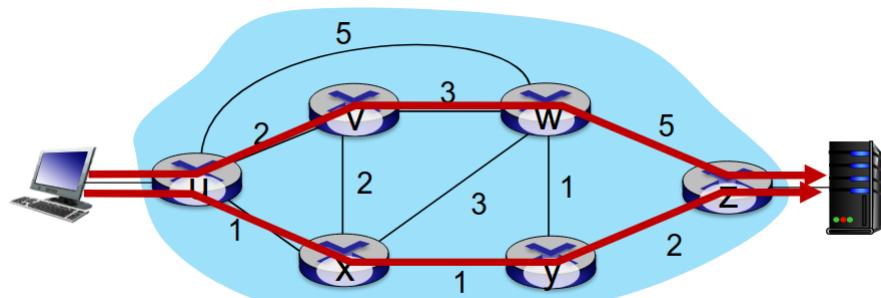
A differenza di un piano di controllo basato sull'approccio distribuito tra i vari router, dunque, il **Software Defined Networking (SDN)** permette l'implementazione di un **singolo piano di controllo** tramite un controller remoto che calcola e poi installa le tabelle di inoltro tramite le **API OpenFlow**, permettendo una gestione della rete più semplice, evitando errori di configurazione dei router e permettendo una **maggior flessibilità dei flussi di traffico**.



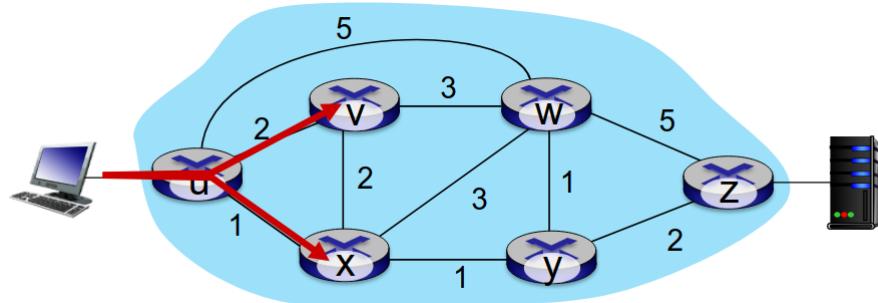
36

Esempi:

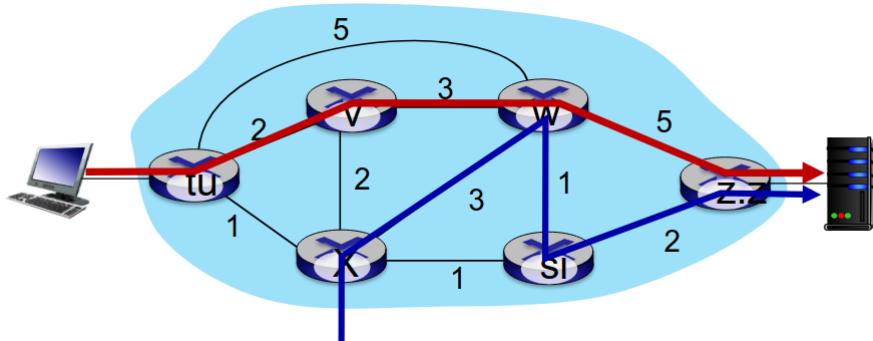
1. • L'ISP vuole far sì che il traffico dal router  $u$  verso il router  $z$  scorra sul percorso  $u, v, w, z$  anziché sul percorso  $u, x, y, z$ .



- Per ottenere ciò, utilizzando il normale approccio distribuito, sarebbe necessario ridefinire i pesi dei collegamenti in modo che l'algoritmo di instradamento del traffico calcoli il percorso desiderato.
  - Alternativamente, sarebbe necessario realizzare un nuovo algoritmo di routing.
2. • L'ISP vuole far sì che il traffico dal router  $u$  verso il router  $z$  venga bilanciato (**load balancing**) sui percorsi  $u, v, w, z$  e  $u, x, y, z$ .



- Utilizzando il normale approccio distribuito, ciò sarebbe impossibile se non tramite un nuovo algoritmo di routing.
- 3. • Il router  $w$  vuole instradare il traffico blu verso il router  $z$  e il traffico rosso verso il router  $z$  tramite due percorsi diversi



- Utilizzando il normale approccio distribuito, ciò sarebbe impossibile se non tramite una tipologia di forwarding diversa dal destination-based forwarding e un nuovo algoritmo di routing.

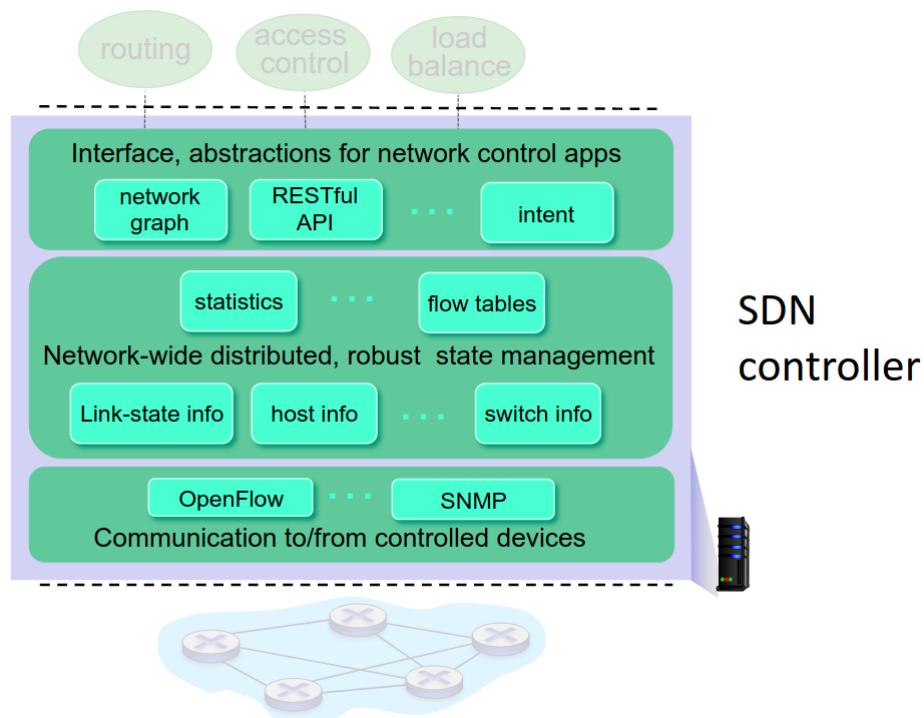
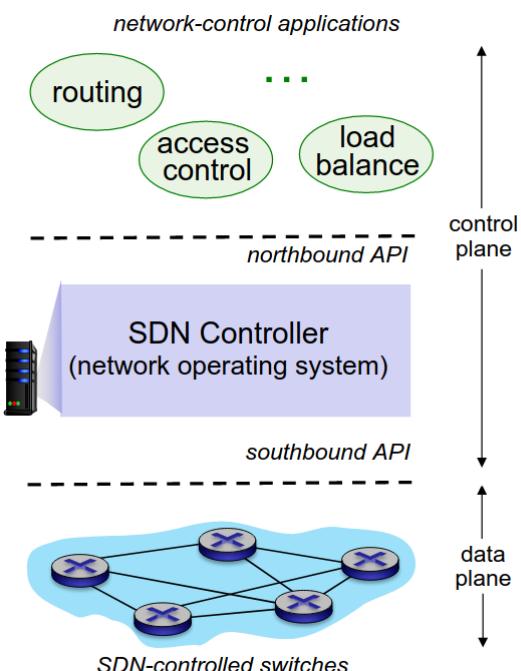
Tramite l'uso di un SDN, inoltre, il forwarding può essere realizzato tramite **switch di rete** veloci e semplici (al posto di normali router più complessi), i quali implementano il **generalized forwarding** all'interno del data plane, dove la **forwarding table** degli switch viene calcolata e installata sotto la supervisione del controller SDN tramite le API OpenFlow e un protocollo per la comunicazione con il controller.

Per quanto riguarda le **applicazioni di controllo della rete** presenti all'interno del control plane, invece, esse implementano funzioni di controllo utilizzando i servizi di livello inferiore (ossia le API fornite dal controller SDN). Possono essere fornite da un fornitore distinto rispetto a quello degli switch e del controller SDN.

Il **controller SDN** viene gestito da un sistema operativo di rete, mantenendo informazioni sullo stato della rete e interagendo con gli altri livelli attraverso delle API:

- **API Northbound**, utilizzate per interagire con le applicazioni di controllo della rete presenti nel control plane
- **API Southbound**, utilizzate per interagire con gli switch di rete all'interno del data plane tramite le **API Southbound**

Per evitare la presenza di un **single point of failure**, ossia un dispositivo il cui malfunzionamento porterebbe al malfunzionamento dell'intera rete, i controller SDN vengono implementati come **sistema distribuito**



#### Definition 46. Protocollo OpenFlow

Il **protocollo OpenFlow** è un protocollo di comunicazione utilizzato per la comunicazione tra controller SDN e switch di rete attraverso il **protocollo TCP** (con crittografia opzionale).

**Attenzione:** il protocollo OpenFlow è **diverso** dalle API OpenFlow, nonostante quest'ultime vengano utilizzate dal protocollo stesso.

I messaggi del protocollo OpenFlow si suddividono in tre categorie:

- **Controller-to-switch:**

- Messaggi di **feature**, ossia una query del controller per conoscere le funzionalità supportate dallo switch
- Messaggi di **configure**, dove il controller modifica parametri di configurazione dello switch
- Messaggi di **modify-state**, dove vengono utilizzate le API OpenFlow per aggiungere, eliminare o modificare campi della forwarding table dello switch
- Messaggi di **packet-out**, dove il controller invia un pacchetto da una specifica porta dello switch

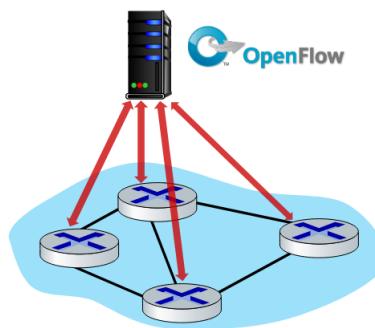
- **Asincroni (Switch-to-controller):**

- Messaggi di **packet-in**, dove viene trasferito un pacchetto al controller
- Messaggi di **flow-removed**, dove lo switch elimina una riga della forwarding table e notifica il controller
- Messaggi di **port-status**, dove lo switch informa il controller della modifica o problematica su una porta

- **Simmetrici (C-to-S & S-to-C)**

- Messaggi di hello, messaggi echo, messaggi di errore, ...

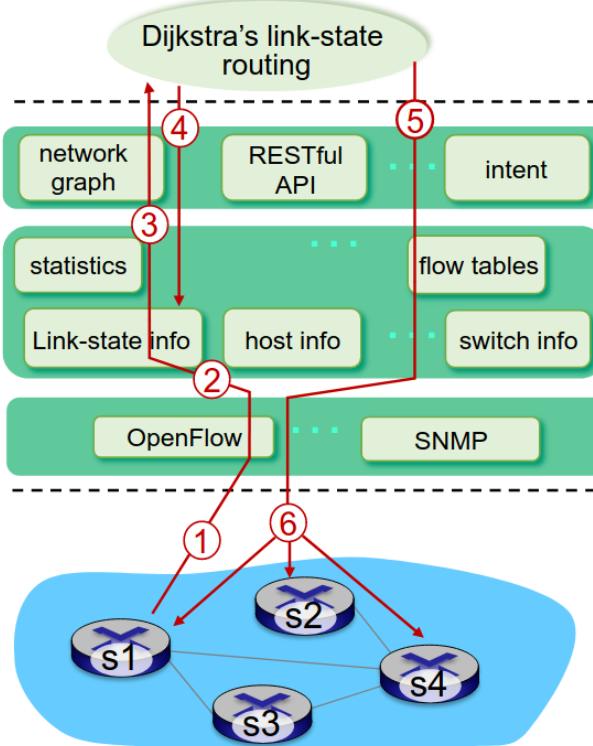
### Controller OpenFlow



### Esempio di interazione piano dati/controllo:

1. All'interno dello switch di rete S1 si verifica un errore sul collegamento verso lo switch di rete S2. Di conseguenza, lo switch S1 invia un messaggio OpenFlow di port-status per informare il controller
2. Il controller SDN riceve il messaggio OpenFlow, aggiornando le informazioni sullo stato del collegamento
3. L'applicazione di controllo della rete inerente al calcolo dei percorsi tramite l'algoritmo link-state di Dijkstra viene richiamata

4. L'applicazione accede alle informazioni sul grafo di rete e alle informazioni sullo stato dei collegamenti, calcolando i nuovi percorsi
5. L'applicazione di routing interagisce con il componente di calcolo delle forwarding table presente all'interno del controller SDN, calcolando le nuove forwarding table degli switch di rete necessarie
6. Il controller utilizza il protocollo OpenFlow e le API OpenFlow per installare le nuove tabelle negli switch che devono essere aggiornati



Per via della sua complessità di gestione, l'utilizzo dei controller SDN è attualmente confinato ai singoli AS, venendo quindi utilizzati come **"sostituto"** del normale **routing intra-AS tradizionale**. Gli obiettivi futuri, dunque, prevedono una maggiore scalabilità tramite la sostituzione anche del routing inter-AS, nonché una maggior robustezza ai guasti ed una maggior affidabilità/sicurezza (versioni aggiornate di OpenFlow usano l'autenticazione).

## 4.11 Amministrazione della rete

L'**amministrazione della rete** prevede la gestione dei vari AS distribuiti all'interno di Internet attraverso quattro componenti fondamentali:

- **Managing server**, ossia un server tipicamente gestito da amministratori della rete
- **Managed device**, ossia un qualsiasi dispositivo della rete con componenti hardware o software configurabili
- **Dati** (es: dati di configurazione dello stato dei dispositivi, dati operativi, statistiche dei dispositivi, ...)
- **Protocollo di network management**, utilizzato dal managing server per interrogare, configurare e gestire i managed device e utilizzato da quest'ultimi per inviare dati o eventi rilevati al server

### Definition 47. Management Information Base (MIB)

Un **Management Information Base (MIB)** è un database presente all'interno di un managed device memorizzante dati sullo stato e la configurazione del dispositivo stesso attraverso il linguaggio **Structure of Management Information (SMI)**

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPIInDatagrams	32-bit counter	total # datagrams delivered
1.3.6.1.2.1.7.2	UDPNoPorts	32-bit counter	# undeliverable datagrams (no application at port)
1.3.6.1.2.1.7.3	UDInErrors	32-bit counter	# undeliverable datagrams (all other reasons)
1.3.6.1.2.1.7.4	UDPOutDatagrams	32-bit counter	total # datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port currently in use

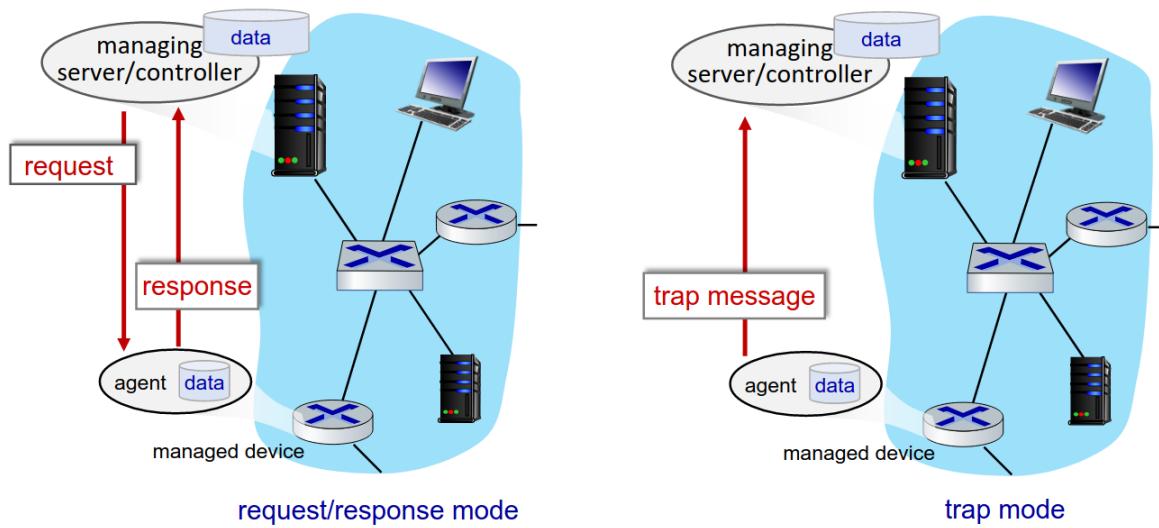
*Esempio di variabili MIB per il protocollo UDP*

### Definition 48. Protocollo SNMP

Il **protocollo Simple Network Management Protocol (SNMP)** è un protocollo di gestione della rete utilizzato per interrogare/impostare i dati presenti nei MIB dei dispositivi. Viene implementato tramite il **protocollo UDP** sulla porta nota 161.

Message type	Function
GetRequest GetNextRequest GetBulkRequest	manager-to-agent: "get me data" (data instance, next data in list, block of data).
SetRequest	manager-to-agent: set MIB value
Response	Agent-to-manager: value, response to Request
Trap	Agent-to-manager: inform manager of exceptional event

I messaggi del protocollo SNMP si differenziano in **messaggi request/response**, dove il server invia una richiesta al dispositivo e quest'ultimo risponde, e **messaggi trap**, dove il dispositivo informa il server a seguito di un'eccezione.



#### Definition 49. Protocollo NETCONF

Il **protocollo Network Configuration Protocol (NETCONF)** è un protocollo di gestione della rete utilizzato per gestire/configurare **attivamente** i dispositivi a livello di rete.

Il protocollo NETCONF sul **paradigma di remote procedure call (RPC)**, inviando messaggi NETCONF codificati in linguaggio XML attraverso un protocollo di trasporto sicuro (es: tramite TLS).

Inoltre, il protocollo NETCONF è in grado di recuperare, modificare, interrogare e attivare configurazioni sui managed devices attraverso dei **commit atomici** su più dispositivi (ossia un singolo commit in grado di modificare simultaneamente tutti i dispositivi)

NETCONF	Operation Description
<get-config>	Retrieve all or part of a given configuration. A device may have multiple configurations.
<get>	Retrieve all or part of both configuration state and operational state data.
<edit-config>	Change specified (possibly running) configuration at managed device. Managed device <rpc-reply> contains <ok> or <rpccerror> with rollback.
<lock>, <unlock>	Lock (unlock) configuration datastore at managed device (to lock out NETCONF, SNMP, or CLIs commands from other sources).
<create-subscription>, <notification>	Enable event notification subscription from managed device

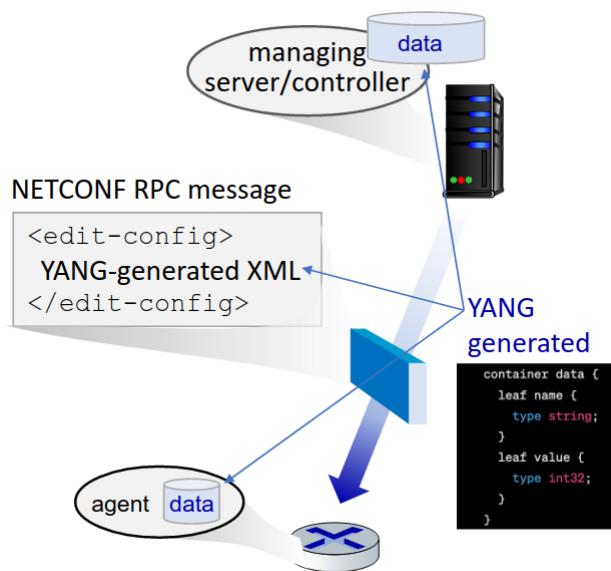
**Esempio:**

```

01 <?xml version="1.0" encoding="UTF-8"?>
02 <rpc message-id="101" note message id
03   xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
04     <edit-config> change a configuration
05       <target>
06         <running/> change the running configuration
07       </target>
08     <config>
09       <top xmlns="http://example.com/schema/
10         1.2/config">
11           <interface>
12             <name>Ethernet0/0</name> change MTU of Ethernet 0/0 interface to 1500
13             <mtu>1500</mtu>
14           </interface>
15         </top>
16       </config>
17     </edit-config>
18   </rpc>

```

Per facilitare la scrittura di messaggi NETCONF RPC, viene utilizzato il **linguaggio di modellazione YANG**. In particolare, ogni documento XML descrivente il dispositivo e le sue funzionalità può essere generato a partire da una descrizione YANG, esprimendo anche vincoli tra dati che devono essere soddisfatti da una configurazione NETCONF valida.



# Capitolo 5

## Livello di collegamento

### 5.1 Panoramica del livello di collegamento

Abbiamo visto come il livello di rete si occupi della comunicazione logica tra dispositivi. Per quanto riguarda il **livello di collegamento**, invece, esso si occupa direttamente del **trasferimento dei datagrammi** tra due dispositivi fisicamente adiacenti lungo un link, ossia un qualsiasi canale di comunicazione tra i due nodi stessi (cablato o non).

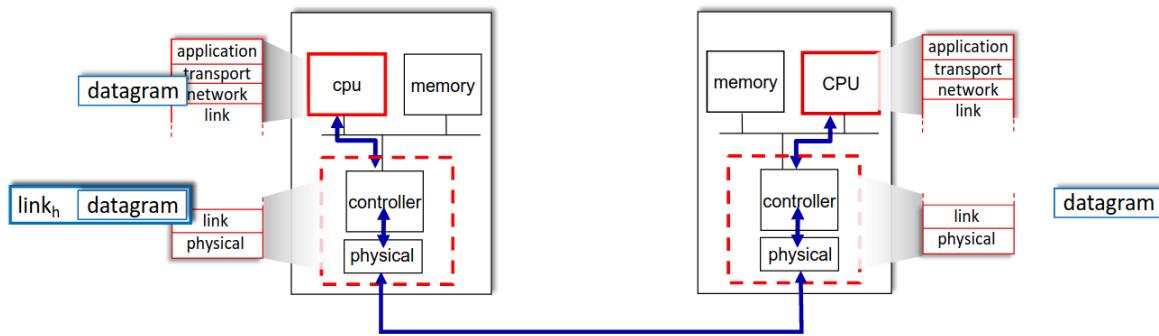
In particolare, il trasferimento di datagrammi tra più dispositivi **non richiede** strettamente **l'uso dello stesso protocollo**. Ad esempio, due dispositivi A e B potrebbero essere collegati da un cavo Ethernet, mentre il dispositivo B potrebbe essere collegato ad un dispositivo C tramite Wi-Fi.

Ogni protocollo di collegamento fornisce servizi diversi, tra cui:

- **Framing**, dove il datagramma viene incapsulato in un frame aggiungendo un header ed un trailer
- **Link access**, dove viene fornito accesso al canale di trasmissione tramite un mezzo condiviso. Gli **indirizzi MAC** nell'header dei frame identificano origine e destinazione (diversi dagli indirizzi IP)
- **Consegna affidabile tra nodi adiacenti**, in modo simile alla consegna affidabile dei dati già vista precedentemente per il livello di trasporto
- **Controllo del flusso**, evitando il sovraccarico dei buffer del nodo di destinazione
- **Rilevamento degli errori**, causati da attenuazione del segnale o da rumore presenti nel mezzo di trasmissione. Alla rilevazione di un errore, il ricevitore può richiedere la trasmissione o scartare direttamente il frame.
- **Correzione degli errori**, dove il ricevente identifica e corregge automaticamente errori presenti nei bit, senza richiedere la ritrasmissione.
- **Half duplex e Full duplex**, dove con il termine half duplex viene intesa una **trasmissione bidirezionale ma non contemporanea**, mentre con il termine full duplex viene intesa una **trasmissione bidirezionale e contemporanea**

Il livello di collegamento viene implementato in **ogni singolo dispositivo** attraverso una **scheda di interfaccia di rete (Network Interface Card - NIC)**, o anche attraverso un semplice chip di rete. La NIC è direttamente collegata ai bus di sistema del dispositivo ed è gestita da una combinazione tra hardware, software e firmware.

Durante una trasmissione, il dispositivo mittente incapsula il datagramma nel frame ed allega ad esso dei **bit aggiuntivi** utilizzati per i **servizi** del livello di collegamento (dunque controllo degli errori, trasferimento affidabile, ...), per spedire il frame stesso tramite la propria NIC. Una volta che la NIC del destinatario riceverà il frame, verranno effettuati i controlli necessari (dunque sempre controllo degli errori, trasferimento affidabile, ...) per poi decapsulare il frame estraendo il datagramma e passandolo al livello superiore.



In modo simile al livello di rete, anche il livello di collegamento è diviso in **due sottolivelli**:

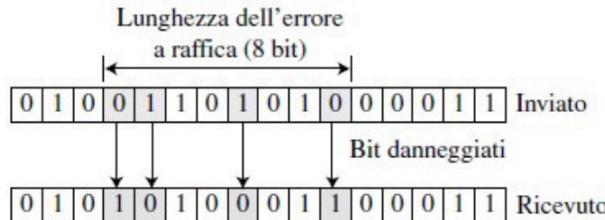
- Il **Data Link Control (DLC)** si occupa di tutte le questioni condivise sia dai **collegamenti point-to-point**, dunque dedicati a due dispositivi, sia da quelli **broadcast**, dunque condivisi tra più dispositivi.

In particolare, il DLC si occupa di servizi come il framing, il controllo del flusso, il rilevamento di errori e la loro correzione.

- Il **Media Access Control (MAC)** si occupa solo degli aspetti specifici dei **canali broadcast**, in particolare del controllo dell'accesso al mezzo condiviso

## 5.2 Rilevamento e correzione degli errori

Gli errori presenti nei frame spediti sono dovuti a interferenze che possano cambiare la forma del segnale. La probabilità che avvenga un errore di tipo **burst** (**a raffica, ossia in sequenza**) è più elevata rispetto a quella di un singolo errore, in quanto la durata dell'interferenza (detta anche rumore) normalmente è più lunga rispetto alla trasmissione di un singolo bit.



Pertanto, il **numero di bit coinvolti** nell'errore dipende dalla **velocità di trasferimento** dei dati e dalla **durata del rumore** (es: un rate pari a 1 Kb/s con un rumore di 0.01 s può influire su 10 bit).

Per rilevare errori nella trasmissione vengono utilizzati dei bit di **error detection and correction** (**EDC bits**), i quali vengono allegati ai dati protetti dal controllo (possono includere anche i campi stessi dell'header). Nonostante sia molto raro che non vengano correttamente rilevati gli errori, è necessario sottolineare che tale procedura non è affidabile al 100%. In particolare, maggiore sarà il numero di EDC bits utilizzati maggiore sarà la capacità di rilevare e correggere l'errore.

Il primo metodo utilizzato per la rilevazione degli errori è il **parity checking**:

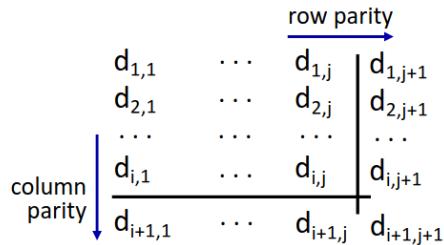
- Viene utilizzato un singolo EDC detto **parity bit**, il quale verrà impostato in modo che il **numero totale di bit impostati ad 1** (incluso il parity bit stesso) sia **pari**
- Di conseguenza, se il numero di bit impostati ad 1 all'interno del campo dati è **dispari**, il parity bit verrà impostato ad 1
- Viceversa, se il numero di bit impostati ad 1 all'interno del campo dati è **pari**, il parity bit verrà impostato ad 0
- Una volta giunto a **destinazione**, viene calcolato nuovamente il valore che deve essere assunto dal parity bit. Se tale valore **non coincide** con il parity bit inserito nel campo EDC, verrà rilevato un errore



Tuttavia, è necessario sottolineare che tale protocollo permetta solo di **rilevare in singolo errore** all'interno della trasmissione senza sapere quale sia il bit effettivamente errato, rendendo **impossibile la correzione automatica** dell'errore.

Una strategia più avanzata prevede l'uso di **parity bit bidimensionali**:

- I bit del campo data vengono disposti in una tabella  $m \times n$
- Per ognuna delle  $m$  righe ed ognuna delle  $n$  colonne viene calcolato il parity bit
- Viene calcolato un parity bit (posto in basso a destra) per tutti gli  $m \times n$  bit del dato originale (dunque esclusi gli  $m + n$  parity bit appena calcolati)



In questo modo, gli  $m \times n$  bit di parità vengono utilizzati per **rilevare e correggere i singoli errori**, mentre il parity bit finale calcolato viene utilizzato per assicurarsi che nessuno di tali parity bit sia errato.

no errors:    1 0 1 0 1   1 1 1 1 1 0   0 0 1 1 1 0   1 0 0 1 0 1   0	<b>detected and correctable single-bit error:</b> 1 0 1 0 1   1 1 0 1 1 0   0      parity error 0 1 1 1 0   1 0 0 1 0 1   0      parity error
--	---

Nonostante la sua buona efficacia vista la sua semplicità, il parity checking con parity bit bidimensionali risulta essere comunque soggetto a molti **errori di rilevazione** (es: possono verificarsi situazioni in cui vi sono più bit errati ma il conteggio di parità risulta essere comunque corretto).

Una codifica di rilevamento degli errori (dunque non correzione) più complessa ma di maggior efficacia è il **Cyclic Redundancy Check (CRC)**, ampiamente utilizzato nella pratica (es: Ethernet, Wi-Fi 802.11):

1. I bit di dati vengono trattati come un numero binario, indicato come  $D$
2. Viene scelto un valore  $r$ , corrispondente al numero di bit da utilizzare per il campo CRC del frame
3. Viene scelto un valore  $G$ , detto **generator**, costituito da  $r + 1$  bit. Il generatore da utilizzare viene scelto dai due endpoint tra una serie di generatori standard, dunque entrambi ne sono a conoscenza.
4. Il valore assunto dal campo CRC corrisponde ad un **valore  $R$**  di  $r$  bit. Posto  $\langle D, R \rangle := (D \cdot 2^r) \oplus R$ , il valore  $R$  deve essere tale che  **$\langle D, R \rangle$  sia esattamente divisibile per  $G$  in modulo 2**, dunque tale che

$$\frac{\langle D, R \rangle}{G} \equiv 0 \pmod{2} \iff \frac{(D \cdot 2^r) \oplus R}{G} \equiv 0 \pmod{2} \iff \\ \iff \exists n \in \mathbb{Z} \mid (D \cdot 2^r) \oplus R \equiv nG \pmod{2}$$

5. A questo punto, è necessario sottolineare che nell'algebra modulo 2 (diversa dall'algebra binaria), le operazioni di somma, sottrazione e XOR siano **algebricamente equivalenti**. Tale dettaglio è di cruciale importanza, poiché altrimenti calcolando la divisione in algebra binaria si otterrebbe un risultato sbagliato.

6. Dunque, il valore  $R$  corrisponde al **resto della divisione in modulo 2 di  $\frac{D \cdot 2^r}{G}$** .

$$R \equiv \frac{D \cdot 2^r}{G} \pmod{2}$$

Inoltre, ricordiamo che  $D \cdot 2^r$  equivale ad effettuare su  $D$  uno **shift sinistro di  $r$  bit**.

7. Pertanto, notiamo che i bit del valore  $\langle D, R \rangle$  corrispondono sempre ai bit del valore  $D$  a cui vengono accodati i bit del valore  $R$ . Tale proprietà nasce direttamente dal fatto stesso che  $\langle D, R \rangle = (D \cdot 2^r) \oplus R$ , motivo per cui all'interno dei frame il valore CRC venga accodato al campo dati
8. Una volta ricevuto il frame, il destinatario utilizzerà il valore  $\langle D, R \rangle$  ricevuto per verificare se  $\frac{\langle D, R \rangle}{G} \equiv 0 \pmod{2}$ . Se il resto ottenuto è diverso da 0, verrà rilevato l'errore. In particolare, possono essere rilevati tutti gli errori burst inferiori a  $r + 1$  bit

### Esempio:

- Vogliamo utilizzare un CRC a 3 bit utilizzando il generatore  $G = 1001_2$
- Dato  $D = 101110_2$  (dunque  $D \cdot 2^3 = 101110000_2$ ), calcoliamo  $\frac{D \cdot 2^3}{G}$  in modulo 2 (ricordiamo che in tale modulo lo XOR e la sottrazione sono equivalenti)

$$\begin{array}{r}
 \begin{array}{ccccccccc}
 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
 \oplus & 1 & 0 & 0 & 1 & & & & \\
 \hline
 & 1 & 0 & 1 & 0 & & & & \\
 \oplus & 1 & 0 & 0 & 1 & & & & \\
 \hline
 & 1 & 1 & 0 & 0 & & & & \\
 \oplus & 1 & 0 & 0 & 1 & & & & \\
 \hline
 & 1 & 0 & 1 & 0 & & & & \\
 \oplus & 1 & 0 & 0 & 1 & & & & \\
 \hline
 & 1 & 1 & & & & & & \\
 \end{array}
 \end{array}
 \left| \begin{array}{cccccc}
 1 & 0 & 0 & 1 \\
 \hline
 1 & 0 & 1 & 0 & 1 & 1
 \end{array} \right.$$

implicando che  $R = 011_2$  e dunque che  $\langle D, R \rangle = 101110011_2$  (notare che esso corrisponde all'accodamento del valore  $R$  al valore  $D$ )

## 5.3 Collegamenti e protocolli MAC

Come accennato nella panoramica del livello di collegamento, principalmente vi sono due tipologie di collegamento:

- Collegamento **point-to-point**, ossia dedicati solo a due dispositivi (es: un cavo Ethernet moderno)
- Collegamento **broadcast**, ossia tramite mezzo condiviso tra dispositivi (es: un cavo condiviso, una radio condivisa, ...)

Nel caso dei collegamenti broadcast, possono verificarsi **due o più trasmissioni simultanee** da parte dei nodi, creando **interferenza** e **collisioni** nel caso in cui un nodo riceva due o più segnali contemporaneamente.

Di conseguenza, è necessario utilizzare dei **protocolli di accesso multiplo**, dunque inerenti al sotto-livello **Media Access Control (MAC)** accennato precedentemente, ossia algoritmi distribuiti in grado di determinare come i nodi condividono un mezzo di trasmissione, dettando quando ogni nodo possa trasmettere.

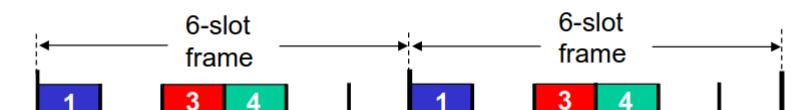
Inoltre, è necessario sottolineare che lo **scambio di messaggi** relativo al protocollo MAC utilizzato debba **utilizzare il canale stesso**. Pertanto, dato un canale di accesso multiplo di velocità  $R$  b/s, vogliamo (idealmente) che:

- Qualora un nodo voglia trasmettere, esso deve poter trasmettere alla velocità  $R$  b/s
- Qualora  $M$  nodi vogliono trasmettere, ognuno di essi può trasmettere ad una **velocità media** pari a  $\frac{R}{M}$  b/s
- Il protocollo deve essere **decentralizzato**, dunque non deve esserci alcun nodo speciale che coordini la trasmissione e non deve esserci alcuna sincronizzazione di orologi o slot temporali

### 5.3.1 Protocolli MAC a partizionamento del canale

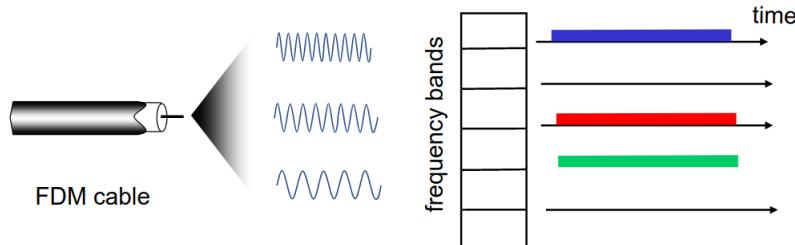
La prima macrocategoria di protocolli MAC è composta dai protocolli basati sul **partizionamento dei canali**, dove il canale viene suddiviso in più parti, allocando ognuna di esse ad un nodo per uso esclusivo:

- **Time Division Multiple Access (TDMA)**, basato sullo stesso principio del Time Division Multiplexing (TDM) visto nel capitolo 1, dove l'accesso al canale viene effettuato in "round": ogni stazione ottiene uno **slot di tempo di accesso al canale** fisso in ogni round e ogni slot inutilizzato diventa inattivo



*LAN a 6 stazioni dove le stazioni 1, 3 e 4 devono inviare pacchetti mentre gli slot 2, 5 e 6 sono inattivi*

- **Frequency Division Multiple Access (FDMA)**, basato sullo stesso principio del Frequency Division Multiplexing (FDM) visto nel capitolo 1, dove lo spettro del canale è suddiviso in bande di frequenza, ciascuna assegnata ad una stazione in modo fisso. Il tempo di trasmissione inutilizzato nelle bande di frequenza diventa inattivo.



*Esempio analogo al precedente ma utilizzando il FDMA invece del TDMA*

- **Code Division Multiple Access (CDMA)**, dove un solo canale occupa l'intera ampiezza di banda e tutte le stazioni possono inviare contemporaneamente (assenza di suddivisione di frequenze e di tempo), utilizzando dei codici personali per effettuare la comunicazione.

I codici scelti all'interno del **CDMA** si basano sulle **sequenze ortogonali**, dove ad ogni stazione viene assegnato un codice, corrispondente ad una sequenza di numeri, detti **chip**.

#### Proposition 9. Proprietà delle sequenze ortogonali

Le **sequenze ortogonali** sono basate sull'ortogonalità tra vettori dell'algebra lineare, godendo delle seguenti proprietà:

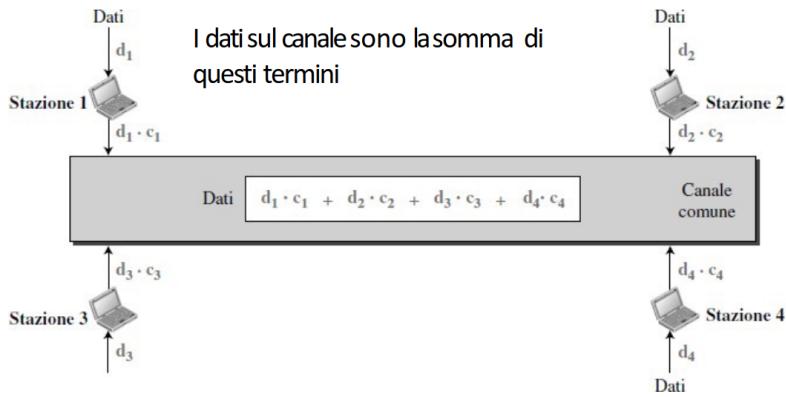
- Ogni codice è una sequenza composta da  $N$  elementi (dove  $N$  è il numero di stazioni ed è una potenza di 2)
- **Sommare/moltiplicare due sequenze** significa sommare/moltiplicare l' $i$ -esimo elemento della prima sequenza con l' $i$ -esimo elemento della seconda sequenza
- Tra due sequenze può essere effettuato il **prodotto scalare**, equivalente a moltiplicare le due sequenze e sommare gli  $N$  valori ottenuti
- Moltiplicando una sequenza per un **numero**, ogni elemento della sequenza viene moltiplicato per tale numero
- Effettuando il **prodotto scalare** tra due sequenze **uguali** il risultato sarà esattamente  $N$ , mentre se esse sono **diverse** il risultato sarà esattamente 0

Se all'interno della rete CDMA una sola delle seguenti proprietà non viene rispettata, le sequenze ortogonali associate ai dispositivi sono **incorrecte**.

**Esempio:**

- Consideriamo le seguenti sequenze ortogonali:
  - $c_1 = [+1, +1, +1, +1]$
  - $c_2 = [+1, -1, +1, -1]$
  - $c_3 = [+1, +1, -1, -1]$
  - $c_4 = [+1, -1, -1, +1]$
- Verifichiamo se si tratti di sequenze ortogonali valide (verificando quindi le ultime due proprietà):
  - Moltiplicazione sequenze uguali e somma dei valori:
    - \*  $c_1 \cdot c_1 = [+1, +1, +1, +1] \cdot [+1, +1, +1, +1] = [+1, +1, +1, +1]$   
 $\Rightarrow 1 + 1 + 1 + 1 = 4$
    - \*  $c_2 \cdot c_2 = [+1, -1, +1, -1] \cdot [+1, -1, +1, -1] = [+1, +1, +1, +1]$   
 $\Rightarrow 1 + 1 + 1 + 1 = 4$
    - \*  $c_3 \cdot c_3 = [+1, +1, -1, -1] \cdot [+1, +1, -1, -1] = [+1, +1, +1, +1]$   
 $\Rightarrow 1 + 1 + 1 + 1 = 4$
    - \*  $c_4 \cdot c_4 = [+1, -1, -1, +1] \cdot [+1, -1, -1, +1] = [+1, +1, +1, +1]$   
 $\Rightarrow 1 + 1 + 1 + 1 = 4$
  - Moltiplicazione sequenze diverse e somma dei valori:
    - \*  $c_1 \cdot c_2 = [+1, +1, +1, +1] \cdot [+1, -1, +1, -1] = [+1, -1, +1, -1]$   
 $\Rightarrow 1 - 1 + 1 - 1 = 0$
    - \*  $c_1 \cdot c_3 = [+1, +1, +1, +1] \cdot [+1, +1, -1, -1] = [+1, +1, -1, -1]$   
 $\Rightarrow 1 + 1 - 1 - 1 = 0$
    - \*  $c_1 \cdot c_4 = [+1, +1, +1, +1] \cdot [+1, -1, -1, +1] = [+1, -1, -1, +1]$   
 $\Rightarrow 1 - 1 - 1 + 1 = 0$
    - \*  $c_2 \cdot c_3 = [+1, -1, +1, -1] \cdot [+1, +1, -1, -1] = [+1, -1, -1, +1]$   
 $\Rightarrow 1 - 1 - 1 + 1 = 0$
    - \*  $c_2 \cdot c_4 = [+1, -1, +1, -1] \cdot [+1, -1, -1, +1] = [+1, +1, -1, -1]$   
 $\Rightarrow 1 + 1 - 1 - 1 = 0$
    - \*  $c_3 \cdot c_4 = [+1, +1, -1, -1] \cdot [+1, -1, -1, +1] = [+1, -1, +1, -1]$   
 $\Rightarrow 1 - 1 + 1 - 1 = 0$
- Le quattro sequenze sono ortogonali tra loro, implicando che possano essere utilizzate per il CDMA tra quattro stazioni

Tramite l'utilizzo delle **sequenze ortogonali**, prima di ogni trasmissione ogni stazione **moltiplica** i propri dati per il proprio codice. In tal modo, i dati sul canale corrispondono alla **somma di tali risultati**.



Qualsiasi stazione voglia ricevere dati da una delle altre stazioni, **moltiplica** i dati ricevuti per il codice del mittente e divide per il numero di **stazioni**, ottenendo così i dati originali.

$$\begin{aligned}
 \text{Dati della Staz. 1} &= \frac{(d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \cdot c_1}{4} = \\
 &= \frac{d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1}{4} = \\
 &= \frac{d_1 \cdot 4 + d_2 \cdot 0 + d_3 \cdot 0 + d_4 \cdot 0}{4} = \frac{d_1 \cdot 4}{4} = d_1
 \end{aligned}$$

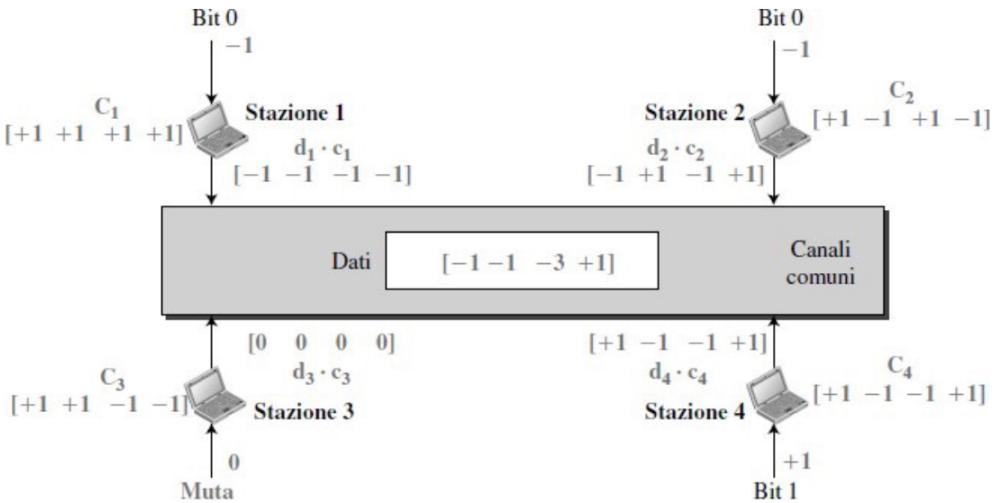
Al fine di poter applicare tale calcolo, dunque, è necessario **codificare i dati** sottoforma di sequenza di  $N$  elementi:

- Se il dato  $d$  ottenuto dal calcolo è  $-1$ , tale dato verrà interpretato come un **bit uguale a 0**
- Se il dato  $d$  ottenuto dal calcolo è  $+1$ , tale dato verrà interpretato come un **bit uguale a 1**
- Se il dato  $d$  ottenuto dal calcolo è  $0$ , tale dato verrà interpretato come **silenzio**

### Esempio:

- Consideriamo le quattro stazioni aventi le seguenti sequenze ortogonali viste precedentemente:
  - $c_1 = [+1, +1, +1, +1]$
  - $c_2 = [+1, -1, +1, -1]$
  - $c_3 = [+1, +1, -1, -1]$
  - $c_4 = [+1, -1, -1, +1]$
- Supponiamo che la sequenza presente sul canale, corrispondente alla somma dei prodotti scalari effettuati, sia  $D = [-1, -1, -3, +1]$
- Il bit inviato dalla stazione S2 corrisponderà a:

$$\frac{D \cdot c_2}{4} = \frac{[-1, -1, -3, +1] \cdot [+1, -1, +1, -1]}{4} = \frac{-4}{4} = -1 \implies \text{Bit}_{S2} = 0$$



Per **generare sequenze di chip** viene utilizzata una **matrice di Walsh**, ossia una matrice  $2^n \times 2^n$  per  $n \in \mathbb{N}$  e dove le entrate sono solo -1 o +1:

- Ogni riga della matrice è una sequenza di chip
- La matrice  $W_1$  di dimensione  $1 \times 1$  è una sequenza di un chip solo e può assumere (a scelta) il valore +1 o -1

$$W_1 = (\pm 1)$$

- Dato un  $N$  qualsiasi, la matrice  $W_{2N}$  di dimensione  $2N \times 2N$  viene calcolata tramite la matrice  $W_N$ :

$$W_{2N} = \begin{pmatrix} W_N & W_N \\ W_N & \overline{W_N} \end{pmatrix}$$

dove  $\overline{W_N}$  è la matrice complementare di  $W_N$  (ossia avente valori di segno inverito)

### Esempio:

- Scelto  $W_1 = (+1)$ , la matrice  $W_2$  corrisponderà a:

$$W_2 = \begin{pmatrix} W_1 & W_1 \\ W_1 & \overline{W_1} \end{pmatrix} = \begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}$$

- Una volta ottenuta  $W_2$ , la matrice  $W_4$  corrisponderà a:

$$W_4 = \begin{pmatrix} W_2 & W_2 \\ W_2 & \overline{W_2} \end{pmatrix} = \begin{pmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{pmatrix}$$

- Le sequenze ortogonali  $c_1, c_2, c_3$  e  $c_4$  per 4 stazioni saranno quindi date dalle righe della matrice  $W_4$

### 5.3.2 Protocolli MAC ad accesso casuale

La seconda macrocategoria di protocolli MAC è composta dai protocolli basati sull'**accesso casuale**, dove nel momento in cui un nodo deve inviare un pacchetto esso viene direttamente inviato alla massima velocità di trasmissione  $R$  del link, per poi **rilevare** e recuperare da eventuali **collisioni**, ossia trasmissioni simultanee nel canale.

#### Definition 50. Protocollo Slotted ALOHA

Il **protocollo Slotted ALOHA** è un protocollo MAC ad accesso casuale, dove:

- Viene **assunto** che:
  - Tutti i **frame** abbiano la **stessa dimensione**
  - Il **tempo** è diviso in **slot di uguali dimensioni**, ognuno pari a  $T_{fr}$  ossia il **tempo impiegato per trasmettere un frame**
  - I nodi iniziano a trasmettere solo all'**inizio dello slot**. Inoltre, essi sono **sincronizzati** e, nel caso in cui due o più nodi trasmettono nello stesso slot di tempo, tutti i nodi rilevano la **collisione**
- Quando un nodo ottiene un nuovo frame, esso viene trasmesso nello **slot di tempo successivo**.
- Se non viene rilevata alcuna collisione, il nodo può inviare un nuovo frame nello slot successivo
- Se invece viene rilevata una collisione, il nodo tenta di ritrasmettere il frame a ogni slot successivo con **probabilità  $p$**  (dunque in modo casuale), fermandosi nel caso in cui la ritrasmissione avvenga



#### Pro dello Slotted ALOHA:

- Se un singolo nodo è attivo, esso può trasmettere continuamente alla massima velocità del canale
- Solo gli slot dei nodi devono essere sincronizzati (alta decentralizzazione)

#### Contro dello Slotted ALOHA:

- Presenza di collisioni, spreco di slot generale e presenza di slot inattivi a seguito di una collisione
- Sincronizzazione degli orologi dei nodi
- I nodi potrebbero essere in grado di rilevare la collisione in un tempo minore di uno slot di tempo

Per quanto riguarda l'**efficienza**, ossia la frazione a lungo termine di slot trasmessi con successo (assumendo molti nodi e molti frame), del protocollo Slotted ALOHA può essere stimata a livello probabilistico:

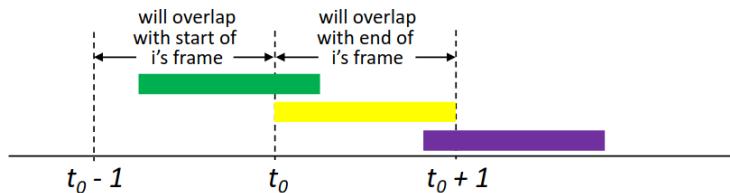
- Assumiamo  $N$  nodi con molti frame da inviare, ognuno trasmette in slot con probabilità  $p$
  - La probabilità che un dato nodo abbia successo in uno slot è  $p(1 - p)^{N-1}$
  - La probabilità che tutti i nodi abbiano successo è  $Np(1 - p)^{N-1}$
  - Dunque, per  $N$  nodi la massima efficienza è sarà data dal valore  $p^*$  in grado di massimizzare  $Np^*(1 - p^*)^{N-1}$  (spesso tale valore massimizzante è  $p^* \approx \frac{1}{N}$ )
  - Per molti nodi (dunque per  $N \rightarrow +\infty$ ) l'efficienza massima sarà:
- $$\lim_{N \rightarrow +\infty} Np^*(1 - p^*)^{N-1} \approx \lim_{N \rightarrow +\infty} N \frac{1}{N} \left(1 - \frac{1}{N}\right)^{N-1} = \lim_{N \rightarrow +\infty} \left(1 - \frac{1}{N}\right)^{N-1} = \frac{1}{e} \approx 0.37$$
- Dunque, il canale viene utilizzato per trasmissioni utili circa il 37% delle volte

### Definition 51. Protocollo Pure ALOHA

Il **protocollo Pure ALOHA** è una variante del protocollo Slotted ALOHA dove:

- Il tempo non è suddiviso in slot. Pertanto, non vi è alcuna sincronizzazione.
- Quando un frame arriva, esso viene trasmesso direttamente.
- Il resto rimane invariato rispetto al protocollo Slotted ALOHA

Per via dell'assenza di sincronizzazione, la probabilità di collisione risulta maggiore. Ad esempio, il frame inviato al tempo  $t_0$  andrà in collisione con i frame inviati nell'intervallo temporale  $[t_0 - 1, t_0 + 1]$  (**tempo di vulnerabilità** pari a  $2 \cdot T_{fr}$ )



Pertanto l'efficienza del Pure ALOHA, ossia circa 18% di trasmissioni utili, risulta essere inferiore rispetto all'efficienza dello Slotted ALOHA.

### Definition 52. Protocollo CSMA

Il **protocollo Carrier Sense Multiple Access (CSMA)** è un protocollo MAC ad accesso casuale dove:

- Prima di trasmettere, ogni nodo **ascolta il canale (Carrier Sense)**
- Se il canale viene rilevato come **inattivo**, viene trasmesso l'intero frame
- Se il canale viene rilevato come **attivo**, la trasmissione viene ritardata

Nonostante l'invio solo in caso di inattività del canale, all'interno del protocollo CSMA possono ancora verificarsi delle **collisioni**. Ad esempi, per via del ritardo di propagazione due nodi potrebbero entrambi rilevare il canale come libero in contemporanea, avviando entrambi la trasmissione.

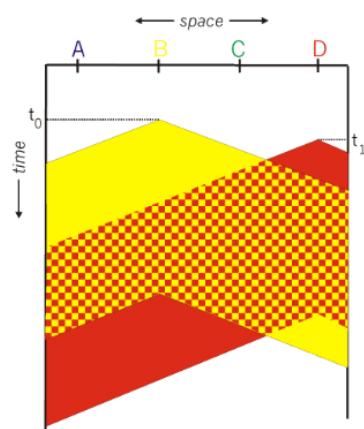
In particolare, dunque, la distanza dei nodi e il ritardo di propagazione giocano un ruolo nel determinare la probabilità di collisione, portando il **tempo di vulnerabilità** ad essere pari a  $D_p$  (propagation delay). Inoltre, nel caso di collisione il tempo di trasmissione dell'intero pacchetto viene **sprecato**.

### Definition 53. Protocollo CSMA/CD

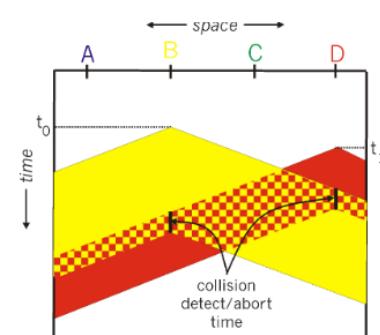
Il **protocollo Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** è una variante del protocollo CSMA:

- **Collision Detection:** viene rilevata una collisione se una stazione trasmittente riceve un bit da parte di un'altra stazione, **interrompendo immediatamente** la trasmissione, inviando un **segnale di jam** (ossia di avvenuta collisione) ed entrando in una fase di **back-off**, ossia l'attesa di un determinato quantitativo di tempo prima di riprendere ad ascoltare
- Il resto rimane invariato rispetto al protocollo CSMA (incluso il **tempo di vulnerabilità**)

**Collisione in CSMA**



**Collisione in CSMA/CD**



Una volta che una stazione A invia completamente un frame, essa **non controlla il mezzo trasmisivo** per rilevare eventuali collisioni con una stazione B. Affinché il Collision Detection funzioni, dunque, la stazione A deve poter **star ancora trasmettendo** al momento in cui riceverà il segnale di jam inviato dalla stazione B, poiché altrimenti A non sarebbe in grado di rilevare la collisione avvenuta.

Per tale motivo, il **tempo di trasmissione di un frame** deve essere **almeno due volte il delay di propagazione** (tempo massimo di andata e ritorno tra A e B), dunque  $T_{fr} \geq 2 \cdot D_p$ , affinché un nodo possa rilevare tutte le possibili collisioni.

Di conseguenza, per ottenere tale tempo di trasmissione minimo, la **dimensione di un frame** deve essere pari a:

$$\text{Dim. frame} = R_t \cdot T_{fr} \geq R_t \cdot 2 \cdot D_p$$

dove  $R_t$  è il rate di trasmissione

**Esempio:**

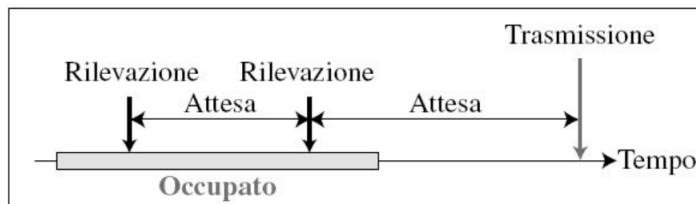
- Una rete che utilizza il CSMA/CD è composta da link cablati con un rate pari a 10 Mb/s. Se il delay di propagazione è  $25.6 \mu s$ , la dimensione minima del frame corrisponde a:

$$\text{Dim. frame} = R_t \cdot T_{fr} \geq R_t \cdot 2 \cdot D_p = 2 \cdot 10 \text{ Mb/s} \cdot 25.6 \mu s = 512 b = 64 B$$

Il protocollo CSMA/CD può essere implementato secondo più **politiche di gestione dell'ascolto del canale**:

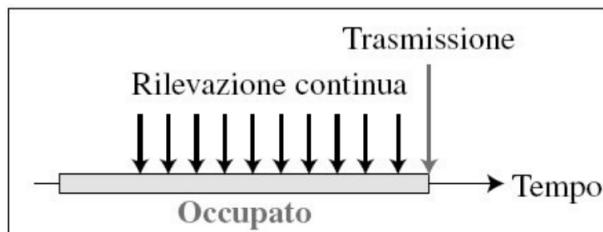
- **Non persistente:**

- Se il canale è libero, la trasmissione avviene subito
- Se il canale è occupato, viene atteso un tempo random per poi riascoltare il canale (carrier sense ad intervalli)
- Se si verifica una collisione la trasmissione viene interrotta (back-off)



- **1-persistente:**

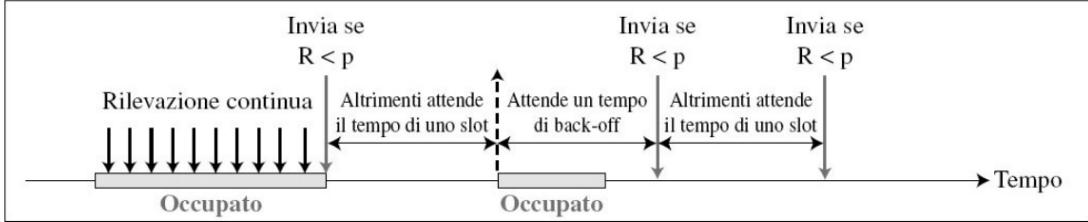
- Se il canale è libero, la trasmissione avviene subito
- Se il canale è occupato, l'ascolto del canale è continuo (carrier sense continuo)
- Se si verifica una collisione la trasmissione viene interrotta (back-off)



- **P-persistente (slottizzato):**

- Se il canale è libero, la trasmissione avviene con probabilità  $p$ , oppure viene atteso l'inizio del prossimo slot di tempo con probabilità  $1 - p$

- Se il canale è occupato, viene usata la procedura di back-off, ossia l'attesa di un tempo random e un nuovo ascolto del canale
- Se si verifica una collisione la trasmissione viene interrotta (back-off)



Il protocollo CSMA/CD viene implementato dal **protocollo Ethernet** tramite il seguente **algoritmo Ethernet CSMA/CD**:

1. La NIC di un nodo riceve un datagramma dal livello di rete e crea il frame
2. La NIC ascolta il canale: se è inattivo la trasmissione viene avviata, altrimenti viene atteso che il canale sia libero (politica **1-persistente**)
3. Se durante la trasmissione la NIC rileva un'altra trasmissione in arrivo, la NIC interrompe la trasmissione e invia un **segnale di jam** (48 bit) per avvisare tutte le altre NIC della collisione
4. Dopo l'interruzione, la NIC entra in stato di **back-off binario** dove, dopo l' $n$ -esima collisione di fila, la NIC sceglie un valore  $K$  casuale tra i valori  $\{0, 1, 2, \dots, 2^n - 1\}$  attendendo che  $K$  frame da parte di altre stazioni vengano trasmessi sul mezzo

Infine, per quanto riguarda l'**efficienza** del protocollo CSMA/CD, si ha che:

$$\text{Eff} = \frac{1}{1 + \frac{5 \cdot D_p}{D_t}}$$

Pertanto, l'efficienza massima, ossia pari a 1, viene raggiunta quando  $D_p \rightarrow 0$  o quando  $D_t \rightarrow +\infty$ . In condizioni ragionevoli, invece, l'efficienza media risulta essere 0.5, implicando che il canale venga utilizzato per trasmissioni utili circa il 50% delle volte.

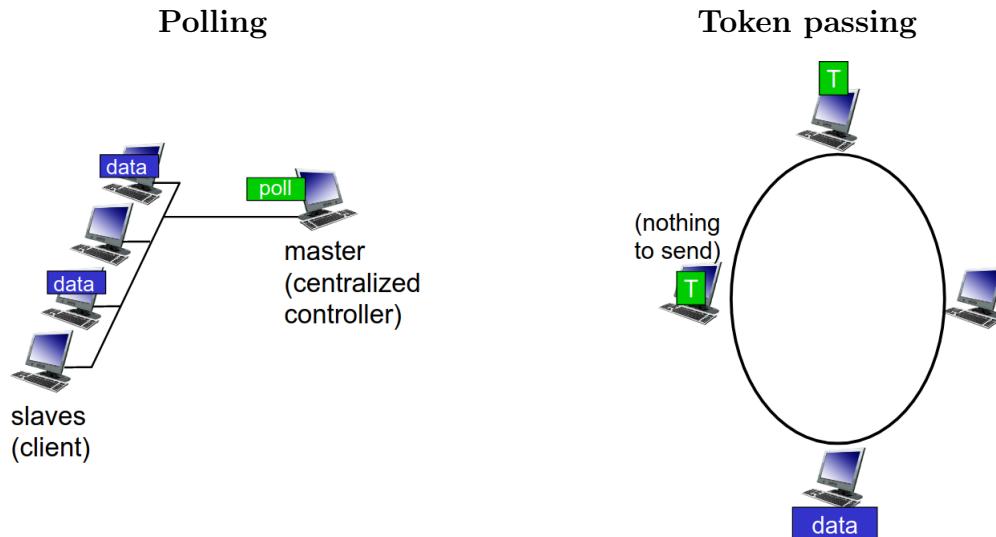
### 5.3.3 Protocollo MAC a rotazione

La terza macrocategoria di protocolli MAC è composta dai protocolli basati sulla **rotazione**, dove si cerca di ottenere una via intermedia tra le altre due macrocategorie (la prima è efficiente con carico elevato e poco efficiente con basso carico, mentre la seconda è efficiente con basso carico e poco efficiente con molto carico).

Le due principali tipologie di protocolli appartenenti a tale categoria sono:

- **Polling**, dove un nodo master "invita" a turno gli altri nodi a trasmettere (se un nodo non ha nulla da trasmettere si passa direttamente al prossimo). Viene tipicamente utilizzato con dispositivi semplici (dumb devices).

- **Token passing**, dove un token di controllo viene passato da un nodo all'altro in sequenza e dove ogni nodo può trasmettere solo se possiede il token.



Entrambe le tipologie presentano una **latenza di accesso** (nel primo dovuto all'attesa dell'invito e nel secondo all'attesa del token) ed un **single point of failure** (l'intero blocco del canale è dovuto nel primo ad un malfunzionamento del master e nel secondo a seguito della possibile perdita del token )

## 5.4 Indirizzamento locale (indirizzo MAC)

Abbiamo visto come l'**indirizzo IP** venga utilizzato come indirizzo dell'interfaccia del livello di rete per effettuare il forwarding.

L'**indirizzo MAC** (anche detto indirizzo LAN, fisico o Ethernet), è un indirizzo **utilizzato localmente** (dunque soltamente all'interno della stessa sottorete locale) per inviare frame da una NIC ad un'altra NIC **fisicamente connessa ad essa**.

Ogni indirizzo MAC è composto da **48 bit** ed è direttamente **hardcoded nella NIC**, rendendolo pertanto **globalmente univoco** (a differenza di IP che è solo localmente univoco). All'interno della stessa LAN, dunque, ogni interfaccia possiede:

- Indirizzo MAC globalmente univoco, paragonabile al codice fiscale dell'interfaccia
- Indirizzo IP localmente univoco, paragonabile all'indirizzo postale dell'interfaccia rendendo un'interfaccia spostabile da una LAN all'altra.

Per rappresentare gli indirizzi MAC viene utilizzata una **notazione esadecimale** composta da 12 caratteri in base 16 separati due a due da un trattino, dove ogni carattere rappresenta 4 bit dell'indirizzo (es: 1A-2F-BB-76-09-AD).

L'allocazione degli indirizzi MAC è gestita dalla IEEE, dove **ogni azienda produttrice di NIC** acquista un **Organizational Unique Identifier (OUI)** interno ai primi 12 bit più significativi, acquistando così uno spazio privato di indirizzi MAC al fine di garantire l'unicità.

**Chiarimento:** ci si potrebbe chiedere se non sia già sufficiente l'indirizzo IP per poter identificare un'interfaccia all'interno della stessa LAN, rendendo superfluo l'indirizzo MAC. Di seguito, vengono elencati alcuni motivi per cui sia **necessario** utilizzare un indirizzo MAC:

- Per struttura stessa dello stack protocollare TCP/IP, il livello di rete e di collegamento sono **completamente isolati**. Pertanto, il livello di collegamento non ha la minima idea di cosa sia un indirizzo IP
- La stessa **NIC** potrebbe essere associata a **più indirizzi IP** nel caso in cui essa appartenga a più reti (es: i gateway router che si interpongono come punto di scambio tra due reti). Pertanto, lavorare con più indirizzi può risultare complesso, mentre l'**unicità assoluta** dell'indirizzo MAC rende il tutto più semplice
- L'indirizzo IP spesso è ottenuto **dinamicamente** tramite il protocollo DHCP. Prima di ottenere tale indirizzo, dunque, gli altri dispositivi della LAN non potrebbero identificare il dispositivo che ha effettuato la richiesta al server DHCP. Inoltre, essendo dinamico, un host potrebbe cambiare il proprio indirizzo IP anche all'interno della stessa LAN (es: a seguito della disconnessione e riconnessione)
- Le **forwarding table** di un nodo servono solo a tener traccia del **flusso di rete**, permettendo ad un dispositivo di sapere su quale porta inviare il pacchetto, mentre l'indirizzo MAC permette di sapere quale dispositivo sia connesso a tale porta.

### 5.4.1 Protocollo ARP

#### Definition 54. Protocollo ARP

Il **protocollo Address Resolution Protocol (ARP)** è un protocollo di risoluzione degli indirizzi in grado di determinare l'indirizzo MAC di un'interfaccia richiesta tramite il suo indirizzo IP.

Ogni nodo appartenente alla LAN possiede una propria **tabella ARP**, formata da mappature nel formato < Indirizzo IP, Indirizzo MAC, TTL >. Allo scadere del TTL (solitamente 20 minuti), una mappatura viene rimossa dalla tabella.



All'interno del pacchetto ARP, il campo **hardware type** indica il protocollo di collegamento utilizzato, mentre il campo **protocol type** viene utilizzato per il demultiplexing con il livello di rete.

Hardware type (2 bytes)		Protocol type (2 bytes)
Hardware address length (1 byte)	Protocol address length (1 byte)	Operation code (2 bytes)
Source hardware address		
Source protocol address		
Target hardware address		
Target protocol address		

Per acquisire gli indirizzi MAC dei dispositivi connessi alla rete, un dispositivo effettua una **query ARP broadcast** utilizzando l'indirizzo MAC di destinazione FF-FF-FF-FF-FF-FF, in modo che il frame arrivi a tutti i dispositivi della LAN. Una volta ricevuta la query, il dispositivo il cui indirizzo IP coincide con l'indirizzo IP di destinazione presente nella query risponderà con il proprio indirizzo MAC.

#### Esempio:

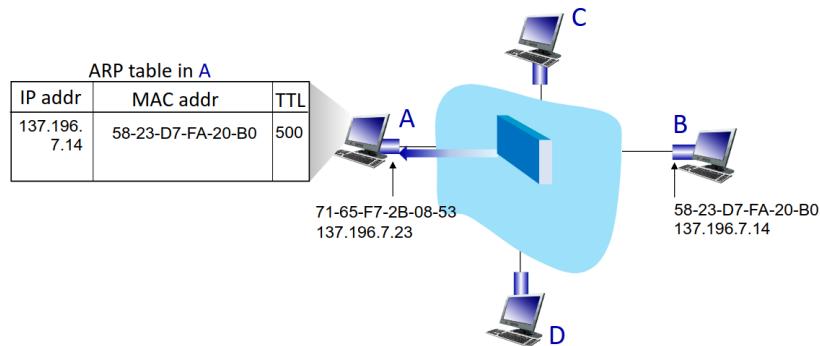
- L'host A vuole inviare un datagramma all'host B. Tuttavia, l'indirizzo MAC dell'host B non è nella tabella ARP dell'host A. L'host A trasmette quindi in broadcast una query ARP contenente l'indirizzo IP dell'host B.



- Una volta ricevuta la query, l'host B invierà una risposta ARP, fornendo il proprio indirizzo MAC



- Una volta ricevuta la risposta, l'host A aggiungerà un'entrata relativa all'IP e al MAC dell'host B nella sua tabella ARP

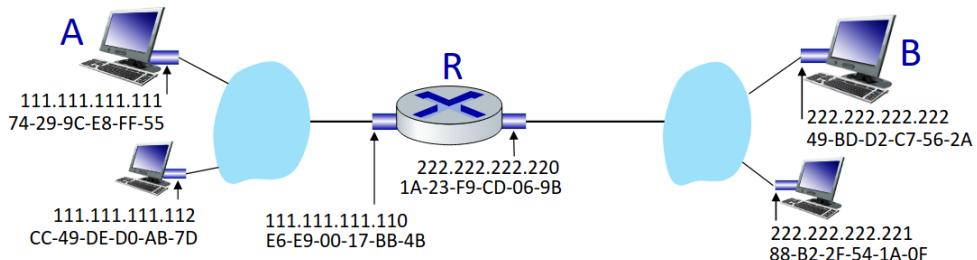


### 5.4.2 Instradamento verso un'altra sottorete

Poiché l'indirizzo MAC è utilizzato solo per l'indirizzamento locale, per poter inviare un pacchetto tra due host in due sottoreti diverse è necessario passare per uno o più (a seconda della gerarchia della rete) router di scambio, **cambiando continuamente l'indirizzo MAC sorgente di destinazione**.

Esempio:

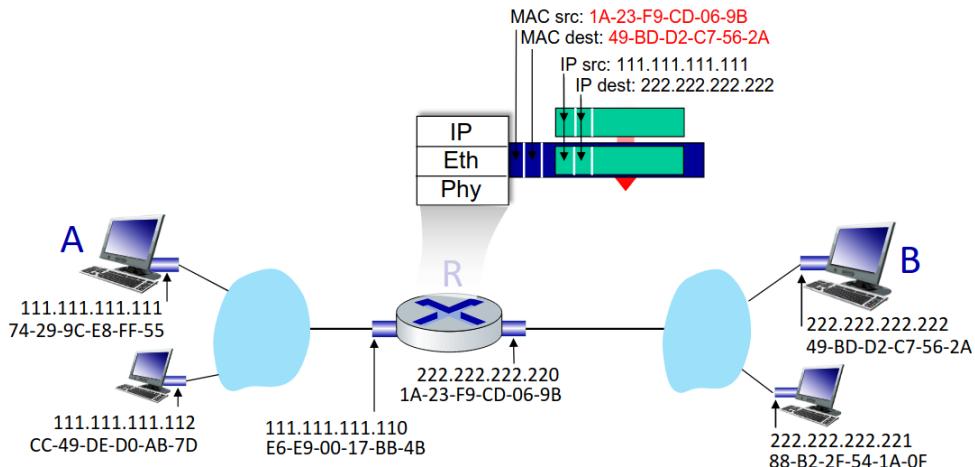
1. L'host A vuole inviare un datagramma verso l'host B appartenente ad un'altra LAN



2. Tramite la sua **forwarding table**, l'host A sa di poter raggiungere l'host B passando per il router R.
3. Diamo quindi già per **assunto** che:
  - L'host A conosca l'indirizzo IP dell'host B
  - L'host A conosca l'indirizzo IP del router R, precedentemente ottenuto tramite DHCP in quanto R è il gateway della sua rete
  - L'host A conosca l'indirizzo MAC del router R, precedentemente ottenuto tramite query ARP
4. Di conseguenza, l'host A crea il **datagramma** con indirizzo IP sorgente 111.111.111.111 (il suo indirizzo IP) ed indirizzo IP di destinazione 222.222.222.222 (l'indirizzo IP dell'host B), per poi successivamente, creare un **frame** contenente il datagramma precedentemente creato, utilizzando 74-29-9C-E8-FF-55 come indirizzo MAC sorgente (il suo indirizzo MAC) e 1A-23-F9-CD-06-9B come indirizzo MAC di destinazione (l'indirizzo MAC del router R), per poi inviarlo



5. Una volta ricevuto il frame, il router R **estrarrà** il datagramma dal frame, invian-dolo al livello di rete. Una volta letto l'indirizzo IP di destinazione nell'header del datagramma, il router R determinerà tramite la sua **forwarding table** l'interfaccia di uscita per poter raggiungere l'host B.
6. Successivamente, il router R creerà un nuovo **frame** contenente il datagramma ricevuto dall'host A, utilizzando 1A-23-F9-CD-06-9B come indirizzo MAC sorgente (il suo indirizzo MAC) e 49-BD-D2-C7-56-2A come indirizzo MAC di destinazione (l'indirizzo MAC dell'host B), per poi inviarlo



7. Una volta che l'host B avrà ricevuto il frame, esso verrà decapsulato estraendo il datagramma. Una volta letto l'indirizzo IP di destinazione nell'header del datagramma, l'host B noterà che esso coincide con il proprio indirizzo IP, inviando quindi il datagramma al proprio livello di trasporto.

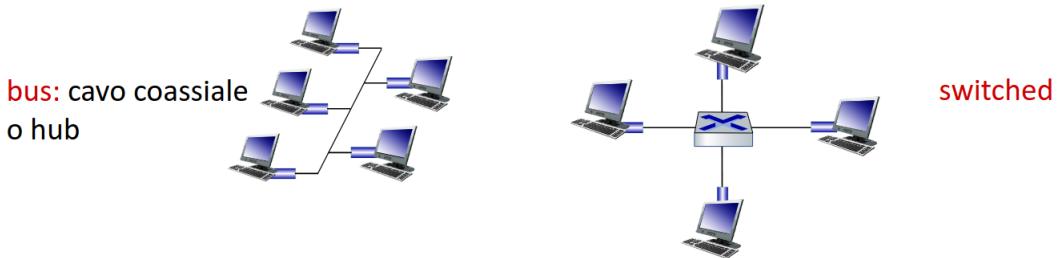
## 5.5 LAN cablate

### 5.5.1 Standard Ethernet

Lo **standard Ethernet** (o meglio, la famiglia di standard Ethernet) è la principale tecnologia cablata utilizzata all'interno delle LAN. Fino alla metà degli anni '90, veniva utilizzato un **bus condiviso** (es: un cavo coassiale condiviso) per lo scambio di frame, portando tutti i nodi ad essere in half-duplex e all'interno dello stesso dominio di collisione.

In alternativa al bus condiviso, poteva essere utilizzato anche un **hub**, ossia un dispositivo di comunicazione **non intelligente**: se un hub riceve un frame, tale frame viene inviato a tutti i dispositivi connessi all'hub (dunque non effettuando alcuna commutazione), fatta eccezione del mittente (ottenendo dunque lo stesso effetto di un bus condiviso).

In tempi moderni, invece, vengono utilizzati degli **switch** all'interno della rete, dove ogni "ramo" dello switch esegue un **protocollo Ethernet** separato dagli altri rami. In tal modo, i nodi non entrano in collisione tra loro e sono tutti potenzialmente full-duplex.



La struttura del frame Ethernet è composta da:

- **Campo preamble**, utilizzato per la sincronizzazione delle frequenze di clock del mittente e del destinatario. Composto da 7 byte di 10101010 seguiti da un byte 10101011
- **Campi addresses**, formati da 6 byte per l'indirizzo MAC del mittente e 6 byte per l'indirizzo MAC del destinatario. Se l'adattatore Ethernet (ossia una NIC compatibile) riceve un frame con indirizzo MAC di destinazione corrispondente al proprio o all'indirizzo di broadcast, il frame viene passato al protocollo di livello di rete. In caso contrario, il frame viene scartato.
- **Campo type**, utilizzato per il demultiplexing con il livello di rete (principalmente IP, ma anche altri possibili)
- **Campo data**, avente una lunghezza minima di 64 byte (viene aggiunto del padding se necessario) e una lunghezza massima pari al MTU impostato (tipicamente 1500 byte)
- **Campo CRC**, utilizzato per il controllo CRC



In particolare, lo standard Ethernet non richiede alcun handshaking tra le NIC dei dispositivi comunicanti (**connectionless**), rendendo tutta via la comunicazione **inaffidabile** per l'assenza di messaggi di ACK o NAK, implicando che i frame scartati possano essere recuperati solo se il mittente utilizza un **protocollo di trasporto affidabile**. Inoltre, lo standard Ethernet prevede l'uso del **protocollo CSMA/CD** senza slot e con backoff per gestire i canali broadcast.

Nonostante esistano molti **diversi standard Ethernet**, tutte le versioni hanno il comune il formato del frame e il protocollo MAC utilizzato, variando solo nella velocità garantita (es: da 2 Mb/s fino a 40 Gb/s) e nei supporti fisici utilizzati (es: cavo coassiale o fibra ottica). Lo standard Ethernet principalmente utilizzato è lo **standard Ethernet 802.3**, con un rate di trasmissione pari a **10 Mb/s**.

### 5.5.2 Funzionalità dello switch

Come già detto più volte, lo **switch** (in particolare lo **switch Ethernet** previsto dallo standard Ethernet) è un dispositivo a livello di collegamento che assume più ruoli:

- Garantisce che il segnale rimanga allo stesso livello (amplificatore)
- Memorizza e inoltra frame Ethernet
- Esamina l'indirizzo MAC del frame in entrata, inoltrandolo **selettivamente** (a differenza dell'hub) ad uno o più collegamenti in uscita all'interno di un **segmento di LAN** (ossia un sottoinsieme di nodi della rete connessi ad una porta, può anche corrispondere ad un singolo nodo)
- Utilizza il CSMA/CD per accedere ad un segmento di rete
- Gli host sono **ignari** della sua presenza (**trasparenza**)
- Non è necessaria la sua configurazione (**self-learning**)

Inizialmente, gli switch Ethernet vennero adottati per aumentare la velocità dello standard, poiché l'uso del CDMA/CD richiedeva la diminuzione della lunghezza del canale per assicurarsi che  $T_{fr} \geq 2D_p$  o direttamente l'abbandono del paradigma a bus condiviso.

Tramite uno switch, invece, gli host dispongono di una **connessione diretta dedicata** dallo switch. In particolare, la **commutazione dei pacchetti** tramite un buffer e l'utilizzo di un protocollo Ethernet utilizzato su **ogni collegamento in entrata**, permette l'uso del **full-duplex** e la presenza di **collisioni solo all'interno dello stesso collegamento**.

#### Esempio:

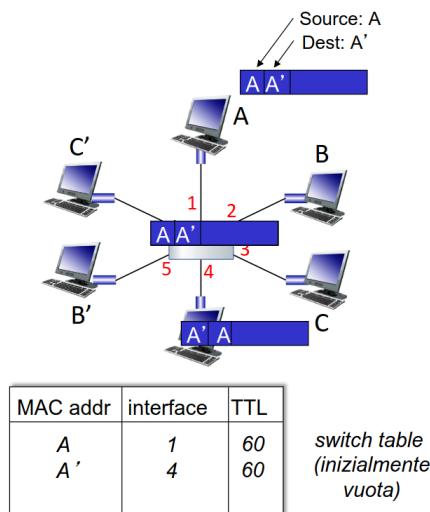
- Tramite la commutazione dei pacchetti, la trasmissione A-A' e la trasmissione B-B' possono avvenire simultaneamente, poiché vengono utilizzati collegamenti completamente diversi

- Tuttavia, le trasmissioni A-A' e C-A' non possono avvenire simultaneamente poiché si verificherebbe una collisione sul collegamento tra A' e lo switch stesso



Per effettuare le commutazioni, ogni switch possiede una **switch table** composta da entrate nel formato < Indirizzo MAC, Porta, TTL > (dunque simile ad una forwarding table).

Poiché è interposto tra i nodi, uno switch è in grado di apprendere automaticamente (**self-learning**) quali host possano essere raggiunti tramite quali interfacce: quando uno switch interposto tra nodi riceve un frame tramite un'interfaccia, lo switch memorizza automaticamente la posizione del mittente, ossia il suo **segmento LAN di appartenenza**, leggendo il suo indirizzo MAC tramite il frame stesso e salvando l'entrata relativa nella switch table.



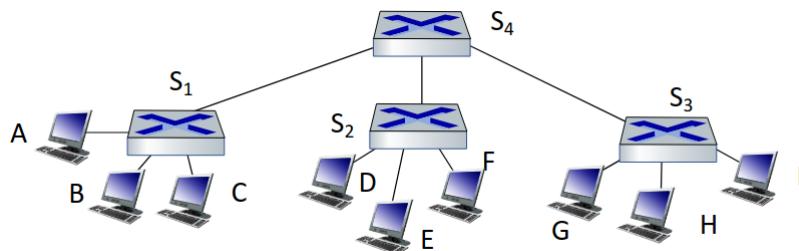
L'**algoritmo di commutazione** utilizzato dagli switch è pertanto molto semplice:

- Quando un frame viene ricevuto, registra il link di entrata e l'indirizzo MAC dell'host mittente
- Cerca nella switch table l'entrata contenente l'esatto indirizzo MAC del destinatario (**exact matching**)
- Se **esiste** un'entrata corretta nella switch table e il dispositivo di destinazione si trova nello **stesso segmento di LAN del mittente**, allora il frame viene scartato

4. Se **esiste** un'entrata corretta nella switch table e il dispositivo di destinazione si trova in un **diverso segmento di LAN del mittente**, allora il frame viene inoltrato sull'interfaccia descritta dall'entrata
5. Se invece **non esiste** un'entrata corretta nella switch table, il frame viene inviato in modalità flooding (dunque inviato a tutte le interfacce tranne quella del mittente)

Il concetto di **segmento di LAN** diventa particolarmente rilevante nel caso in cui vi siano **più switch interconnessi**. Difatti, tramite il self-learning è possibile tranquillamente interconnettere più switch tra loro, ottenendo lo stesso effetto di un "unico grande switch".

Nella seguente immagine, ad esempio, per lo switch  $S_4$ , gli host A, B e C appartengono allo stesso segmento di LAN, inoltrando verso lo switch  $S_1$  qualsiasi pacchetto avente uno di essi come destinazione.



### 5.5.3 Virtual LAN (VLAN)

#### Definition 55. Virtual LAN

Una **virtual LAN (VLAN)** è un **partizionamento logico** di una LAN connessa a livello fisico in più **LAN virtuali**. Ogni VLAN definita sulla stessa infrastruttura fisica viene interpretata dai dispositivi come una LAN completamente separata dalle altre.

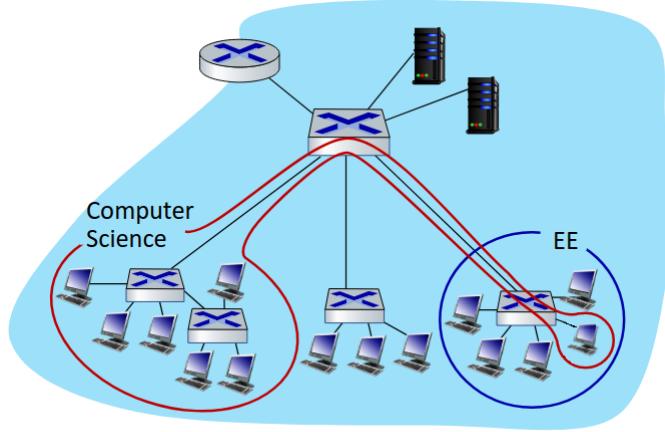
L'utilizzo delle VLAN permette una gestione più efficiente del traffico interno ad una LAN di grandi dimensioni. Ad esempio, senza il partizionamento logico fornito dalle VLAN, le **trasmissioni broadcast** verrebbero propagate all'interno dell'intera LAN, generando una grande quantità di traffico.

L'utilizzo delle VLAN fornisce una **maggior sicurezza** all'interno della stessa LAN tramite la possibilità di impedire a due VLAN interne alla stessa LAN di poter comunicare tra di loro, nonostante in realtà esse siano fisicamente collegate tra di loro.

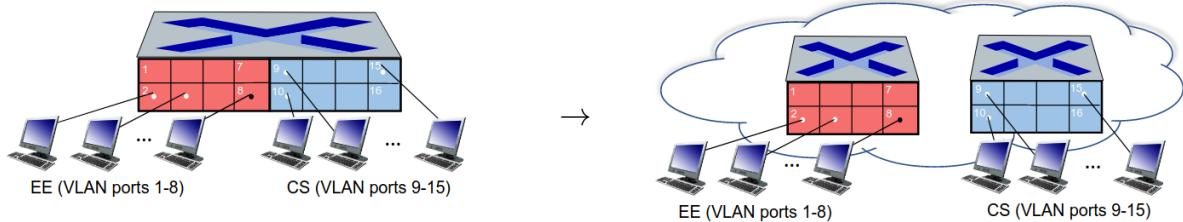
Inoltre, in tal modo un dispositivo può connettersi in qualsiasi punto della LAN, potendo tuttavia accedere sempre e solo alla VLAN di appartenenza.

**Esempio:**

- Un host appartenente alla VLAN definita per il dipartimento di Computer Science può connettersi in un qualsiasi punto della LAN, potendo accedere sempre e solo alla VLAN del dipartimento



Il partizionamento in VLAN può essere effettuato tramite molti criteri (es: anche in base al protocollo di un pacchetto). Il criterio più semplice e più utilizzato è il **port-based VLAN**, dove le porte di uno switch vengono **raggruppate** a livello logico, dunque tramite software di configurazione, in modo che il singolo switch operi in realtà come se fosse composto da più **switch virtuali**. Le porte possono inoltre essere assegnate dinamicamente tra le varie VLAN (**membership dinamica**).



Tramite il port-based VLAN, dunque, è possibile **isolare il traffico**, (es. riprendendo l'immagine precedente: permettendo ai frame da/verso le porte 1-8 di raggiungere solo le porte 1-8). Per tale motivo, due VLAN definite all'interno dello stesso switch **non possono comunicare direttamente tra di loro** attraverso lo switch stesso, richiedendo l'uso di un **router** (o un altro switch) collegato ad entrambe le VLAN.



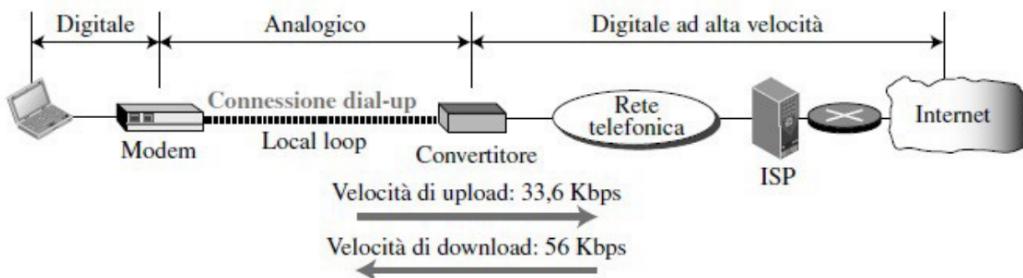
Alcuni switch sono inoltre dotati di una **porta trunk**, tramite cui possono essere trasportati frame tra VLAN definite su più switch fisici (**VLAN trunking**).



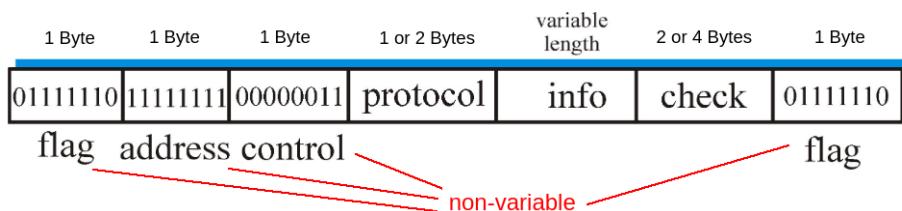
Tali frame, tuttavia, non possono essere frame definiti secondo il formato standard. Ben-sì, essi richiedono un **campo ID VLAN** aggiuntivo per poter identificare le VLAN di appartenenza (standard 802.1q)

#### 5.5.4 Reti point-to-point e protocollo PPP

Come già accennato, una **rete point-to-point** è composta da un collegamento dedicato solo a due dispositivi. Esse non utilizzano il controllo di accesso al mezzo condiviso (dunque funzionalità del sotto-livello MAC), bensì utilizzano protocolli dedicati, come il **Point-to-Point Protocol (PPP)**, sviluppato come protocolli per definire uno standard per la gestione della trasmissione dati per più di una rete sullo stesso collegamento seriale indipendentemente dal produttore dei dispositivi di rete (es: traffico IP classico, traffico AppleTalk, ..., traffico Novell IPX, ...).



Trattandosi di un collegamento con **solo un mittente e solo un destinatario**, il protocollo PPP non richiede l'uso di un protocollo MAC e degli indirizzi MAC. Durante la trasmissione, il protocollo PPP utilizzato deve essere in grado di rilevare la presenza di eventuali **guasti** nel collegamento in modo da segnalare l'errore a livello di rete e rilevare la presenza di **errori** nella trasmissione (non necessariamente la correzione di essi).



## 5.6 LAN wireless (WLAN)

### 5.6.1 Caratteristiche ed architettura di reti wireless

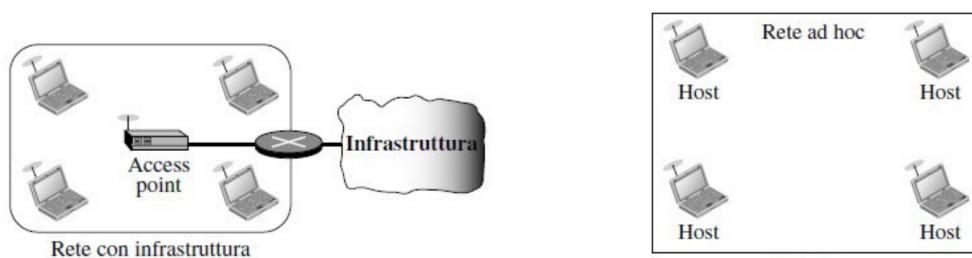
A differenza delle LAN cablate, le **wireless LAN (WLAN)** utilizzano l'aria come mezzo trasmissivo tramite l'uso di onde radio. Per natura stessa della trasmissione, dunque, il mezzo di trasmissione (dunque l'aria) è condiviso da tutti gli host della rete, implicando che le trasmissioni avvengano sempre ed unicamente in modalità **broadcast**. Pertanto, esse richiedono una gestione più elaborata rispetto alle reti cablate.

Ogni **host wireless** non è fisicamente connesso alla rete, potendosi dunque muovere liberamente al suo interno. Gli host wireless comunicano tra di loro inviando e ricevendo segnali da una stazione base detta **Access Point (AP)** (es: stazione radio, satellite, modem ADSL), il quale è solitamente connesso con una parte cablata della rete. L'access point è dunque responsabile dello scambio di pacchetti tra dispositivi appartenenti alla parte wireless di una LAN e la parte cablata di una LAN.



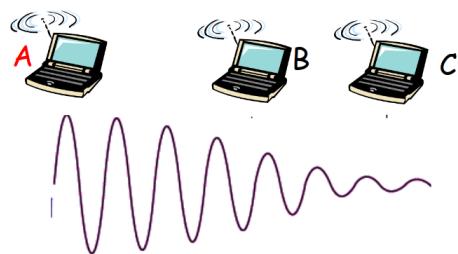
A livello infrastrutturale, dunque, un access point può essere visto come uno "switch wireless". Difatti, per migrare da un ambiente cablato ad un ambiente wireless è sufficiente sostituire la NIC (cambiando di conseguenza anche gli indirizzi MAC) dei vari dispositivi con delle **NIC wireless** e sostituire lo switch a cui esse sono connesse con un semplice access point.

Le WLAN connesse anche ad una parte cablata vengono dette **reti con infrastruttura**. Le WLAN possono anche essere composte da un insieme di host che si auto-organizzano per formare e gestire la rete (**reti ad hoc**), implicando che ogni host debba eseguire tutte le funzionalità di rete (network setup, routing, forwarding, ...).

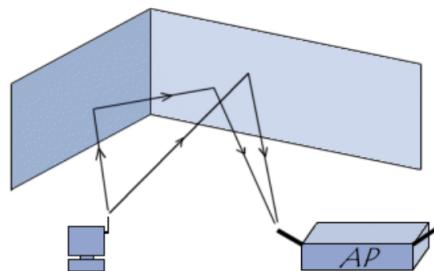


Per via dell'uso dell'aria come mezzo trasmissivo, la trasmissione all'interno delle reti wireless possiede alcune **caratteristiche sfavorevoli**:

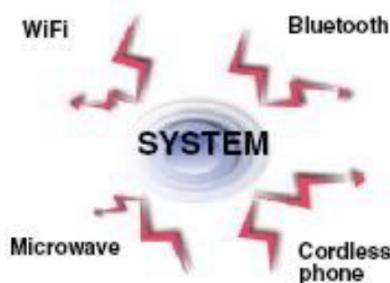
- **Attenuazione del segnale**, dovuta alla rapida diminuzione della forza dei segnali radio all'aumentare della distanza dal trasmettitore per via della dispersione del segnale in ogni direzione



- **Propagazione multi-path**, dovuta alla riflessione delle onde radio al contatto con un ostacolo (con aggiunta di perdita di potenza). Pertanto, un segnale può arrivare tramite una successione di riflessi a raggiungere una stazione o un AP attraverso percorsi multipli



- **Interferenze**, dovute all'uso della stessa banda di frequenza da parte di più trasmettitori (es: più tipologie di trasmissioni wireless utilizzano una banda a 2.4 GHz, come il Bluetooth e il Wi-Fi). Inoltre, anche la presenza dei multi-path può generare interferenza

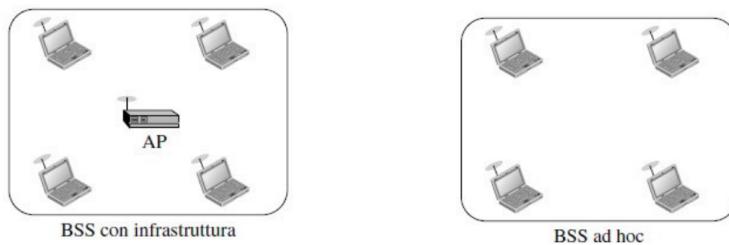


Per gestire gli errori generati da tali casistiche viene utilizzato un **Signal to Noise Ratio (SNR)**, dove se il segnale in arrivo è più forte del rumore allora esso viene accettato e convertito in dati reali, venendo scartato in caso contrario.

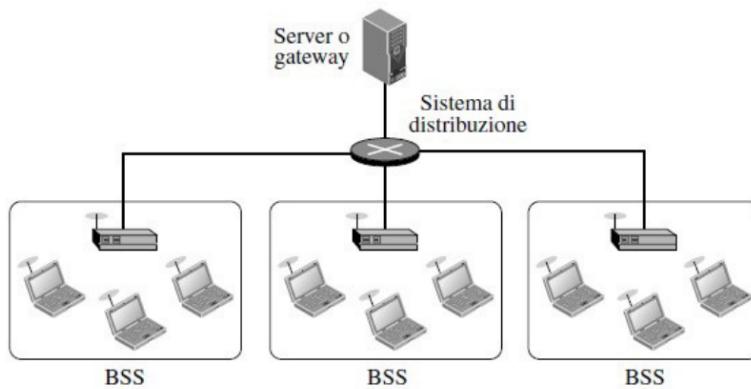
L'IEEE ha definito all'interno dello standard 802.11 le specifiche inerenti ai livelli di collegamento e fisico delle WLAN. In particolare, il **Wireless Fidelity (Wi-Fi)** è una tipologia di WLAN certificata dalla Wi-Fi Alliance, associazione no-profit composta da circa 300 aziende che si occupa di promuovere la crescita delle WLAN.

All'interno dello standard viene definita la seguente gerarchia per il wireless:

- **Basic Service Set (BSS)**, costituito da uno o più host wireless connessi (con l'aggiunta di un AP nel caso delle BSS con infrastruttura). Le **celle delle reti cellulari**, dunque, corrispondono ad una BSS con infrastruttura dove l'AP è il ripetitore cellulare.



- **Extended Service Set (ESS)**, costituito da due o più BSS con infrastruttura, i quali sono collegati tramite un sistema di distribuzione (ossia una rete cablata o wireless)



Lo spettro di frequenze dai 2.4 GHz ai 2.485 GHz è diviso in **11 canali** parzialmente sovrapposti. All'interno di una WLAN, l'amministratore dell'AP sceglie **uno o più canali** da utilizzare per le trasmissioni, rendendo possibili le interferenze con altri AP nel caso in cui vengano utilizzati gli stessi canali.

Tuttavia, i canali non interferiscono tra di loro nel caso in cui siano a **4 o più canali di distanza**, portando il numero massimo di canali utilizzabili da AP diversi per non ottenere interferenze pari a **tre canali** (es: utilizzando i canali 1, 6 e 11).

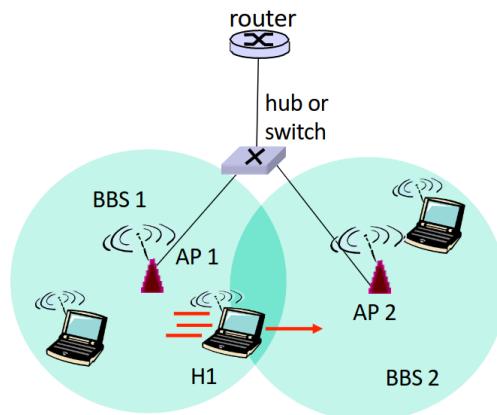
Inoltre, lo standard 802.11 prevede che una singola stazione wireless sia sempre **associata ad un AP** (e di conseguenza ad un BSS) per poter accedere ad Internet. Di conseguenza, per associarsi ad un BSS è necessario conoscere gli AP disponibili al suo interno, richiedendo quindi l'uso di un **protocollo di associazione**:

- L'AP invia segnali periodici, detti segnali di beacon, che includono l'identificatore univoco dell'AP, ossia il **Service Set Identifier (SSID)**, e il proprio indirizzo MAC
- La stazione wireless che vuole entrare all'interno di un BSS scandisce gli 11 canali trasmisivi alla ricerca di un frame beacon (**passive scanning**)
- Alla fine della scansione, la stazione sceglierà l'AP da cui ha ricevuto un **beacon con maggiore potenza di segnale**, inviandogli un frame con una richiesta di associazione
- L'AP accetterà la richiesta con un frame di risposta di associazione (a meno che non sia richiesta un'autenticazione), permettendo all'host entrante di inviare successivamente una richiesta DHCP per ottenere un indirizzo IP

Nonostante sembri un problema apparentemente difficile, l'uso di **celle** (dunque di BSS) all'interno della stessa rete cellulare permette il passaggio da una cella all'altra tramite le associazioni agli AP senza alcun problema.

### Esempio:

- L'host H1 si sta spostando tra due celle della stessa rete cellulare

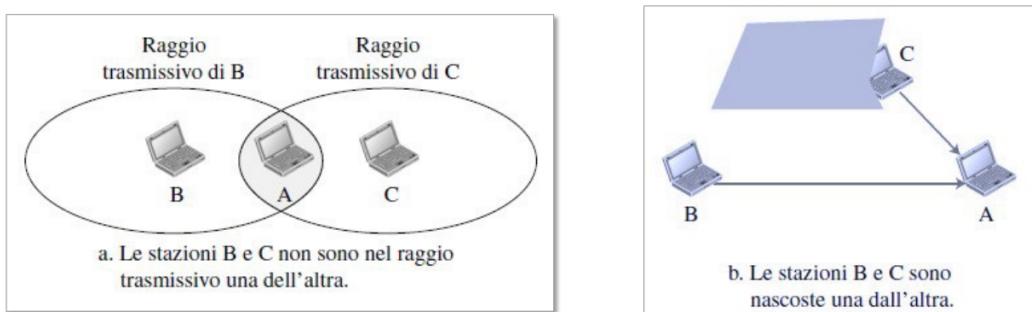


- L'host H1 sente che il segnale dall'access point AP1 si stia **affievolendo** ed avvia una scansione per cercare un segnale più forte, ossia AP2, disassociandosi da AP1 ed associandosi a quest'ultimo, mantenendo lo **stesso indirizzo IP** e le **stesse sessioni TCP aperte**
- Lo switch apprende la nuova porta su cui inoltrare i pacchetti con MAC address H1

## 5.6.2 Gestione delle collisioni nel wireless

Essendo l'unico mezzo trasmissivo condiviso tra tutti i dispositivi, vi è una stretta necessità di controllare l'accesso a tale mezzo per evitare le **collisioni**. Come per la gestione cablata, per rilevare una collisione un host deve poter **trasmettere e ricevere contemporaneamente**. Tuttavia, poiché la **potenza del segnale ricevuto** è molto **inferiore** a quella del segnale trasmesso, sarebbe troppo costoso utilizzare un adattatore di rete in grado di rilevare collisioni (**no collision detection**).

Inoltre, per via delle caratteristiche sfavorevoli del wireless, un host potrebbe **non accorgersi** che un altro host stia trasmettendo e dunque che sia impossibilitato a rilevare la collisione (**hidden terminal problem**)



Per accedere al mezzo di comunicazione, dunque, nello standard 802.11 vengono definiti vari **protocolli MAC wireless**, ricadenti principalmente in due tecniche di accesso:

- **Distributed Coordination Function (DCF)**, dove i nodi si contendono l'accesso al canale
- **Point Coordination Function (PCF)**, dove l'AP coordina gli accessi al canale, rimuovendo la contesa

Per quanto riguarda i protocolli DCF, l'idea principale consiste nel riutilizzare il **protocollo CSMA/CD** previsto dallo standard Ethernet. Tuttavia, per via dell'hidden terminal problem e del no collision detection, l'uso del CSMA/CD risulta **impossibile** nelle reti wireless.

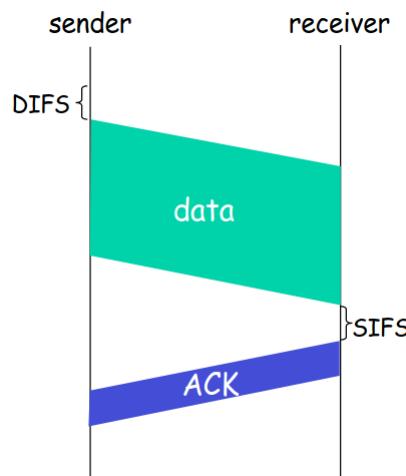
#### Definition 56. Protocollo CSMA/CA

Il **protocollo Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** è una variante del protocollo CSMA dove:

- **Non vi è collision detection**
- Viene utilizzato un riscontro (**messaggio di ACK**) per capire se una trasmissione sia andata a buon fine senza alcuna collisione
- Viene utilizzato un **doppio ascolto** sul canale, uno per i dati ed uno per l'ACK
- La collisione può avvenire anche per gli ACK

Per tentare di evitare collisioni col le stazioni che hanno già iniziato a trasmettere, le stazioni ascoltano il canale per un determinato periodo di tempo, detto **interframe space (IFS)**. Gli IFS si suddividono in **Short IFS (SIFS)**, utilizzato per l'alta priorità, e **DCF IFS (DIFS)**, utilizzato per la bassa priorità.

In particolare, prima di inviare un frame, la stazione mittente ascolta il canale e avvia la trasmissione se e solo se esso è libero per un tempo pari ad un **DIFS**. Una volta ricevuto il frame senza alcuna collisione, il ricevente invia un **ACK** dopo un tempo pari ad un **SIFS**. Viene utilizzato un tempo di DIFS maggiore rispetto ad un tempo di SIFS, in modo da dare priorità alle comunicazioni già iniziate (priorità agli ACK).



Dopo aver atteso un tempo pari ad un DIFS, se il canale è ancora inattivo la stazione attenderà un ulteriore **finestra di contesa (contention window)**, ossia un lasso di tempo di back-off per cui viene ascoltato il canale prima di trasmettere (il tempo è suddiviso in slot e ad ogni slot viene eseguito l'ascolto del canale):

- Viene scelto un valore  $k$  casuale nell'intervallo  $[0, CW]$ , dove  $CW$  varia a seconda del numero di collisioni precedenti
- Finché  $k > 0$ , viene ascoltato il canale per uno slot di tempo. Se il canale è libero per la durata dello slot, allora il valore  $k$  viene decrementato di uno. In caso contrario, viene atteso nuovamente che il canale si liberi per poi ripetere nuovamente la procedura di back-off
- Nel caso in cui il valore  $k$  raggiunga 0, viene inviato il frame



Per risolvere il problema dell'**hidden terminal**, tuttavia, è necessario anche un meccanismo di **prenotazione del canale** tramite dei messaggi di **request-to-send (RTS)** e **clear-to-send(CTS)**:

1. Il mittente attende un DIFS, seguito dalla finestra di contesa
2. Successivamente, viene inviato un RTS da parte del mittente, richiedendo di poter trasmettere i dati
3. Una volta ricevuta la richiesta, il destinatario attende un SIFS per poi inviare un messaggio di CTS
4. Dopo aver atteso un SIFS, il mittente invia i dati.
5. Infine, dopo aver atteso un ulteriore SIFS, il destinatario invia un ACK per la corretta ricezione dei dati

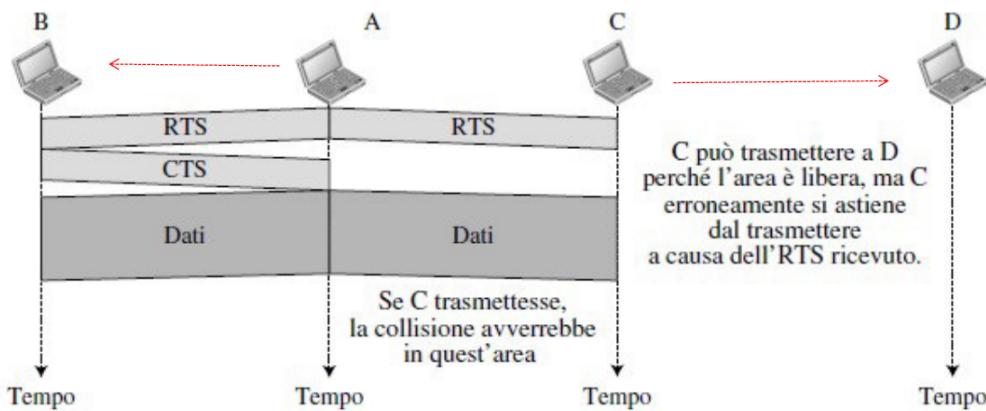
Affinché le **altre stazioni** che non sono coinvolte nella comunicazione ma sono nel **raggio di trasmissione della destinazione** sappiano quanto tempo devono astenersi dal trasmettere, all'invio del RTS viene inclusa la **durata di tempo** per cui verrà occupato il canale per trasmettere il frame e ricevere l'ACK, la quale, inoltre, viene inclusa anche nel CTS inviato dal destinatario.

Le stazioni influenzate da tale trasmissione avviano un timer, detto **Network Allocation Vector (NAV)**, indicante il tempo di attesa prima di poter ascoltare nuovamente il canale.

Se il mittente di una trasmissione non riceve il messaggio di CTS, esso assumerà che si sia verificata una collisione, riprovando la trasmissione dopo un **tempo di back-off**.



L'utilizzo di RTS/CTS, tuttavia, porta anche a situazioni sfavorevoli. Ad esempio, una stazione potrebbe astenersi dall'usare il canale nonostante possa trasmettere (**exposed terminal problem**).



Il frame utilizzato all'interno delle WLAN pertanto segue una struttura molto diversa dal frame Ethernet:

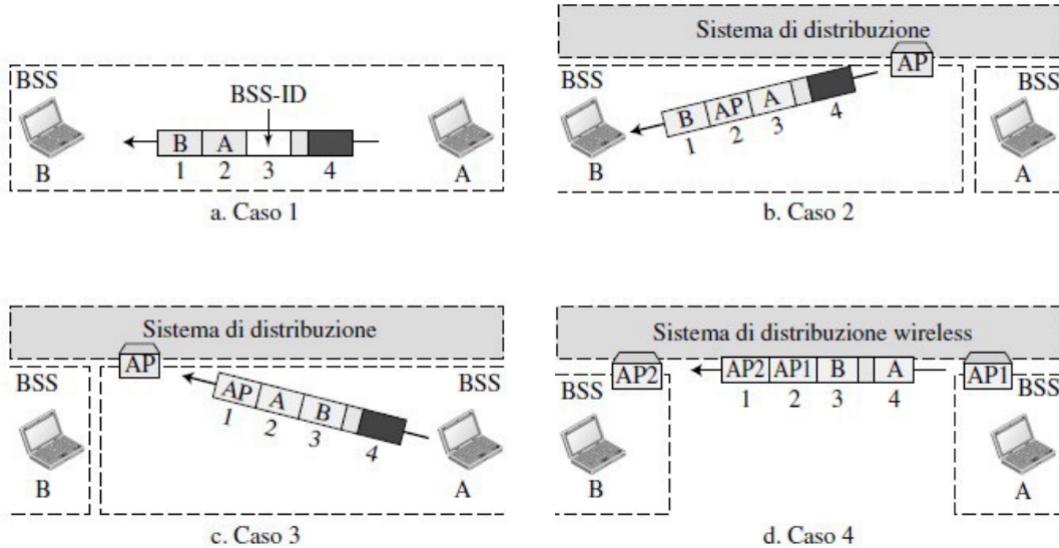
- **Campo Frame Control (FC)**, indicante la tipologia di frame (sotto-campo Type, 2 bit) e alcune informazioni di controllo
  - **Type 00 - Frame di gestione**, usati per le comunicazioni iniziali tra stazioni e AP
  - **Type 01 - Frame di controllo**, usato per accedere e dare riscontro assieme al sotto-campo Subtype (Subtype 1011: RTS, Subtype 1100: CTS, Subtype 1101: ACK)
  - **Type 10 - Frame di dati**, vengono usati per trasportare i dati
- **Campo Duration**, indica la durata della trasmissione successiva (corrispondente al tempo NAV di attesa prima di riascoltare)
- **Campo Sequence Control**, utilizzato per il numero di sequenza dei frammenti (gestione dei frame e degli ACK come nel livello di trasporto)

- **Campo Frame Check Sequence**, utilizzato per il CRC a 32 bit
- **4 Campi Indirizzi**, utilizzati per l'indirizzamento tra sistemi di distribuzione assieme ai sotto-campi To DS e From DS del campo FC



In particolare, l'indirizzamento tra sistemi di distribuzione attraverso i campi del frame ricade nei seguenti quattro casi:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destinazione	Sorgente	BSS ID	N/A
0	1	Destinazione	AP mittente	Sorgente	N/A
1	0	AP ricevente	Sorgente	Destinazione	N/A
1	1	AP ricevente	AP mittente	Destinazione	Sorgente

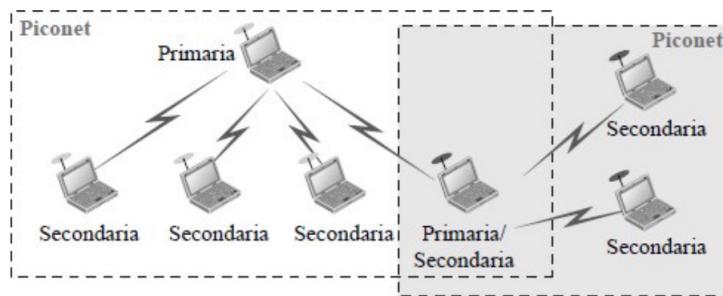


### 5.6.3 Bluetooth ed RFID

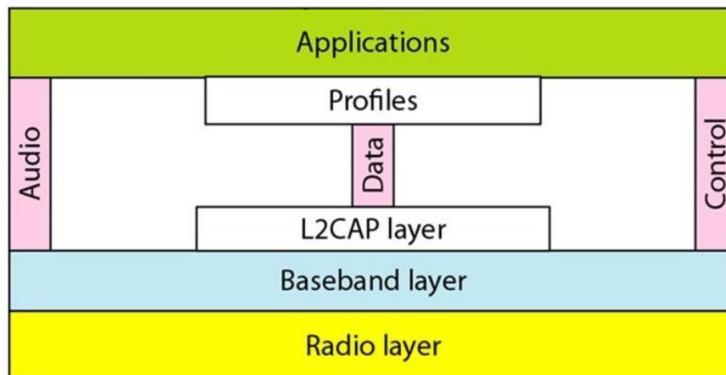
Il **Bluetooth** è una tecnologia LAN wireless progettata per connettere pochi dispositivi con diverse funzioni senza necessità di una stazione base (una LAN Bluetooth è una **rete ad hoc** di piccole dimensioni).

All'interno del Bluetooth vengono definite due tipologie di reti:

- **Piconet**, ossia una rete composta da al massimo 8 dispositivi, tra cui **una stazione primaria e 7 stazioni secondarie** sintonizzate con la prima. Se vi sono altre stazioni secondarie sintonizzate con la primaria, esse vengono messe in stato di **parked**, rimanendo in attesa che una stazione attiva venga spostata in stato di parked o lasci la rete
- **Scatternet**, ossia una combinazione di piconet. Una stazione può essere anche secondaria all'interno di una piconet e primaria all'interno di un'altra piconet



La tecnologia Bluetooth prevede l'uso di un trasmettitore radio di breve portata (massimo 10 metri) con date pari a 1 Mb/s e un'ampiezza di banda pari a 2.4 GHz. Pertanto, esse possono **interferire** con reti WLAN IEEE 802.11b, necessitando di un protocollo per minimizzare tale interferenza. Inoltre, la tecnologia Bluetooth definisce un **diverso stack protocollare** rispetto a quello TCP/IP.



Per via delle sue caratteristiche fisiche, la tecnologia non può utilizzare efficientemente il protocollo MAC CSMA/CA. Pertanto, al suo interno viene utilizzato il **protocollo MAC TDMA**:

- Vengono utilizzati slot temporali di  $625 \mu\text{s}$
- La comunicazione tra primaria e secondarie è **half duplex** (dunque non contemporanea)

- La stazione primaria utilizza slot **pari**, mentre le secondarie utilizzano slot **dispari**
- Se vi sono più stazioni secondarie, ad ogni slot utilizzato dalla stazione primaria viene specificata quale sia la prossima secondaria a trasmettere



Un'altra tecnologia molto utilizzata nell'ambito wireless è il sistema **Radio Frequency Identification (RFID)**, dove viene utilizzata una trasmissione wireless per ottenere identificazione, tracciamento automatico o contabilità.

Vengono utilizzati dei chip radiotrasmissenti di piccole dimensioni detti **tag**. Il segnale emesso da tali tag viene letto da un dispositivo **reader**, il quale leggerà l'ID contenuto in tale segnale.

In particolare, i tag possono essere **attivi**, ossia in grado di generare direttamente il segnale (richiedendo energia elettrica), o **passivi**, ossia in grado di riflettere il segnale inviato dal reader (**back-scattering**) alterandolo leggermente in modo da inserire il proprio ID (non richiedendo energia).

Esempi tipici della tecnologia RFID sono l'utilizzo di tessere (corrispondente ad un semplice tag passivo) per l'identificazione e l'autorizzazione all'accesso ad un luogo o servizio e l'utilizzo di sensori per il tracciamento di oggetti, come un bagaglio all'interno di un aeroporto.

La tipologia di comunicazione RFID più utilizzata prevede la presenza di un solo reader e più tag passivi (**single-reader with passive tags**), dove il primo invia un segnale di interrogazione e i vari tag rispondono con il loro ID.

Tale comunicazione, tuttavia, prevede la presenza di **collisioni** a seguito della risposta simultanea di più tag. Inoltre, essendo passivi, i tag non possono ascoltare il canale, rendendo impossibile l'uso del carrier sense e del collision detection. Di conseguenza, è necessario che sia il **reader** stesso a gestire gli accessi al canale. Uno dei protocolli MAC più utilizzati nella tecnologia RFID è il **Tree Slotted Aloha (TSA)**, dove ad ogni slot di collisione viene generato un nuovo frame figlio e solo i tag rispondenti allo stesso slot partecipano alla trasmissione.

# Capitolo 6

## Sicurezza della rete

La **sicurezza della rete** consiste nell'applicazione di una serie di operazioni di protezione dei dati, applicazioni, dispositivi e sistemi connessi alla rete. In particolare, in essa possiamo individuare **quattro principi** ricadenti all'interno della più generica triade **CIA (Confidentiality, Integrity and Availability)** utilizzata nella **sicurezza informatica**:

- **Riservatezza:** soli ed unicamente il mittente e il destinatario previsti da una comunicazione devono essere in grado di poter accedere il contenuto di un messaggio. Alla base di tale principio vi è l'uso della **crittografia**, dove il mittente cifra un messaggio e il destinatario decifra il messaggio una volta ricevuto.
- **Autenticazione:** il mittente e il destinatario devono essere in grado di confermare l'identità l'uno dell'altro
- **Integrità del messaggio:** il mittente e il destinatario devono poter accertarsi che il messaggio non sia stato manomesso
- **Accesso e disponibilità:** i servizi devono essere accessibili e disponibili per gli utenti

Per via della natura stessa di Internet, senza l'utilizzo di operazioni inerenti alla sicurezza di rete, un qualsiasi intruso può intercettare, cancellare, aggiungere o modificare i messaggi in transito tra mittente e destinatario. In particolare, le principali forme di **attacco** da parte di un soggetto esterno ricadono in:

- **Eavesdropping** (tradotto: *origliare*), ossia l'intercettazione di un messaggio (problema di **riservatezza**)
- **Fabrication**, dove vengono attivamente inseriti messaggi nella comunicazione (problema di **autenticazione**)
- **Impersonation**, dove viene falsificato l'indirizzo di origine del pacchetto, come l'**IP Spoofing** (problema di **autenticazione**)
- **Hijacking**, dove un soggetto esterno prende controllo della comunicazione, sostituendosi al mittente o al destinatario all'insaputa dell'altro lato della comunicazione (problema di **autenticazione** e **riservatezza**)

- **Denial of Service (DoS)**, dove viene impedito che il servizio venga correttamente utilizzato, ad esempio sovraccaricando le risorse (problema di **accesso e disponibilità**)

## 6.1 Principi di crittografia

Nelle successive sezioni faremo uso del classico **modello Alice & Bob** per trattare esempi di trasmissione sicura ed insicura, dove (solitamente) Alice è il **mittente** e Bob il **destinatario**. Ad esempio, consideriamo il seguente schema di crittografia:



1. Alice vuole inviare il messaggio  $m$  verso Bob
2. Invece di inviare il **messaggio in chiaro** (ossia non cifrato, dunque il messaggio  $m$ ), Alice applica, tramite un algoritmo di crittografia, la propria **chiave di cifratura**  $K_A$  sul messaggio  $m$ , inviando a Bob il **ciphertext** (**testo cifrato**)  $K_A(m)$
3. Durante la trasmissione del testo cifrato, l'intruso Trudy intercetta il messaggio. Tuttavia, essendo cifrato, essa non è in grado di poterlo comprendere, rendendo inutile l'intercettazione
4. Una volta raggiunto Bob, quest'ultimo applicherà la propria **chiave di decifratura**  $K_B$  per poter accedere al messaggio di Alice (dunque si ha che  $K_B(K_A(m)) = m$ )

Sebbene tale sistema generale sembra apparentemente sicuro, la vera sicurezza del sistema dipende interamente dalle **chiavi e l'algoritmo di cifratura** utilizzate:

- **Attacco con solo testo cifrato**: una volta ottenuto il testo cifrato, Trudy può provare **tutte le chiavi di decifratura possibili**, richiedendo una quantità di tempo in base alla complessità della chiave e dell'algoritmo, o effettuare un'**analisi statistica**, riducendo il numero di tentativi necessari
- **Attacco con testo in chiaro noto**: Trudy conosce alcune corrispondenze tra il testo in chiaro e testo cifrato, riuscendo a ricostruire il messaggio originale  
(es: ottenendo una buona parte di corrispondenze, è facile capire quali siano le lettere mancanti per ottenere la parola originale)

- **Attacco con testo in chiaro selezionato:** osservando molti testi cifrati generati dallo stesso algoritmo utilizzato, Trudy riesce a ricostruire il messaggio originale (es: in modo analogo a come il team di Alan Turing riuscì a decifrare il codice nazista generato dalla macchina Enigma)

### Definition 57. Crittografia a chiave simmetrica

Uno schema crittografico viene detto a **chiave simmetrica** se la stessa chiave è utilizzata sia per la cifratura che per la decifratura.

Tra i principali schemi crittografici a chiave simmetrica troviamo:

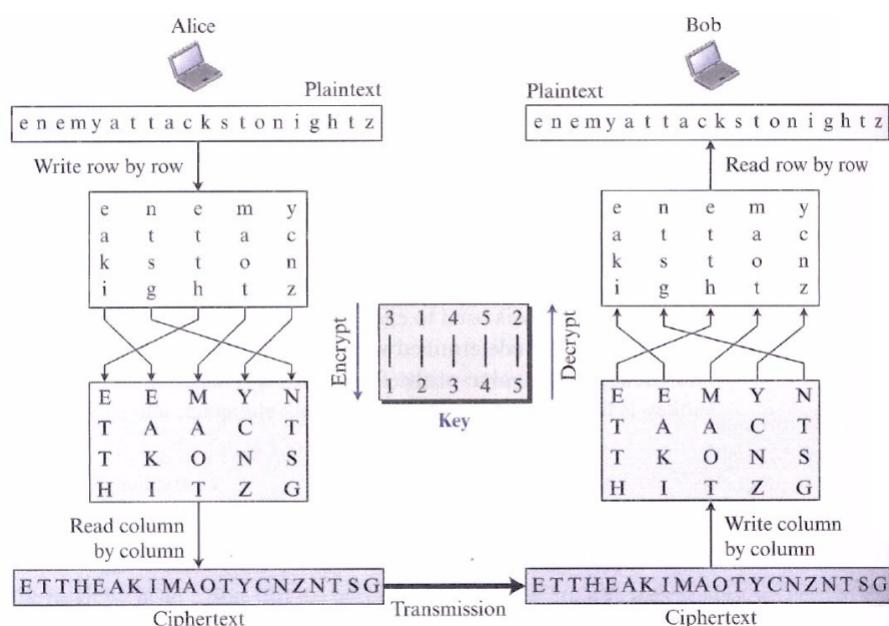
- **Cifrario per sostituzione**, dove parti del messaggio vengono sostituite tramite una mappatura biettiva. Esempi tipici sono il **cifrario monoalfabetico**, dove ogni lettera viene univocamente associata ad un'altra (es: la lettera A viene mappata alla lettera K), o il **cifrario di Cesare**, dove ogni lettera viene trasposta di un determinato numero di posizioni (es: se viene scelto il numero 3 come numero di trasposizioni, le lettere A, B, C, ... verranno mappate alle lettere D, E, F, ...)

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

**Plaintext:** bob. i love you. alice  
**ciphertext:** nkn. s gktc wky. mgsbc

*Esempio di crittografia con cifrario monoalfabetico*

- **Cifrario per trasposizione**, dove parti del messaggio vengono trasposte secondo una regola invertibile (es: disporre il messaggio per una tabella e scambiare la quarta riga con la prima, la seconda con la settima, ...)



- **Cifrario a blocchi**, dove il messaggio viene suddiviso in blocchi e vengono utilizzate tabelle di corrispondenza tra blocchi in chiaro e blocchi cifrati, spesso ripetendo il procedimento più volte.

Esempio tipico è il **Data Encryption Standard (DES)**, utilizzante una chiave simmetrica a 56 bit ed un input di testo in chiaro a 64 bit ed una cifratura a blocchi con concatenazione di blocchi di cifratura.



Tuttavia, la chiave a 56 bit utilizzata dal DES risulta essere troppo debole, richiedendo meno di un giorno per essere decifrata tramite bruteforce. Per rendere il DES più sicuro, in passato veniva utilizzato il **Triple DES (3DES)**, applicando 3 chiavi DES sul testo cifrato, mentre attualmente viene utilizzato l'**Advanced Encryption Standard (AES)**, basato su blocchi a 128 bit ed una chiave a 128, 192 o 256 bit, richiedendo circa 149 trilioni di anni per la decifratura.

### Definition 58. Crittografia a chiave asimmetrica

Uno schema crittografico viene detto a **chiave asimmetrica (o a chiave pubblica)** se la chiave di cifratura è diversa dalla chiave di decifratura.

In particolare, a differenza della crittografia a chiave simmetrica, dove è richiesto che il mittente e il destinatario conoscano la chiave condivisa, viene utilizzato un approccio radicalmente differente:

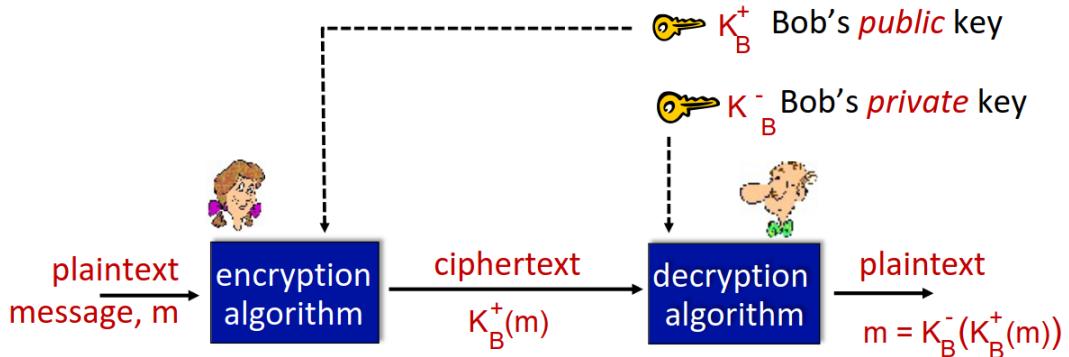
- La chiave di cifratura è **pubblica e nota a tutti**. Per tale motivo, essa viene anche detta **chiave pubblica**
- La chiave di decifratura è **nota solo al destinatario**. Per tale motivo, essa viene anche detta **chiave privata**
- La chiave pubblica e la chiave privata sono **l'una l'inversa dell'altra**.

Per via della loro natura, ogni **coppia di chiavi** può essere utilizzata per comunicare solo in una direzione:

- Se Alice e Bob vogliono comunicare usando una crittografia asimmetrica, sarà necessario generare **due coppie di chiavi**, dove la prima chiave pubblica e la seconda

chiave privata andranno ad Alice, mentre la prima chiave privata e la seconda chiave pubblica andranno a Bob

- Tutti i mittenti che vogliono inviare un messaggio cifrato a Bob possono usare la **stessa chiave pubblica**, permettendo a Bob di decifrare ogni messaggio con la chiave privata associata a tale chiave pubblica



Essendo più complessa della crittografia simmetrica, la crittografia asimmetrica viene solitamente utilizzata per cifrare/decifrare quantità limitate di informazioni (es: un breve messaggio o la chiave di un cifrario simmetrico, in modo che non venga intercettata durante la trasmissione).

Inoltre, in linea generale, si ha che:

- Il testo in chiaro  $m$  e il testo cifrato  $c$  vengono considerati **numeri interi**
- La cifratura e decifratura avviene tramite **due funzioni matematiche inverse tra loro**
- Il testo cifrato può essere inteso come  $c = K_{pub}(m)$ , mentre il testo in chiaro può essere inteso come  $m = K_{priv}(c)$

### 6.1.1 Crittosistema RSA

Il crittosistema a chiave asimmetrica più diffuso è il **crittosistema RSA** (nome dato dai suoi inventori: Rivest, Shamir e Adleman), basato interamente sull'algebra modulare e lo studio dei numeri primi:

1. Vengono scelti **due numeri primi**  $p, q \in \mathbb{P}$  molto elevati (es: 1024 bit ciascuno)
2. Vengono calcolati  $n := p \cdot q$  e  $\phi = (p - 1)(q - 1)$
3. Viene scelto un valore  $e$  (con  $e < n$ ) tale che esso sia **coprimo con  $\phi$**  (ossia non abbia fattori in comune con esso)
4. Viene scelto  $d$  tale che  $e \cdot d \equiv 1 \pmod{\phi}$ , ossia tale che  $d \equiv e^{-1} \pmod{\phi}$
5. La **chiave pubblica** corrisponderà alla coppia  $K_{pub} := (e, n)$ , mentre la **chiave privata** corrisponderà a  $K_{priv} := (d, n)$

6. Per la cifratura si ha che

$$m^e \equiv c \pmod{n}$$

mentre per la decifratura si ha che

$$c^d \equiv m \pmod{n}$$

implicando quindi che

$$(m^e)^d \equiv m \pmod{n}$$

7. Poiché i calcoli involgono potenze molto elevate, vengono utilizzate molte proprietà dell'algebra modulare per velocizzare il calcolo

### Esempio:

- Bob vuole generare la propria coppia di chiavi, in modo che chiunque possa comunicare in modo sicuro con lui cifrando un messaggio tramite la chiave pubblica generata
  1. Bob sceglie  $p = 5$  e  $q = 13$ , implicando che  $n = 5 \cdot 13 = 65$  e che  $\phi = 4 \cdot 12 = 48$
  2. Bob sceglie il primo valore coprimo con  $\phi = 48$ , ossia  $e = 5$ .
  3. Viene scelto  $d = 29$ , poiché  $d \equiv e^{-1} \pmod{\phi} \implies 29 \equiv 5^{-1} \pmod{48}$
  4. Le chiavi generate sono  $K_{pub} = (5, 65)$  e  $K_{priv} = (29, 65)$
- Una volta generate le chiavi e diffusa la chiave pubblica, Alice vuole inviare un messaggio a Bob.

Ad esempio, supponiamo che il messaggio sia  $m := 12$ , corrispondente alla lettera "L". Il testo cifrato ottenuto sarà:

$$12^5 \equiv c \pmod{65} \implies 17 \equiv c \pmod{65}$$

Per decifrarlo, dunque, sarà sufficiente applicare la chiave privata sul testo cifrato:

$$17^{29} \equiv m \pmod{65} \implies 12 \equiv c \pmod{65}$$

Tuttavia, le chiavi generate da Bob risultano essere **estremamente deboli**. Per trovare le chiavi, è sufficiente trovare i valori  $p$  e  $q$  tramite cui sono state generate:

1. Poiché la chiave pubblica  $K_{pub} = (e, n)$  contiene anche il valore  $n$  (è necessario che sia pubblico per effettuare la cifratura e la decifratura), è sufficiente trovare i due fattori che lo compongono
2. Poiché nel nostro esempio si ha che  $n = 65$ , è sufficiente provare a dividere  $n$  per i primi 3 numeri primi (ossia 2, 3 e 5), ottenendo che  $\frac{65}{5} = 13$  e dunque che  $p = 5$  e  $q = 13$
3. Successivamente, tramite  $p$  e  $q$  sarà facilmente calcolabile il valore  $\phi$  e il valore  $d \equiv e^{-1} \pmod{\phi}$  componente la chiave privata

Come già accennato, il funzionamento dell'algoritmo RSA deriva direttamente dalle proprietà dell'**algebra modulare**:

- È dimostrabile che dati  $p, q \in \mathbb{P}$  si ha che

$$x^y \equiv x^{y(\text{mod}(p-1)(q-1))} (\text{mod } pq)$$

da cui otteniamo che

$$(m^e)^d \equiv m^{ed} \equiv m^{ed(\text{mod}(p-1)(q-1))} \equiv m^{1(\text{mod}(p-1)(q-1))} \equiv m (\text{mod } n)$$

- Inoltre, poiché

$$m \equiv (m^e)^d \equiv (m^d)^e (\text{mod } n)$$

è possibile applicare le due chiavi in un **qualsiasi ordine**

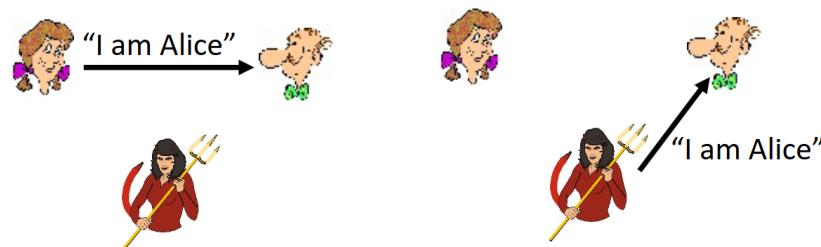
La **sicurezza dell'algoritmo RSA**, dunque, è determinata esclusivamente dai due valori  $p$  e  $q$  scelti, poiché numeri di grandi dimensioni sono molto **difficili da fattorizzare**.

Inoltre, poiché è richiesta una grande quantità di calcoli per l'uso dell'algoritmo RSA e poiché gli algoritmi DES e AES sono estremamente più veloci di RSA, la crittografia a chiave pubblica viene utilizzata per stabilire un canale sicuro tra i due interlocutori, per poi scambiare una seconda chiave, detta **chiave simmetrica di sessione**, da utilizzare durante lo scambio di messaggi.

## 6.2 Autenticazione ed Integrità del messaggio

Per poter autenticare correttamente un utente sulla rete, è necessario l'utilizzo di un **authentication protocol (ap)** in grado di impedire che un soggetto di terze parti possa impersonare un utente.

- Bob vuole che Alice sia in grado di dimostrarlo la sua identità prima di concederle l'accesso ad un dato sensibile
- **Protocollo ap1.0:**
  - Alice invia a Bob un messaggio "*I am Alice*" in cui afferma di essere Alice
  - Poiché all'interno di una rete Bob non ha alcun modo per sapere chi sia Alice, Trudy può semplicemente fingere di essere Alice, inviando a Bob lo stesso messaggio "*I am Alice*"



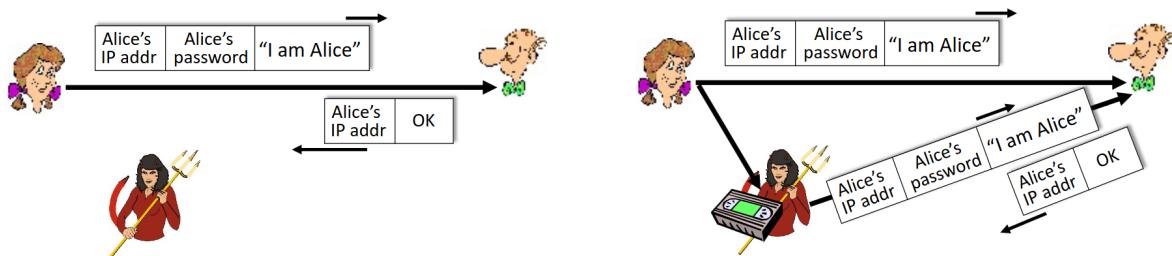
- **Protocollo ap2.0:**

- Oltre al messaggio "I am Alice", Alice inserisce anche il proprio indirizzo IP all'interno del pacchetto da inviare a Bob
- Tramite l'**IP spoofing** (ossia la falsificazione dell'indirizzo IP del mittente di un datagramma), Trudy può inserire l'indirizzo IP di Alice nel campo sorgente, fingendosi essa



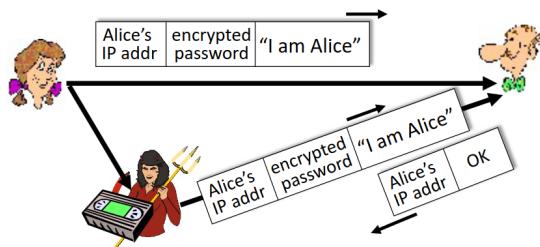
- **Protocollo ap3.0:**

- Oltre al messaggio "I am Alice" e al proprio indirizzo IP, Alice inserisce anche una password segreta precedentemente accordata con Bob
- Trudy può intercettare il pacchetto inviato da Alice e registrarla, per poi inviarla in un secondo momento a Bob, fingendosi Alice (**replay attack**)



- **Protocollo ap3.1 :**

- Oltre al messaggio "I am Alice" e al proprio indirizzo IP, Alice inserisce anche una password segreta **crittografata** precedentemente accordata con Bob
- Il replay attack effettuato da Trudy funziona ancora



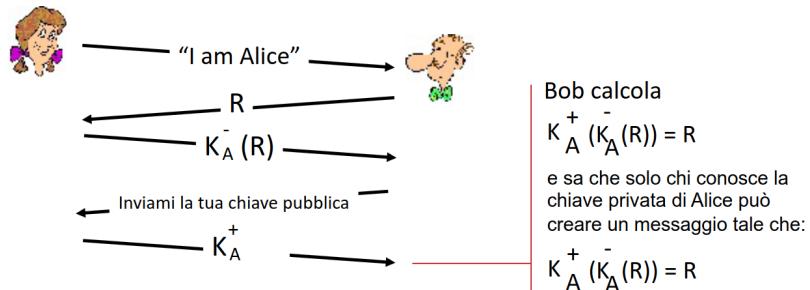
- Protocollo ap4.0 :

- Dopo aver ricevuto il pacchetto di autenticazione da Alice, Bob invia un **nonce**  $R$  ad Alice, ossia un **numero usato once-in-a-lifetime**.
- Successivamente, Bob rimarrà in attesa che Alice invii il nonce  $R$  cifrato con una **chiave simmetrica segreta**, in modo da potersi accertare che Alice sia "live" in quanto solo Alice è a conoscenza della chiave
- Per utilizzare tale protocollo, tuttavia, è necessario stabilire in anticipo un canale sicuro per potersi scambiare preventivamente la chiave simmetrica

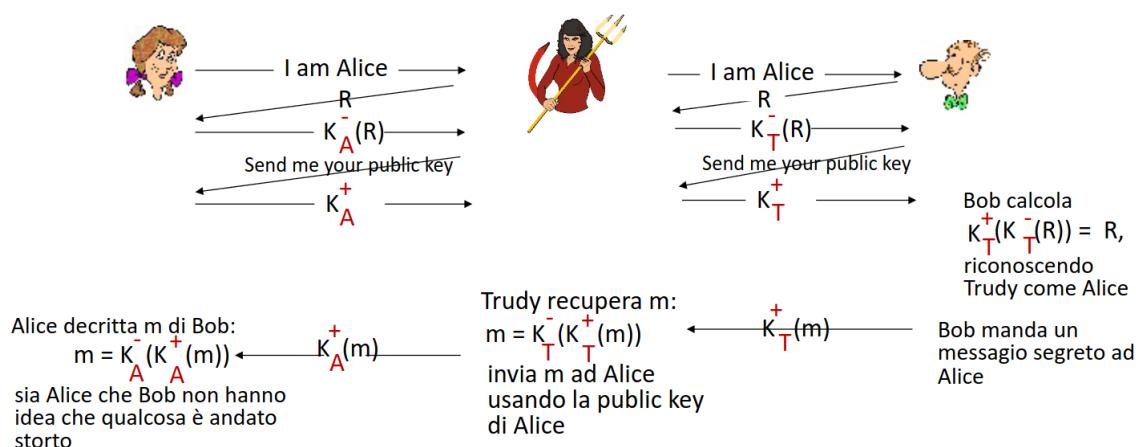


- Protocollo ap5.0 :

- Alice cifra con la sua **chiave privata** il nonce ricevuto da Bob, per poi inviarlo
- Successivamente, Bob chiede ad Alice di inviargli la propria chiave pubblica, in modo da poter decifrare il nonce ricevuto



- Trudy può immettersi nella conversazione, impersonando Alice quando comunica con Bob e impersonando Bob quando comunica con Alice (**man in the middle attack**)



### 6.2.1 Firma digitale e Message digest

#### Definition 59. Firma digitale

La **firma digitale** è un metodo matematico/crittografico utilizzato per dimostrare l'**autenticità di un documento digitale** autenticando l'autore di tale documento ed accertandosi dell'integrità del documento, ossia che non sia stato manipolato.

La **firma digitale** viene riconosciuta dalle varie nazioni come **strumento legale valido** e può essere utilizzata in **sede giuridica** per dimostrare l'avvenuta firma da parte di un soggetto.

Poiché l'**ordine di applicazione** di chiave pubblica e privata non è importante per ottenere il messaggio originale e poiché la chiave privata viene **posseduta solo ed esclusivamente da un soggetto**, per autenticare il soggetto stesso è sufficiente applicare la sua chiave pubblica su un **documento firmato tramite la sua chiave privata**, dunque  $K_{pub}(K_{priv}(m)) = m$

**Esempio:**

- Supponiamo che Alice riceva da Bob il messaggio  $m$  firmato con la chiave privata  $K_B^-$  di Bob (dunque riceve  $K_B^-(m)$ )
- Per verificare che sia stato effettivamente firmato da Bob, Alice applica la chiave pubblica di Bob sul messaggio firmato
- Se  $K_B^+(K_B^-(m)) = m$ , allora chiunque abbia firmato il messaggio  $m$  deve aver utilizzato la chiave privata di Bob. Inoltre, poiché  $K_B^+(K_B^-(m)) = m$ , Alice può assicurarsi che il messaggio non sia stato alterato
- Qualora qualcuno si impossessasse della chiave privata di Bob, tale soggetto potrebbe **legalmente firmare digitalmente documenti al posto di Bob**, rendendo quindi fondamentale che Bob conservi in modo sicuro la sua chiave privata

#### Definition 60. Message digest

Un **message digest** è l'output ottenuto applicando una **funzione di hash ottimale** su un messaggio. La funzione di hash utilizzata deve rispettare le seguenti proprietà:

- Il digest prodotto deve essere di **dimensioni fisse**
- Deve essere **computazionalmente impossibile** ricostruire il messaggio originale tramite un suo digest
- Applicando la funzione sullo stesso messaggio il digest ottenuto sarà sempre lo stesso (dunque il digest deve essere **invariante nel tempo**)
- Alterando leggermente il messaggio il digest ottenuto deve essere **radicalmente diverso**
- Il numero di **collisioni hash**, ossia parole aventi lo stesso digest, deve essere il minimo possibile

Poiché risulta essere computazionalmente costoso cifrare e decifrare messaggi lunghi con chiave pubblica o privata, il **message digest** viene utilizzato per ridurre l'**impronta digitale** di un messaggio crittografato, ossia la quantità di calcoli necessaria per processarlo.

Poiché la funzione hash ottimale deve essere **invariante**, se Bob invia ad Alice il messaggio  $m$  e il digest  $H(m)$ , Alice può verificare l'**integrità del messaggio** applicando la stessa funzione di hash sul messaggio  $m$  ricevuto, verificando se i due digest **coincidono**.

Di conseguenza, per ridurre l'impronta digitale della firma digitale, Bob applica la sua chiave privata  $K_B^-$  sul digest  $H(m)$  del messaggio che vuole inviare ad Alice, per poi **accodare**  $K_B^-(H(m))$  al **messaggio originale**.

In tal modo, una volta ricevuto il pacchetto, Alice è in grado di applicare la chiave pubblica sul digest crittografato, per poi calcolare il digest dei messaggio  $m$  ricevuto e verificare se esso **coincida** con quello decifrato, verificando così sia l'**autenticità** del documento sia la sua **integrità**.



Le funzioni hash più utilizzate sono:

- **Message-Digest 5 (MD5)**, una funzione hash ampiamente utilizzata anche all'interno del documento RFC 1321. Il messaggio viene convertito in un digest di 128 bit tramite un processo a 4 fasi
- **Secure Hash Algorithm 1 (SHA-1)**, una funzione standard prevista da molti standard. Il digest prodotto è di 160 bit.

Nonostante la loro efficacia, entrambe le funzioni hash precedentemente citate vengono considerate **insicure**, poiché non computazionalmente laboriose per i computer moderni, richiedendo massimo un giorno tramite un approccio bruteforce. Altre loro varianti, come MD6 e SHA-2 vengono utilizzate al loro posto.

## 6.2.2 Certification Authorities (CA)

### Definition 61. Certification Authority (CA)

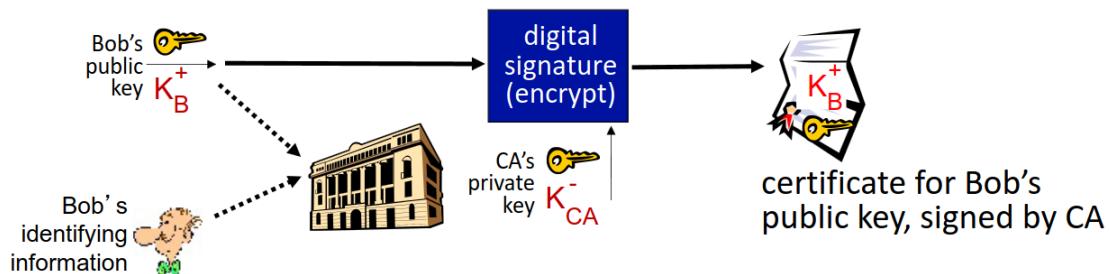
Una **certification authority (CA)** è un'organizzazione o ente certificato atto all'associazione di chiavi pubbliche ad una particolare entità.

L'entità, la quale può essere una persona, un sito web o un router, **registra la propria chiave pubblica** fornendo una prova d'identità alla CA, la quale successivamente creerà un **certificato digitale** che attesta l'associazione tra l'entità e tale chiave pubblica.

La chiave pubblica inserita nel certificato viene **firmata con la chiave privata della CA**, al fine di garantirne l'autenticità, per poi pubblicizzare il certificato affermando che tale chiave pubblica appartenga all'entità certificata.

#### Esempio:

1. Bob vuole certificare la propria chiave pubblica
2. Bob invia in modo sicuro (ad esempio utilizzando la chiave pubblica della CA) la propria chiave pubblica e la propria prova d'identità
3. Una volta verificata l'identità di Bob, la CA firmerà con la propria chiave privata la chiave pubblica di Bob, per poi inserire la firma e la chiave pubblica nel certificato



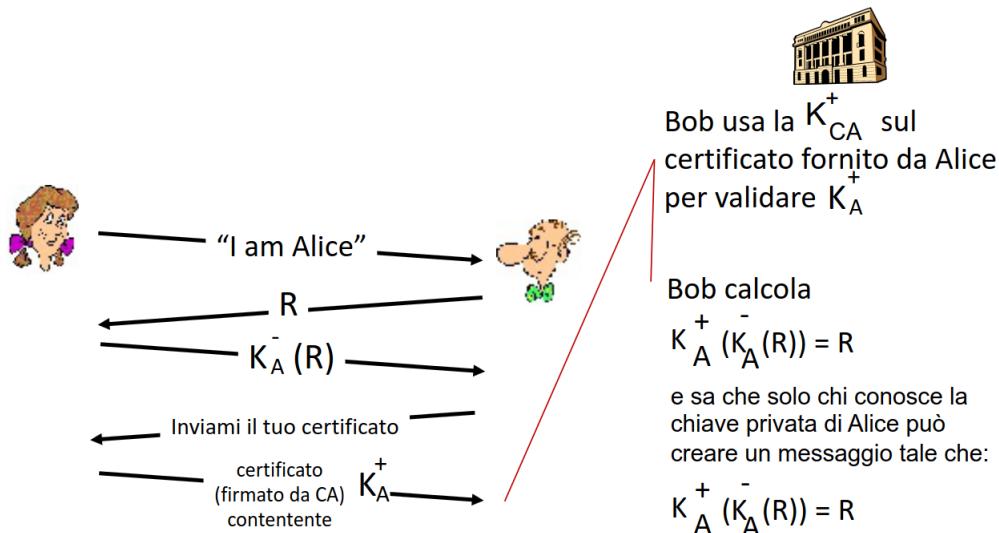
I **certificati digitali** seguono la seguente struttura:

- Informazioni:
  - Versione
  - Numero seriale
  - ID dell'algoritmo
  - Ente emittente
  - Validità
  - Non prima
  - Non dopo

- Soggetto
- Informazioni sulla chiave pubblica del soggetto
- Algoritmo per l'utilizzo della chiave pubblica
- Chiave pubblica
- Codice identificativo univoco dell'emittente (facoltativo)
- Codice identificativo univoco del soggetto (facoltativo)
- Estensioni (facoltativo)
- ...
- Algoritmo di firma del certificato
- Firma del certificato

Tramite l'uso dei certificati digitali è possibile **validare l'autenticità della chiave pubblica di un soggetto**, risolvendo completamente il **man in the middle attack** (a meno che la CA stessa non venga compromessa):

- Quando Alice vuole la chiave pubblica di Bob, richiede il suo certificato direttamente a Bob o ad un ente esterno
- Alice applica la chiave pubblica della CA sulla firma presente nel certificato, confrontandola con la chiave pubblica presente nel certificato
- Se le due chiavi coincidono, Alice potrà assicurarsi che la chiave pubblica sia effettivamente di Bob, impedendo a Trudy di immettersi nella comunicazione impersonando Bob



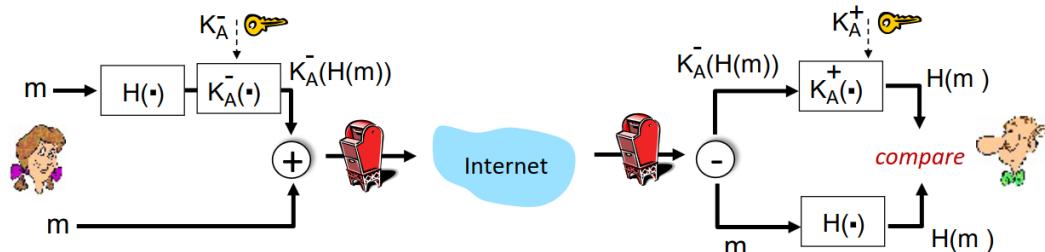
## 6.3 Sicurezza della posta elettronica

Tramite l'uso di chiavi pubbliche e private, è possibile ottenere **riservatezza**, **autenticità** e **integrità** in varie tipologie di applicazioni di rete:

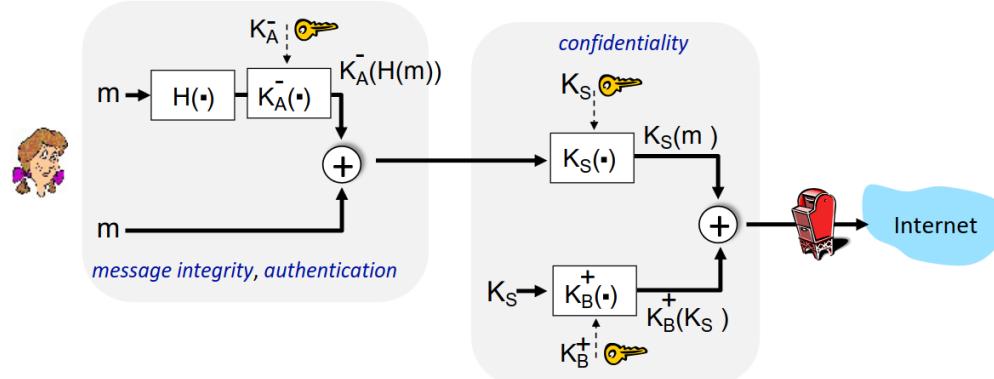
- Alice desidera scambiare email a Bob in modo **riservato**.
  - Alice genera una chiave simmetrica  $K_S$
  - Alice crittografa l'email  $m$  con  $K_S$  (per maggiore efficienza), per poi crittografare la chiave  $K_S$  con la chiave pubblica di Bob
  - Alice invia sia  $K_S(m)$  sia  $K_B^+(K_S)$  a Bob
  - Bob usa la propria chiave privata  $K_B^-$  per decifrare  $K_B^+(K_S)$ , in modo da ottenere  $K_S$ , per poi utilizzarla per decifrare l'email
  - Bob e Alice possono accordarsi per continuare ad utilizzare la chiave simmetrica  $K_S$  in futuro, senza richiedere che ne venga nuovamente generata un'altra



- Alice desidera inviare un'email a Bob assicurando a quest'ultimo l'**autenticità** e l'**integrità** dell'email stessa (non è interessata alla riservatezza)
  - Alice calcola il digest della sua email  $m$  e firma digitalmente tale digest
  - Alice invia a Bob  $K_A^-(H(M)) + m$ , ossia un messaggio composto da  $K_A^-(H(M))$  e  $m$
  - Una volta ricevuto il messaggio, Bob recupererà la chiave pubblica di Alice tramite il suo certificato digitale, per poi decifrare il digest
  - Successivamente, Bob calcolerà il digest del messaggio ricevuto e lo comparerà con quello decifrato



- Alice desidera inviare un'email a Bob garantendo **riservatezza**, **autenticità** e **integrità** dell'email
  - Alice calcola il digest della sua email  $m$  e firma digitalmente tale digest
  - Alice genera una chiave simmetrica  $K_S$
  - Alice crittografa il messaggio  $K_A^-(H(m)) + m$  con  $K_S$  (per maggiore efficienza), per poi crittografare la chiave  $K_S$  con la chiave pubblica di Bob
  - Alice invia sia  $K_S(K_A^-(H(m)) + m)$  sia  $K_B^+(K_S)$  a Bob
  - Bob usa la propria chiave privata  $K_B^-$  per decifrare  $K_B^+(K_S)$ , in modo da ottenere  $K_S$ , per poi utilizzarla per decifrare  $K_S(K_A^-(H(m)) + m)$
  - Una volta ottenuto il messaggio  $K_A^-(H(m)) + m$ , Bob recupererà la chiave pubblica di Alice tramite il suo certificato digitale, per poi decifrare  $K_A^-(H(m))$
  - Successivamente, Bob calcolerà il digest del messaggio ricevuto e lo comparerà con quello decifrato



Il software più utilizzato per gestire tale tipologia di comunicazioni è il software **Pretty Good Privacy (PGP)** (attualmente esiste anche una versione open source, ossia OpenPGP).

## 6.4 Sicurezza a livello di trasporto (TLS)

Come già accennato nel capitolo inerente al livello di trasporto, alcuni protocolli di tale livello sprovvisti di sicurezza utilizzano spesso il **Transport Layer Security (TLS)**, un protocollo di sicurezza ampiamente diffuso situato "al di sopra" del livello di trasporto (tra applicativo e trasporto).

Ad esempio, la versione del protocollo HTTP facente uso del TLS è l'HTTPS (HTTP Secure, porta TCP/443).

Il TLS fornisce **riservatezza** tramite crittografia simmetrica, **autenticazione** tramite crittografia a chiave asimmetrica e **integrità** tramite hashing crittografico. Inizialmente

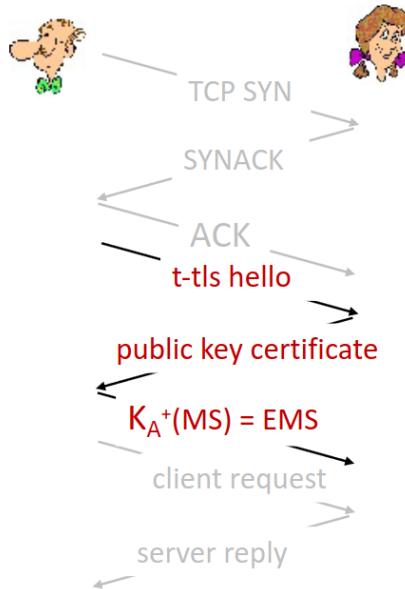
fu implementato tramite socket sicuri (**Secure Socket Layer - SSL**), per poi venir deprecato nel 2015 e sostituito con il protocollo **TLS 1.3**.

Prima di discutere dell'implementazione effettiva del TLS 1.3, analizziamo la costruzione di un protocollo TLS "giocattolo", il quale chiameremo **Toy-TLS (T-TLS)**. In particolare, abbiamo già visto precedentemente tutte le parti necessarie:

- **Handshake**, dove Alice e Bob usano i loro certificati e le loro chiavi private per autenticarsi a vicenda e scambiarsi uno **shared secret**, ossia una "master key" da utilizzare per generare **chiavi simmetriche di sessione**
- **Key derivation**, Alice e Bob usano lo shared secret per generare le chiavi di sessione
- **Data transfer**, dove i dati trasferiti vengono visti come una serie di record di dati e non più come un unico bytestream, richiedendo di tenere traccia dello stato della connessione
- **Chiusura della connessione**, tramite messaggi speciali

Vediamo quindi una possibile implementazione del nostro T-TLS handshake:

1. Bob stabilisce una connessione TCP con Alice, effettuando quindi il normale handshake a 3 vie
2. Bob invia un messaggio di "T-TLS hello", chiedendo ad Alice il suo certificato
3. Una volta verificata l'identità di Alice, Bob cifra il Master Secret (MS), ossia la chiave principale utilizzata per generare tutte le altre chiavi durante la sessione TLS



Nella sua semplicità, tale implementazione proposta richiede ben 3 RTT prima che Bob possa iniziare a ricevere i dati da Alice, risultando quindi un'implementazione poco efficiente, ma comunque efficace.

Passiamo ora quindi alla generazione delle chiavi. Per effettuare un trasferimento sicuro dei dati, è necessario utilizzare un crittografia per un **message authentication code (MAC)** e una crittografia per il messaggio stesso. Tuttavia, in generale è considerato **insicuro** utilizzare la stessa chiave per più di una funzione crittografica.

Di conseguenza, necessitiamo di **quattro chiavi simmetriche**:

- $K_C$ , ossia la chiave di cifratura per i dati inviati dal client al server
- $K_S$ , ossia la chiave di cifratura per i dati inviati dal server al client
- $M_C$ , ossia la chiave MAC per autenticare i dati inviati dal client al server
- $M_S$ , ossia la chiave MAC per autenticare i dati inviati dal server al client

Tali chiavi vengono derivate da una **Key Derivation Function (KDF)**, la quale utilizza il MS e alcuni dati casuali aggiuntivi per generare le chiavi.

Una volta generate le chiavi, è necessario considerare il modo in cui esse verranno applicate sui dati. In particolare, sappiamo che il TCP fornisce un bytestream per l'astrazione del flusso dati.

Tuttavia, non è possibile crittografare i dati man mano che essi arrivano al socket TCP, poiché altrimenti non sapremmo **quando inviare il MAC**. Ad esempio, se la firma MAC venisse inviata alla fine del bytestream, potremmo garantire l'integrità del messaggio solo una volta che esso è stato completamente ricevuto, rendendo inutile l'intera trasmissione nel caso in cui il messaggio sia stato alterato.

Di conseguenza, è necessario suddividere il bytestream in una serie di **record**, dove ogni record client-server contiene un MAC creato utilizzando  $M_C$  e dove ogni record server-client contiene un MAC creato utilizzando  $M_S$ . In tal modo, il ricevitore può agire su ogni record man mano che essi arrivano. Infine, possiamo applicare la chiave  $K_C$  (o  $K_S$ , a seconda del mittente) sull'intero record, per poi passarlo al layer di trasporto.

$$K_c(| \text{length} | \text{data} | \text{MAC} | )$$

Tuttavia, poiché il layer di trasporto è posto **al di sotto del TLS**, l'header TCP non è cifrato. Di conseguenza, è possibile effettuare alcuni **attacchi al bytestream**:

- **Reordering attack**: tramite un man in the middle attack vengono intercettati i segmenti TCP e riordinati, manipolando i numeri di sequenza nell'intestazione TCP non crittografata
- **Replay attack**: viene salvato il bytestream per riutilizzarlo successivamente

Per risolvere tali problematiche, possiamo utilizzare dei **numeri di sequenza TLS** incorporati nel MAC (rendendo il riordinamento inefficace), un **nonce** dove la chiave MAC cambia ad ogni record (rendendo il replay attack inefficace). A questo punto, inoltre, non è più necessario che il MAC venga cifrato anche con  $K_C$  (o  $K_S$ ).

$$K_c(| \text{length} | \text{data} | ) M_C( | \text{MAC} | )$$

Rimane tuttavia un possibile **attacco alla chiusura della connessione**:

- **Truncation attack:** poiché l'header TCP non è cifrato, l'attaccante potrebbe falsificare il segmento di chiusura della connessione, portando una o entrambe le parti a terminare immediatamente la connessione

La soluzione a tale problema risulta molto semplice: è sufficiente aggiungere un **campo type** nel record il quale verrà impostato a 0 se la trasmissione riguarda i dati o ad 1 se la trasmissione deve essere chiusa (ricordiamo che il record verrà poi cifrato). Inoltre, in tal modo il MAC sarà calcolato utilizzando il campo data, il campo type e il numero di sequenza del record

$$K_c(\boxed{\text{length} \quad | \text{type} \quad | \text{data}}) M_c(\boxed{\text{MAC}})$$

#### 6.4.1 Protocollo TLS 1.3

##### Proposition 10. TLS 1.3 e Cipher suite

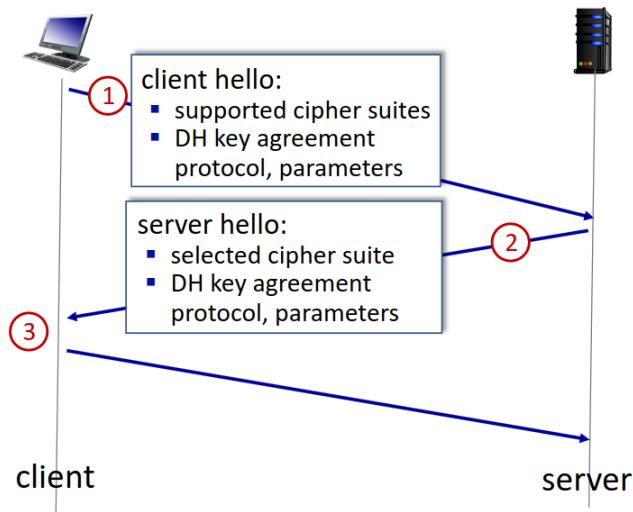
Ogni versione del protocollo TLS è dotata varie **cipher suite**, ossia vari insiemi di diverse combinazioni di algoritmi utilizzabili per la generazione delle chiavi, per la cifratura, per il MAC e per la firma digitale (es: la suite TLS\_AES\_128\_GCM\_SHA256)

In particolare, per il protocollo TLS 1.3 si ha che:

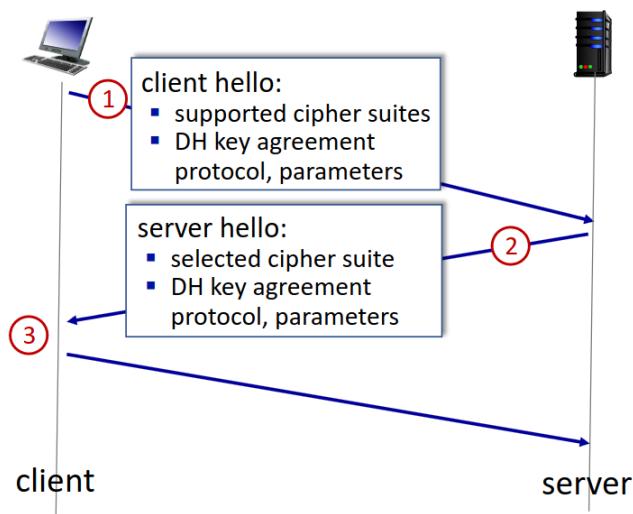
- La quantità di scelte possibili rispetto al TLS 1.2 passa da 37 a solamente 5
- Viene utilizzato l'algoritmo **Diffie-Hellman (DH)** per lo scambio delle chiavi al posto di RSA
- Viene unita la crittografia all' algoritmo di autenticazione (una sorta di "crittografia autenticata" basata sull'algoritmo AES) per i dati invece dell'uso di una cifratura seriale assieme all'autenticazione tramite MAC
- Viene utilizzato un **Hash-based MAC (HMAC)**, corrispondente al digest del record calcolato tramite SHA-2 (256 bit o 284 bit)

L'implementazione dell'handshake TLS 1.3 si suddivide in due tipologie:

- **TLS 1.3 handshake ad 1 RTT**, la quale, come da nome, richiede 1 RTT per stabilire la connessione TLS prima di poter inviare gli effettivi dati:
  1. Il client invia un messaggio di TLS client hello, **indicando** al server le cipher suite supportata e **proponendo** un protocollo di scambio chiavi e parametri
  2. Il server risponde con un messaggio di TLS server hello, scegliendo la suite di cifratura, scegliendo il protocollo di scambio chiavi e parametri e inviando il proprio certificato firmato
  3. Il client controlla il certificato del server e genera la master key che verrà utilizzata per la sessione



- **TLS 1.3 handshake a 0 RTT**, richiedente 0 RTT per stabilire la connessione TLS prima di poter inviare gli effettivi dati:
  - Il messaggio TLS client hello contiene già dati cifrati tramite l'uso della master key della sessione precedente ("ripresa" della connessione)
  - Essendo vulnerabile ai replay attack, viene utilizzata solo per richieste che non modificano lo stato del server (es: ottenere un documento)



## 6.5 Sicurezza a livello di rete (IPsec)

La suite di protocolli **IPsec** fornisce crittografia, autenticazione e integrità a livello di datagramma, sia per il traffico utente che per il traffico di controllo. Tali protocolli possono essere implementati in due modalità:

- **Modalità di trasporto**, dove soltanto il payload del datagramma è cifrato e autenticato
- **Modalità tunnel**, dove:
  - L'intero datagramma è cifrato e autenticato
  - Il datagramma cifrato viene incapsulato in un nuovo datagramma con una nuova intestazione IP ed inviato verso la destinazione
  - Chi osserva il traffico vede solo il traffico cifrato tra client e server, senza poter sapere la sorgente iniziale e la destinazione finale del pacchetto incapsulato

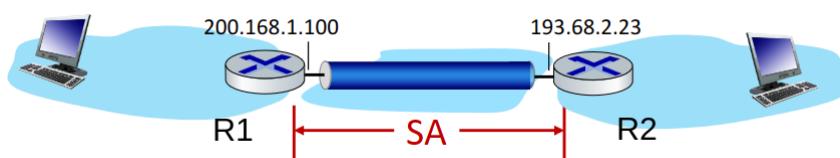


In particolare, all'interno della suite IPsec troviamo il protocollo **Authentication Header (AH)**, il quale fornisce autenticazione del mittente e integrità dei dati ma non la loro riservatezza, e il protocollo **Encapsulation Security Protocol (ESP)**, il quale fornisce anche riservatezza (ed è pertanto più utilizzato di AH).

Prima dell'invio dei dati, viene stabilita una **security association (SA)**, ossia un insieme di regole utilizzate per stabilire un percorso sicuro da effettuare dall'entità di invio a quella ricevente. Dunque, i due router devono memorizzare le informazioni sullo stato della SA. Inoltre, per via della necessità di scambio di chiavi ed altre operazioni, IPsec è **orientato alla connessione**, mentre IP no, richiedendo una gestione diversa.

**Esempio:**

- Consideriamo la seguente SA tra due router



- Il router R1 dovrà memorizzare:
  - Identificatore a 32 bit per la SA, ossia un **Security Parameter Index (SPI)**
  - Interfaccia di origine della SA, ossia **200.168.1.100**

- Interfaccia di destinazione della SA, ossia 193.68.2.23
- Tipo di crittografia utilizzato
- Chiave crittografica
- Tipo di controllo di integrità utilizzato
- Chiave di autenticazione

### 6.5.1 Protocollo ESP

Il **protocollo ESP** viene principalmente utilizzato in **tunnel mode** creando un canale crittografico riservato ed autenticato tramite una SA, venendo impiegato anche per la realizzazione di **Virtual Private Network (VPN)**, ossia una rete privata realizzata tramite un "canale virtuale" (nome derivato dalla presenza di un canale crittografato "invisibile" agli altri utenti sulla rete fisica)



#### Esempio:

- Un router vuole inviare un datagramma all'interno di un tunnel ESP, costruendo il datagramma ESP contenente il datagramma originale nel seguente modo:
  1. Viene aggiunto un trailer ESP alla fine del datagramma originale
  2. Viene cifrato il risultato ottenuto utilizzando l'algoritmo e la chiave specificati nella SA
  3. Viene aggiunge un header ESP davanti alla parte cifrata
  4. Viene creata l'autenticazione MAC utilizzando l'algoritmo e la chiave specificati nella SA, per poi aggiungerlo alla fine del nuovo datagramma
  5. Viene creato un header aggiuntivo contenente gli endpoint del tunnel
  6. Viene spedito il datagramma ESP

Per evitare la presenza di replay attack, vengono utilizzati **numeri di sequenza**:

- Alla creazione di una SA, il mittente inizializza il numero di sequenza a 0
- Ogni volta che viene inviato un datagramma viene incrementato il numero di sequenza, inserendo il nuovo valore all'interno del campo Seq # dell'header (il quale verrà anche autenticato)