Fondamenti di Telecomunicazioni T

Seconda parte

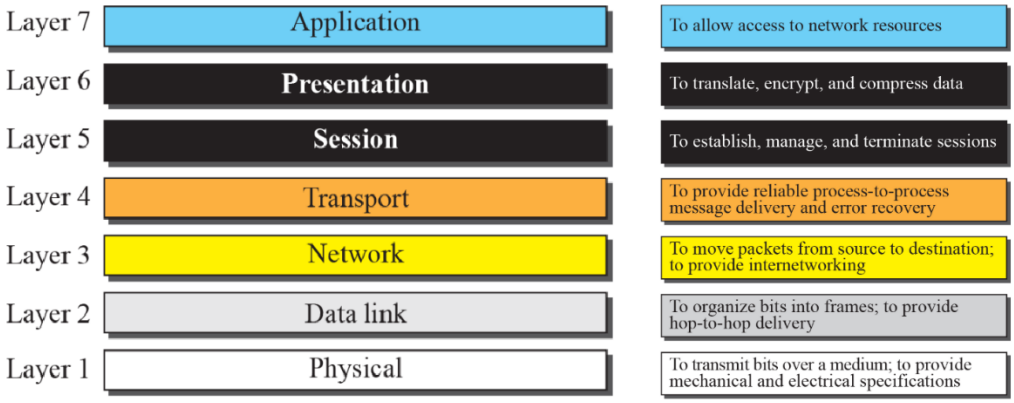
Autore: Urbinati Cristian

Contatto: cristian.urbinati@studio.unibo.it

INTRODUZIONE

IL MODELLO OSI

Negli ultimi anni '70 l'ISO (International Standard Organization) introdusse un modello standard che copriva tutti gli aspetti della comunicazione di rete, il cosiddetto modello OSI (Open Systems Interconnection).
Esso è composto di 7 livelli:

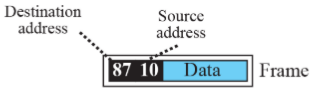


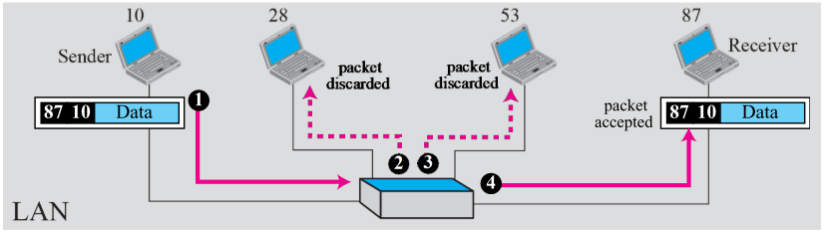
I dispositivi finali sfruttano tutti i livelli mentre quelli intermediari, come ad esempio router o switch, fino al livello 3.

L'unità di comunicazione al livello 1 è: il *bit*
L'unità di comunicazione al livello 2 è: il pacchetto (*frame*)
L'unità di comunicazione al livello 3 è: il datagramma (*datagram*)
L'unità di comunicazione al livello 4 è: il segmento (*segment*), datagramma utente (*user datagram*) o il pacchetto (*frame*) a seconda del protocollo usato a questo livello
L'unità di comunicazione ai livelli 5-6-7 è: il messaggio (*message*)

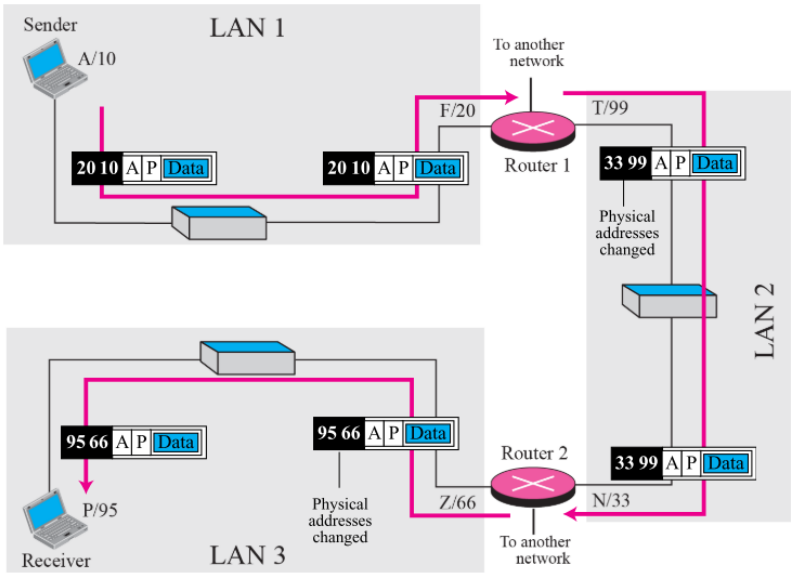
ESEMPI

ESEMPIO LAN



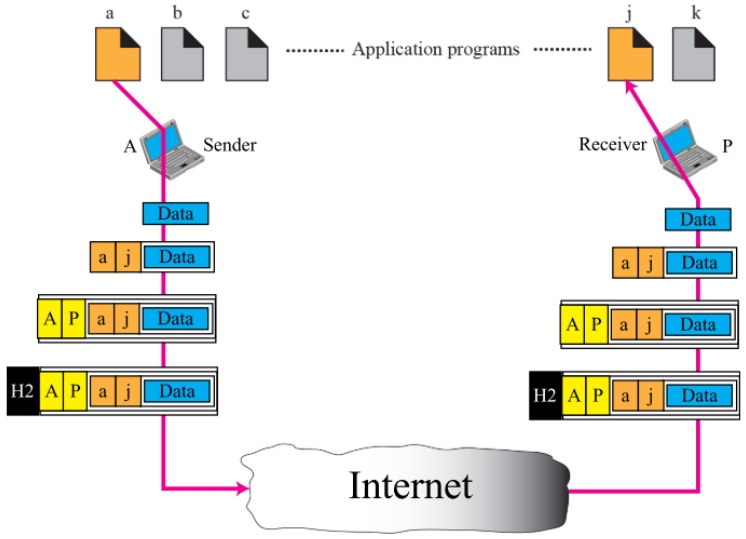


ESEMPIO INTER-LAN



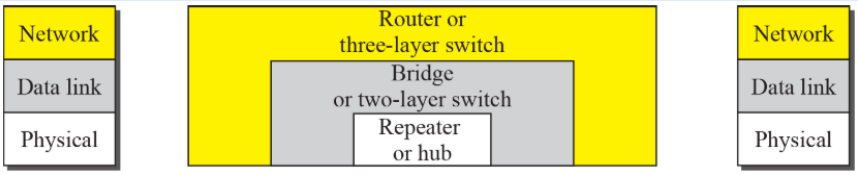
L'indirizzo fisico cambia da hop a hop, ma l'indirizzo logico rimane lo stesso

ESEMPIO INTERNET E PORTE



L'indirizzo fisico cambia da hop a hop, ma l'indirizzo logico e la porta rimangono gli stessi

DISPOSITIVI DI CONNESSIONE



RIPETITORE O HUB

Un ripetitore inoltra ogni bit, non ha la capacità di filtrare.

BRIDGE O SWITCH

Un bridge ha una tabella usata per filtrare. Esso non cambia l'indirizzo fisico (MAC) in un pacchetto.
Un bridge connette segmenti di una LAN.

ROUTER

Un router è un dispositivo di livello 3. Esso cambia l'indirizzo fisico (MAC) in un pacchetto.
Un router connette LANs o WANs per creare un internetwork.

LIVELLO 2 – LINK ETHERNET & WIFI

FRAME ETHERNET

Il pacchetto (frame) di una comunicazione ethernet è strutturato come segue:

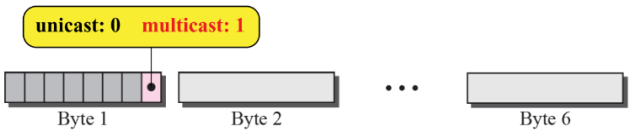
Preambolo	SFD	Indirizzo Dest.	Indirizzo Mitt.	Lunghezza o tipo	Dati e padding	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes		4 bytes

Il **preambolo** è composto da 56 bits di 1 e 0 che si alternano e che servono per la sincronizzazione a livello fisico. Lo **SFD** (Start Frame Delimiter) costituisce gli ultimi 8 bits e delimita la fine del preambolo che si conclude con la ripetizione dell'ultima cifra (es: 10101011).
Il carico di **dati** deve essere compreso nell'intervallo [46 - 1500] bytes. Se inferiore viene riempito con degli spazi.
Il **CRC** serve per determinare se ci sono stati degli errori nella trasmissione del pacchetto.
La lunghezza totale del frame ethernet è compresa nell'intervallo [64 - 1518] bytes.

INDIRIZZO ETHERNET

Un indirizzo fisico è formato da 12 caratteri esadecimali per un totale di 6 bytes ed è strutturato come segue:

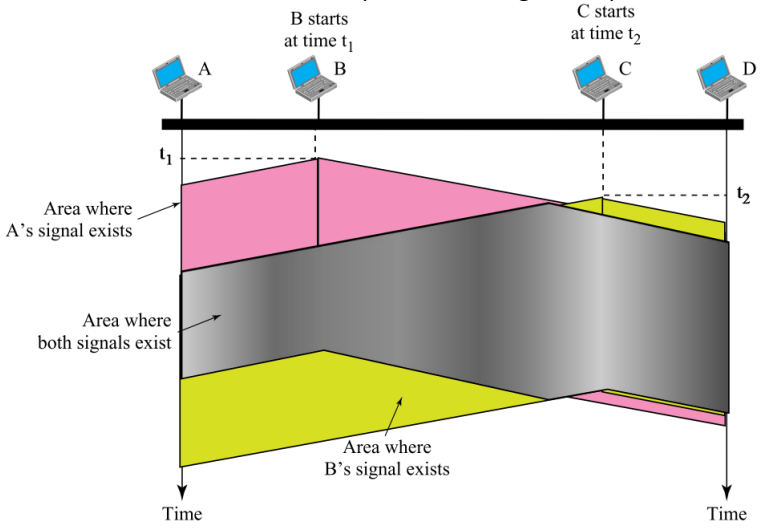
$$d_1\ d_2 : d_3\ d_4 : d_5\ d_6 : d_7\ d_8 : d_9\ d_{10} : d_{11}\ d_{12}$$



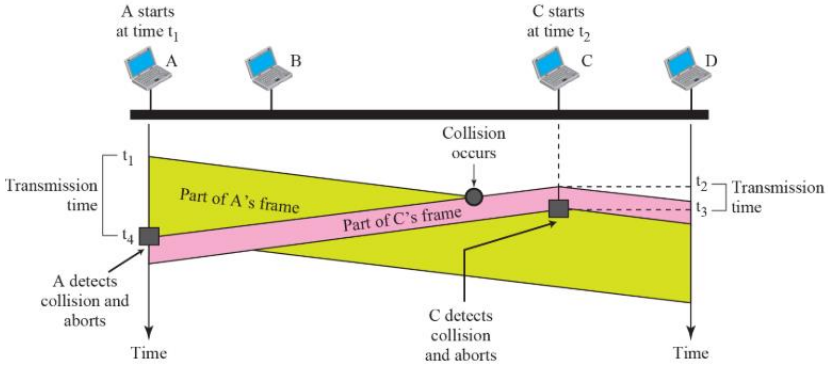
Se l'ultimo bit del primo byte è uguale a 0 significa che la comunicazione è **unicast**, cioè con un solo destinatario.
Se tale bit è uguale a 1 allora significa che la comunicazione è **multicast**, cioè con più di un destinatario.
Se tutti i bit sono pari a 1 allora la comunicazione è **broadcast**, cioè indirizzata a tutti.

COLLISIONI

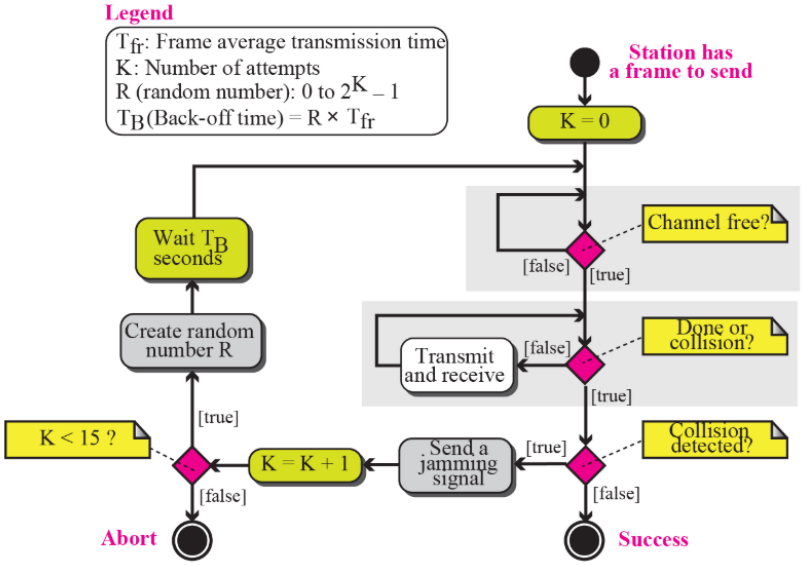
CSMA (Carrier Sense Multiple Access) è una tecnica di trasmissione appartenente ad un protocollo MAC di livello 2 il quale stabilisce che se un canale di comunicazione è già impegnato, altri dispositivi non possono iniziare una nuova comunicazione. Ma, analizzando il caso reale in cui un segnale impiega un certo tempo per propagarsi sul canale, altri dispositivi potrebbero iniziare una nuova comunicazione prima che il segnale di partenza arrivi, generando collisioni:



CSMA/CD (Carrier Sense Multiple Access with Collision Detection) è un'estensione della tecnica precedente che individua eventuali collisioni e permette l'interruzione della trasmissione.



L'algoritmo è strutturato come segue:



EVOLUZIONE TOPOLOGIA ETHERNET

1. Bus
   - Connessioni realizzate mediante cavo coassiale
   - I segmenti possono essere connessi da un massimo di 4 ripetitori
   - Un solo dominio di collisioni, è necessario CSMA/CD, half-duplex
2. Stella fisica
   - Connessioni realizzate mediante cavo RJ45
   - I nodi sono connessi ad un hub (il centro della stella) quindi maggiore affidabilità
   - Un solo dominio di collisioni, è necessario CSMA/CD, half-duplex
3. Stella logica
   - Connessioni realizzate mediante cavo RJ45
   - I nodi sono connessi ad uno switch (il centro della stella) quindi collegamenti diretti tra mitt. e dest.
   - Non ci sono possibili collisioni, è possibile il full duplex
4. Struttura gerarchica
   - Connessioni a stella logica interconnesse seguendo una politica gerarchica

CAVI

Il raggio limite tra le connessioni è dato dalla lunghezza massima del cavo usato. Alcune tipologie di cavi:

10 Mbit/s

Caratteristiche	10Base5	10Base2	10Base-T	10Base-F
Mezzo	Cavo coassiale spesso	Cavo coassiale fino	2 UTP	2 Fibra
Lunghezza Massima	500m	185m	100m	2.000m

100 Mbit/s

Caratteristiche	100Base-TX	100Base-FX	100Base-T4
Mezzo	2 STP	2 Fibra	4 UTP
Lunghezza Massima	100m	100m	100m

1 Gbit/s

Caratteristiche	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T4
Mezzo	2 Fibra a onda corta	2 Fibra a onda lunga	2 STP	4 UTP
Lunghezza Massima	550m	5.000m	25m	100m

10 Gbit/s

Caratteristiche	10GBase-S	10GBase-L	10GBase-E
Mezzo	2 Multi-mode Fiber	2 Single-mode Fiber	2 Single-mode Fiber
Lunghezza Massima	300m	10.000m	40.000m

ETHERNET 10Mb/s

- Doppino telefonico
- Codifica Manchester
- Alfabeto con codifica binaria

ETHERNET 100Mb/s

- Si passa dal doppino telefonico a al doppino categoria 5
- Si utilizza la codifica NRZ al posto della codifica Manchester
- 4 bit di informazione seguiti da 1 di ridondanza per controllare gli errori (4 su 5 sono di dati)

ETHERNET 1Gb/s

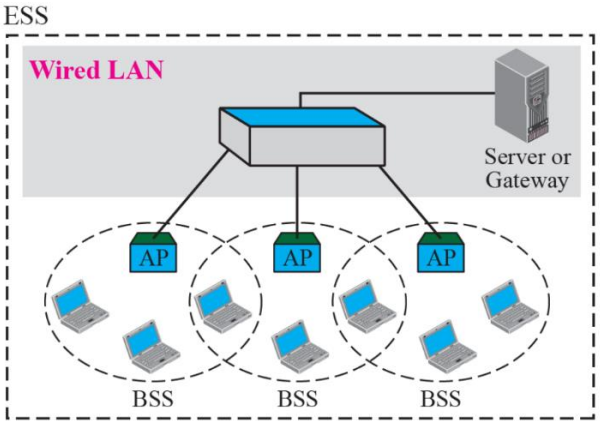
- Buffer più grande
- Circuiteria diversa: ho 4 volte la velocità di prima sia per ricevere che per trasmettere (4 * 125 * 2 = 1000)
- 8 bit di informazione seguiti da 2 di ridondanza per controllare gli errori (8 su 10 sono di dati)
- Alfabeto con codifica multilivello a 16 bit (L=5)

IEEE 802.11 (WIFI)

Il livello logico di controllo (LLC) al livello 2 e il livello 1 sono gli stessi di quelli dello standard ethernet. Il sottolivello MAC al livello 2 però è differente.

EXTENDED SERVICE SET (ESS)

Un insieme di dispositivi interconnessi è detto **Basic Service Set** (BSS); essi possono essere interconnessi direttamente o indirettamente passando attraverso un dispositivo ausiliario detto **Access Point** (AP). L'interconnessione di più BSS è detta **Extended Service Set** (ESS).



FRAME

FC	D	Address 1	Address 2	Address 3	SC	Address 4	Frame body	FCS
2 bytes	2 byte	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 – 2312 bytes	4 bytes

Addresses:
SA (chi ha generato il frame); DA (destinatario del frame)
TA (chi ha trasmesso il frame); RA (chi ha ricevuto il frame)

Versione protocollo	Tipo	Sottotipo	To DS	From DS	More flag	Retry	Pwr mgt	More data	WEP	Rsvd
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

More flag	1 se non è l'ultimo frame	WEP	Vecchio standard per la cifratura, non più usato
Retry	1 il frame corrente è stato ritrasmesso	Rsvd	Riservato
More data	1 se la stazione ha altri dati da spedire		

FRAME DI CONTROLLO

- RTS (Request To Send)

FC	D	Address 1	Address 2	FCS
2 bytes	2 byte	6 bytes	6 bytes	4 bytes

- CTS (Clear To Send) o ACK

FC	D	Address 1	FCS
2 bytes	2 byte	6 bytes	4 bytes

CANALE CONDIVISO

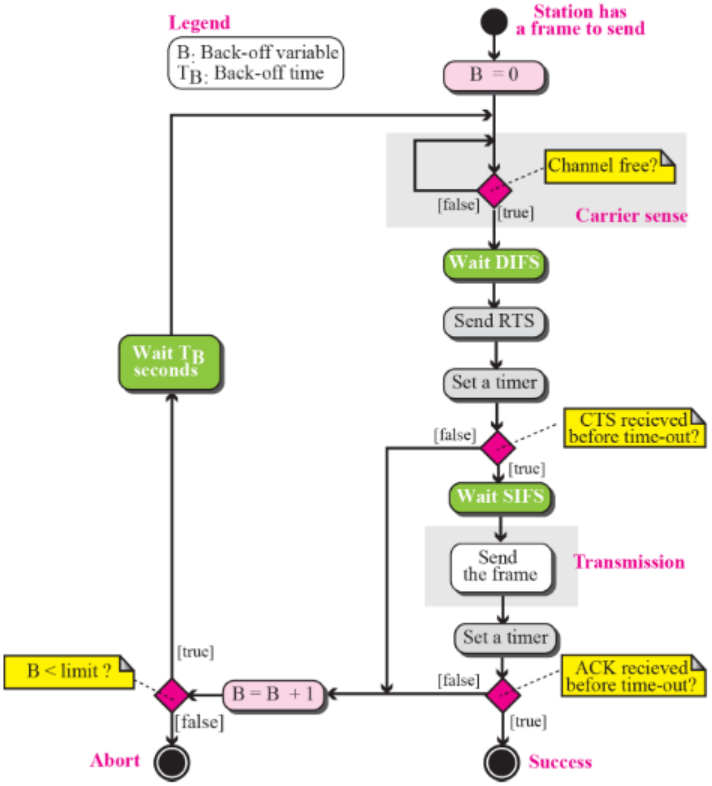
Quando un canale è condiviso esistono due possibili approcci:

- Polling (centralizzato): L'AP chiede alle stazioni se hanno frame da inviare
- Contesa (distribuito): Le stazioni devono competersi l'uso del canale, viene usato CSMA-CA

Entrambe le tecniche vengono usate nello standard 802.11.

CSMA-CA (CSMA COLLISION AVOIDANCE)

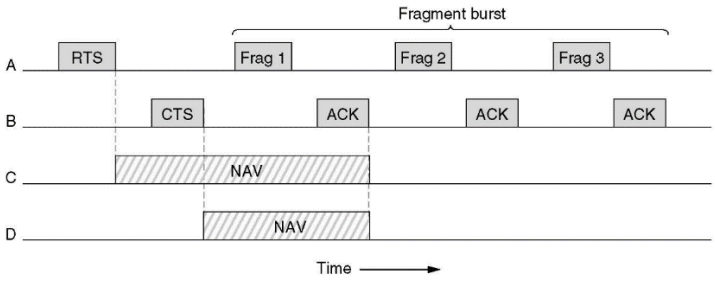
L'algoritmo di contenimento per il protocollo 802.11 è differente da quello per l'ethernet. Questo perché nel caso di comunicazione wireless vi è il problema di dispositivi possibilmente non visibili tra loro (ostacoli, lontananza), e che quindi non sanno se il canale è occupato. L'algoritmo per risolvere tale problema applica una sorta di meccanismo di prenotazione del canale tramite la comunicazione di pacchetti RTS e CTS. Esso è definito come segue:



DIFS: Tempo che il dispositivo mittente aspetta prima di inviare RTS.

SIFS: Tempo che il dispositivo ricevente aspetta prima di inviare CTS. Oppure il tempo che aspetta il dispositivo mittente prima di inviare i frammenti.

SIFS < DIFS



Qui vediamo un esempio di trasmissione di un pacchetto diviso in frammenti. Il dispositivo C è visibile come B dal dispositivo A e quindi riceve il segnale RTS e si pone in NAV. Il dispositivo D non è invece visibile da A ma lo è da B e si pone in NAV (No carrier sensing) quando B comunica il CTS.

1. Il dispositivo A aspetta DIFS prima di inviare RTS
2. Il dispositivo B aspetta SIFS prima di inviare CTS
3. Il dispositivo aspetta SIFS prima di inviare Frag1, se riceve ACK come risposta allora continua a inviare i successivi frammenti ad intervalli di tempo SIFS.
4. Dopo un tempo PIFS (> SIFS) di silenzio dall'invio dell'ultimo ACK, l'AP può prendere il canale.
5. Dopo un tempo DIFS (> PIFS) di silenzio dall'invio dell'ultimo ACK, una stazione può mandare un RTS.
6. Dopo un tempo EIFS (> DIFS) di silenzio dall'invio dell'ultimo ACK, i frame errati possono essere ritrasmessi.

LIVELLO 3 – RETE & IP

SWITCHING

Il passaggio di un messaggio da un mittente ad un destinatario implica molte decisioni. Quando un pacchetto raggiunge un dispositivo di connessione, questo deve prendere una decisione su quale porta instradare il pacchetto per farlo arrivare a destinazione.

CIRCUIT SWITCHING

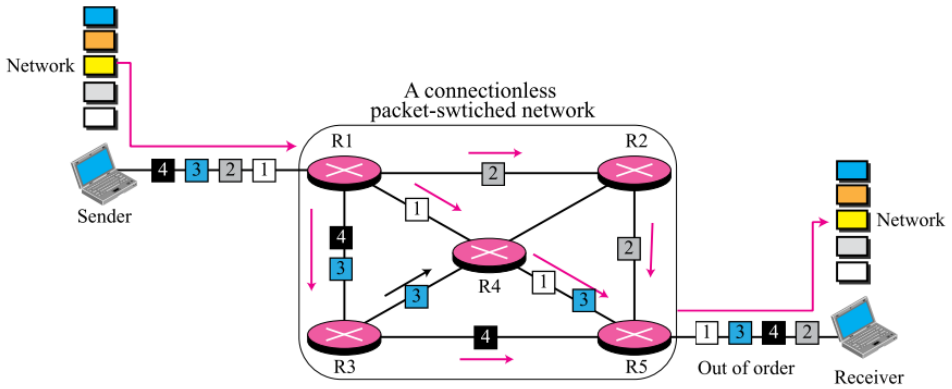
Nel caso di switching di circuito, l'intero pacchetto viene inviato al destinatario, senza essere diviso in pacchetti.
Un esempio è il sistema telefonico (di qualche anno fa) nel quale il percorso viene stabilito attraverso la digitazione del numero. Quando il destinatario della chiamata risponde il percorso è stato stabilito e il canale non può essere occupato da altri. Al momento della terminazione della chiamata il canale viene chiuso.

PACKET SWITCHING

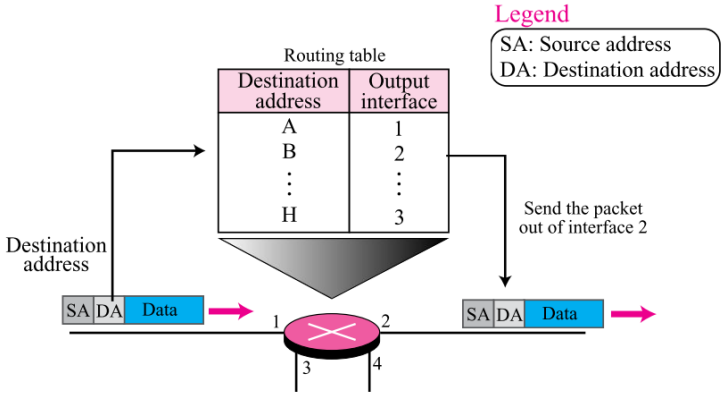
Nel caso di switching di pacchetto, il messaggio viene diviso in pacchetti dal mittente prima di essere trasmesso e viene riassemblato una volta arrivato a destinazione.
Il livello di network segue tale politica: il messaggio frame viene diviso in pacchetti detti **datagrammi**, trasferiti al destinatario e riassemblati a formare il messaggio originale.

CONNECTIONLESS SERVICE

Nel caso di rete senza connessione basata su packet-switching, l'istradamento è deciso unicamente in base all'indirizzo di destinazione del pacchetto.

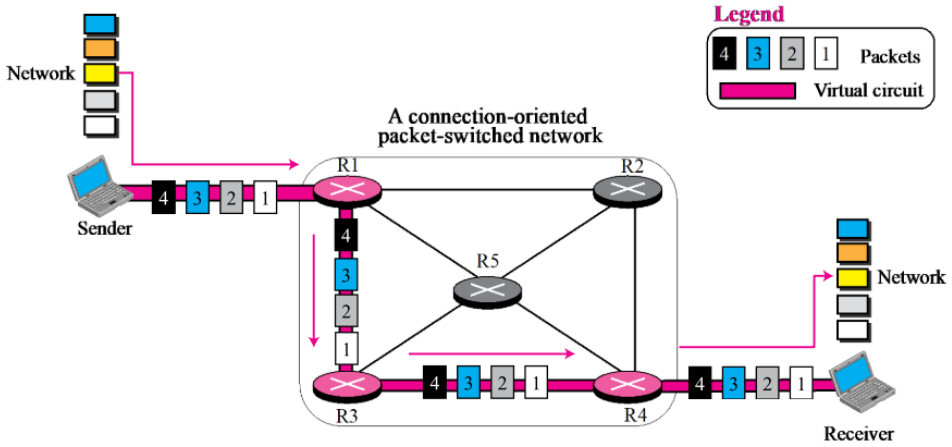


L'istradamento ai nodi viene deciso consultando una particolare tabella, chiamata **tabella di routing**, che associa all'indirizzo destinazione l'interfaccia di output che consente il raggiungimento del dispositivo destinatario. Nel caso l'entry non vi sia, il pacchetto viene spedito in broadcast.

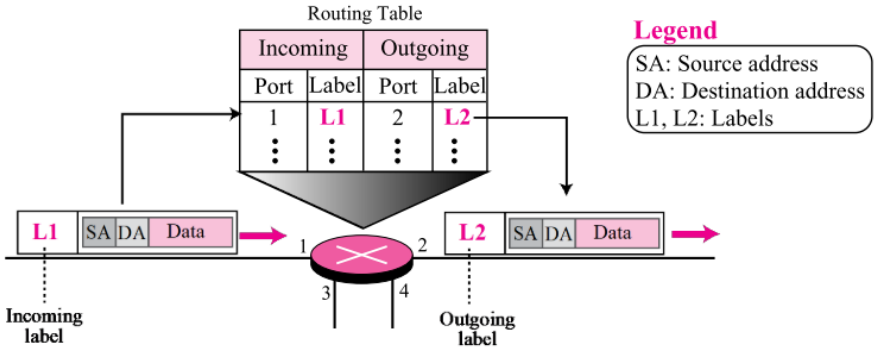


CONNECTION-ORIENTED SERVICE

Nel caso di rete orientata alla connessione basata su packet-switching, l'istradamento è basato sull'etichetta dei pacchetti.



L'istradamento ai nodi viene deciso consultando una particolare tabella, chiamata **tabella di routing**, che associa all'etichetta in ingresso in una porta, l'interfaccia di output che consente il raggiungimento del dispositivo con l'etichetta desiderata. Prima della trasmissione del pacchetto vi è una fase di setup in cui vengono spediti dei pacchetti particolari per determinare il percorso e aprire la connessione.

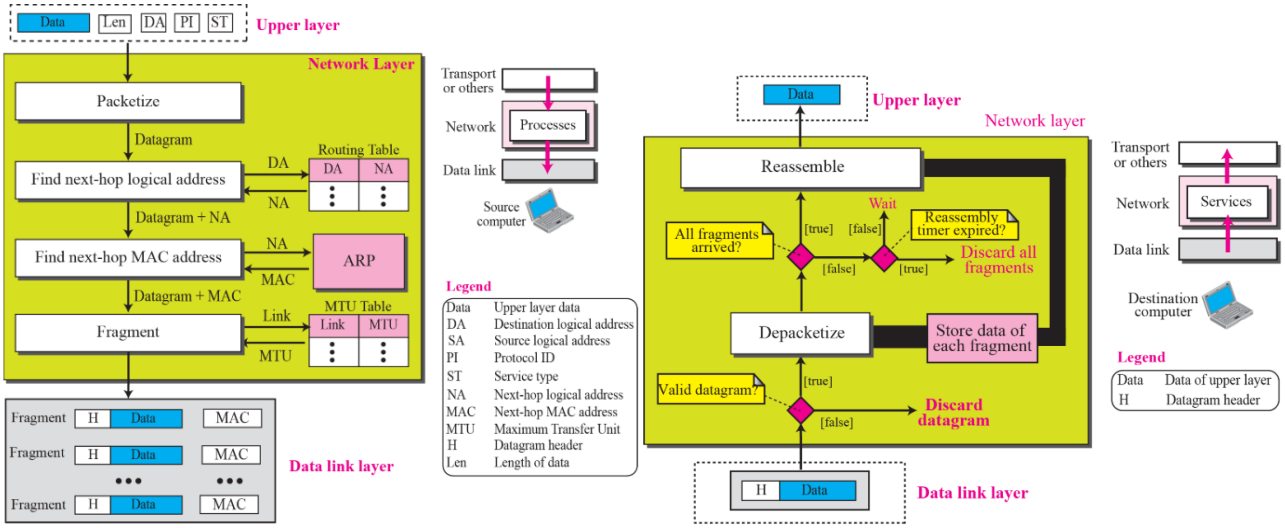


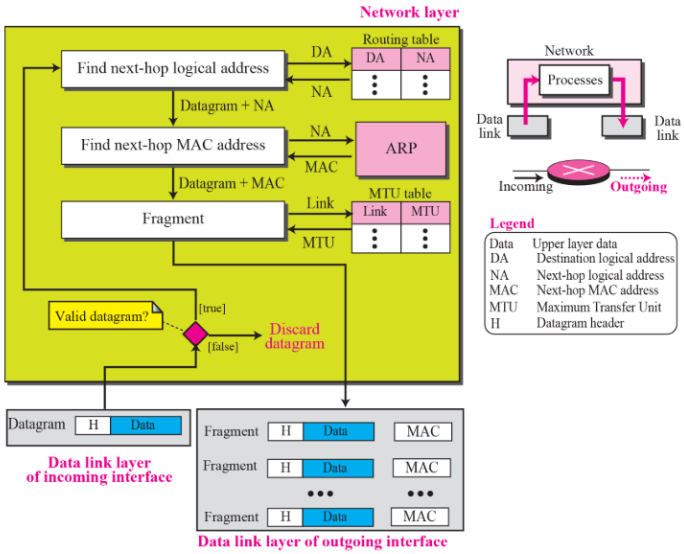
LIVELLO NETWORK

Il livello 3 è necessario per interconnettere reti con diverse tecnologie di livello 1 e 2, e permettere uno switching più efficiente e scalabile (l'indirizzo MAC è piatto, non permette di definire strutture logiche).
Gli indirizzi al livello 3 sono detti logici e sono formati da 4 byte. Esempio di indirizzo IPv4: 137.204.59.12.
Ogni NIC deve avere un indirizzo logico e uno fisico. Gli indirizzi logici possono essere di due tipi:

- *pubblici* se associati ad una specifica rete, e di conseguenza esposti sulla rete pubblica
- *privati* se associati ad una rete privata, e quindi a scopo di organizzazione interna

La corrispondenza tra indirizzi logici e fisici è mantenuta in ogni host dalla **tabella ARP** (Address Resolution Protocol).

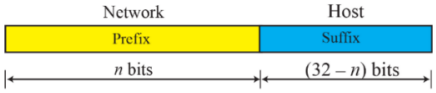




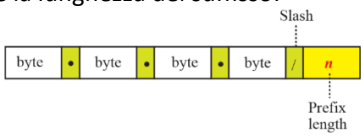
L'indirizzo IP è formato da:

- *prefisso* che indica la rete
- *suffisso* che identifica l'host all'interno della rete

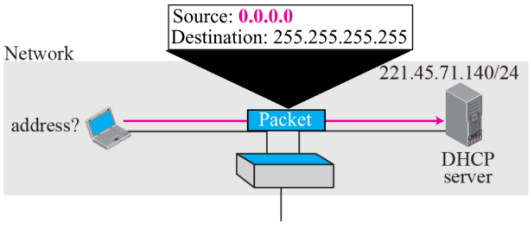
Il confine è variabile e definito dal numero di 1 di cui è composta la **netmask**:



La notazione con slash permette di definire la lunghezza del suffisso:



Esempio di richiesta in broadcast con indirizzo tutti-zero: richiesta di indirizzo al server DHCP:



Una richiesta broadcast viene bloccata dal router di confine che non la fa uscire dalla rete locale.
Un tipo di indirizzo particolare è il 127.x.x.x, gli indirizzi di questo tipo riferiscono alla macchina stessa.

Gli indirizzi privati utilizzabili sono:

Blocco	Numero di indirizzi	Blocco	Numero di indirizzi
10.0.0.0/8	16.777.216	192.168.0.0/16	65.536
172.16.0.0/12	1.047.584	169.254.0.0/16	65.536

NAT & PAT

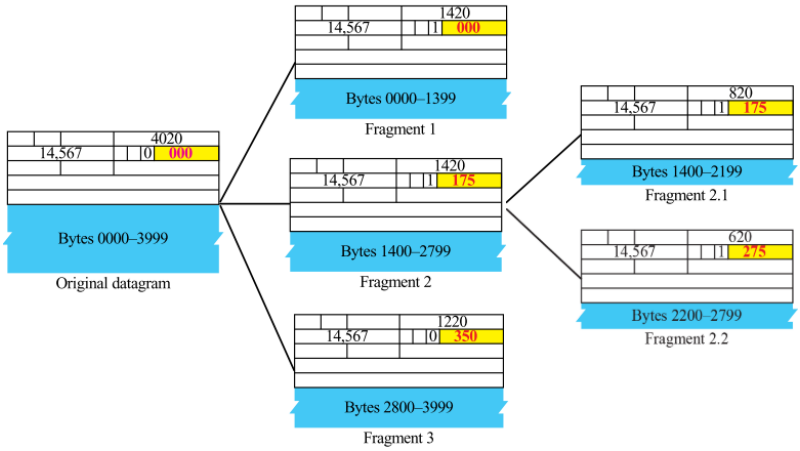
La distribuzione degli indirizzi da parte degli ISP ha creato un nuovo problema. Se il richiedente ha bisogno di un range di indirizzi più largo, l'ISP potrebbe non essere in grado di soddisfare la richiesta perché gli indirizzi precedenti o successivi sono già stati associati ad altre reti. Per situazioni di questo tipo è stata definita la tecnologia **NAT** (Network Address Translation): poiché infatti solo una porzione di computer in una piccola rete necessitano di accedere ad internet simultaneamente è possibile sostituire l'indirizzo IP in transito su un dispositivo di routing adibito al NAT con l'indirizzo esterno di tale dispositivo in modo trasparente al ricevente. Quando la risposta perviene per il dispositivo di routing essa viene reindirizzata attraverso l'indirizzo modificato.
La stessa tecnica può essere applicata alle porte, in tal caso di parla di **PAT** (Port Address Translation).

FRAMMENTAZIONE

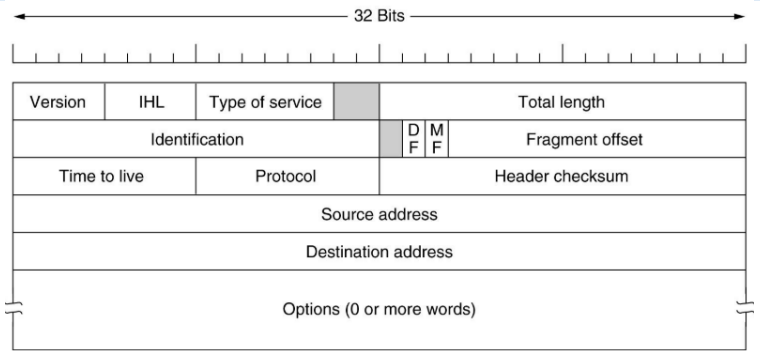
Un datagramma può passare attraverso diverse reti, ogni router decapsula l'IP dal pacchetto che riceve, lo processa e lo incapsula in un altro pacchetto. Solo i dati del datagramma vengono frammentati.

	D	M	fragmentation offset

D: Do not fragment
M: More fragment



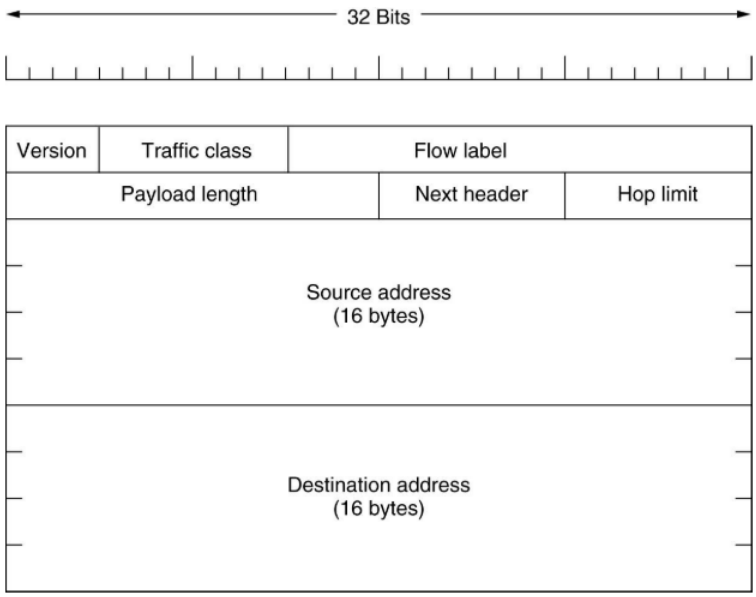
IPv4 HEADER



Option	Descrizione
Security	Specifica quanto è segreto il pacchetto
Strict source routing	Dà l'intero percorso da seguire
Loose source routing	Dà la lista dei router in cui passare sicuramente
Record route	Fa in modo che ogni router appenda il proprio indirizzo IP
Timestamp	Fa in modo che ogni router appenda il proprio indirizzo IP e il timestamp

IPv6 HEADER

Gli indirizzi IPv4 non erano più sufficienti per gestire tutti i dispositivi.
Al posto di 4 byte vengono utilizzati 16 byte per gli indirizzi.



LIVELLO 4 – TRASPORTO

UDP (User Datagram Protocol)

CARATTERISTICHE:

Si

- Implementa il meccanismo delle **porte**
- Verifica degli errori mediante checksum
- Unicast, Multicast, Broadcast

No

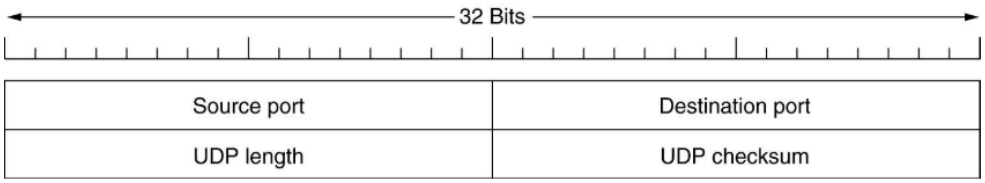
- Connessione
- Controlli sull'avvenuta ricezione del messaggio
- Riordinamento di pacchetti
- Controllo di flusso
- Controllo di congestione

VANTAGGI	SVANTAGGI
Semplice, consegna veloce dei dati	Non affidabile

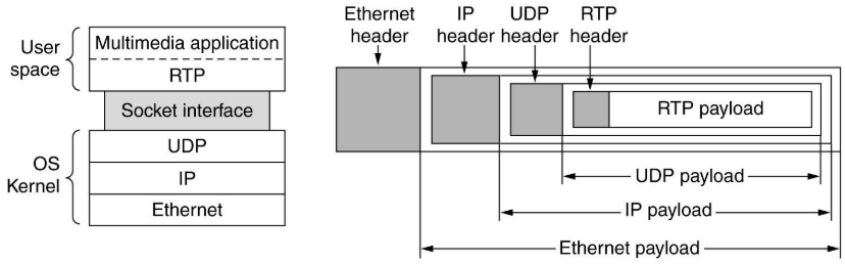
UTILIZZO

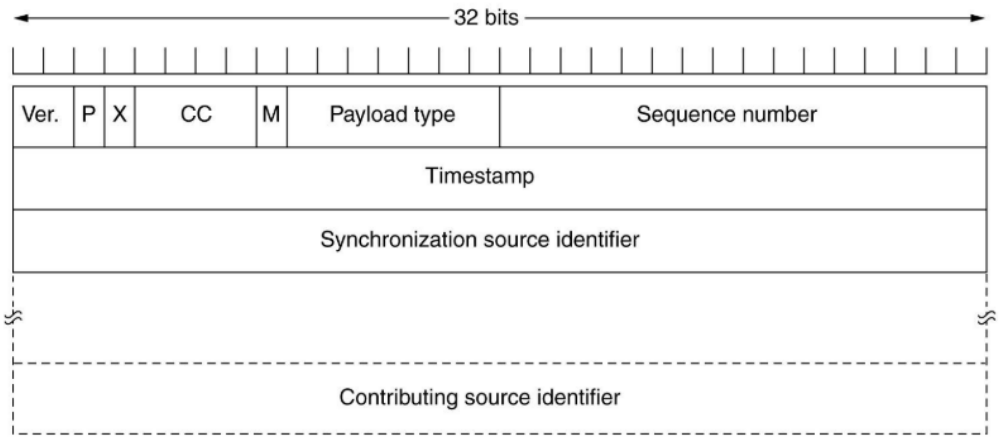
- ✓ Domain Name System (DNS)
- ✓ Dynamic Host Configuration Protocol (DHCP)
- ✓ Simple Network Management Protocol (SNMP)
- ✓ Routing Information Protocol (RIP)
- ✓ Voice over IP (VoIP)
- ✓ Real-time Transport Protocol (RTP)

HEADER



RTP





TCP (Transmission Control Protocol)

CARATTERISTICHE:

Si

- Connessione
- Implementa il meccanismo delle **porte**
- Verifica degli errori mediante checksum
- Unicast, Multicast, Broadcast
- Riordinamento di pacchetti
- Controlli sull'avvenuta ricezione del messaggio
- Controllo di flusso
- Controllo di congestione

Nel TCP i dati inviati, organizzati in segmenti, devono essere confermati da un **ACK**:

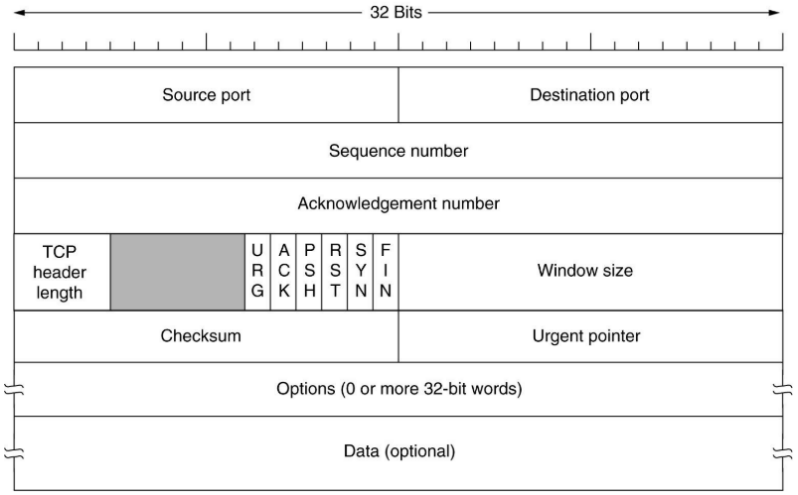
- Ogni segmento inviato è contraddistinto da un numero di sequenza (il primo byte del payload)
- Ogni ACK indica qual è il prossimo numero di sequenza che il ricevitore si aspetta di ricevere e conferma tutti quelli precedenti (ACK cumulativo): se dei segmenti si perdono, il ricevitore invia altri ACK separati per recuperarli (*DupACK*)
- Ogni segmento ricevuto genera l'invio di un ACK (esclusa **delayed ACK** per i quali si ha un ACK ogni due)
- Il tempo che intercorre tra l'invio di un segmento e l'arrivo dell'ACK si dice Round Trip Time (**RTT**)

VANTAGGI	SVANTAGGI
Affidabile	Complesso (richiede una macchina a stati), il ritardo di consegna può subire forti variazioni

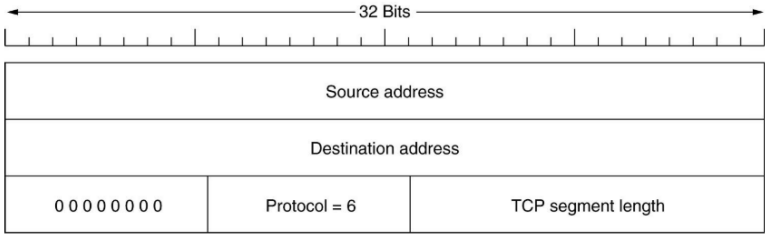
UTILIZZO

- ✓ World Wide Web (WWW)
- ✓ E-mail
- ✓ File Transfer Protocol (FTP)
- ✓ Secure Shell
- ✓ peer-to-peer file sharing

HEADER

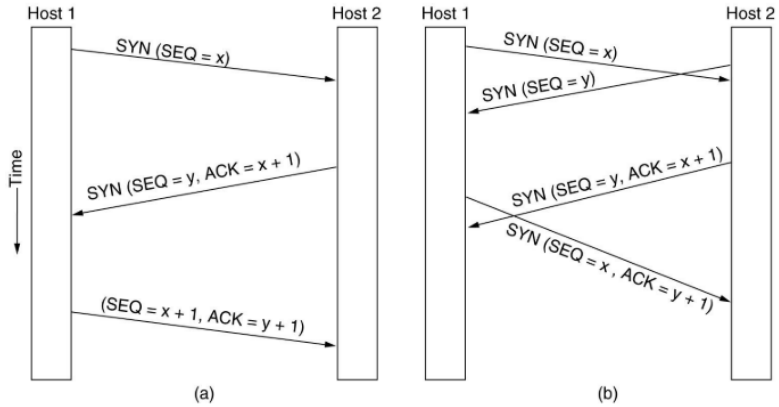


Lo pseudo-header incluso dentro il checksum è:



Per calcolare il checksum dell'header del segmento TCP, lo pseudo-header viene prima costruito e posizionato, logicamente, prima del segmento TCP. Il checksum viene quindi calcolato sia sullo pseudo-header che sul segmento TCP. Lo pseudo header viene quindi scartato. Quando il segmento TCP arriva a destinazione, il ricevente esegue lo stesso calcolo: forma lo pseudo-header, la antepone al segmento TCP effettivo e quindi esegue il checksum. Se c'è un disallineamento tra il suo calcolo e il valore che il dispositivo sorgente ha inserito nel campo Checksum, ciò indica che si è verificato un errore di qualche tipo e il segmento è normalmente scartato.

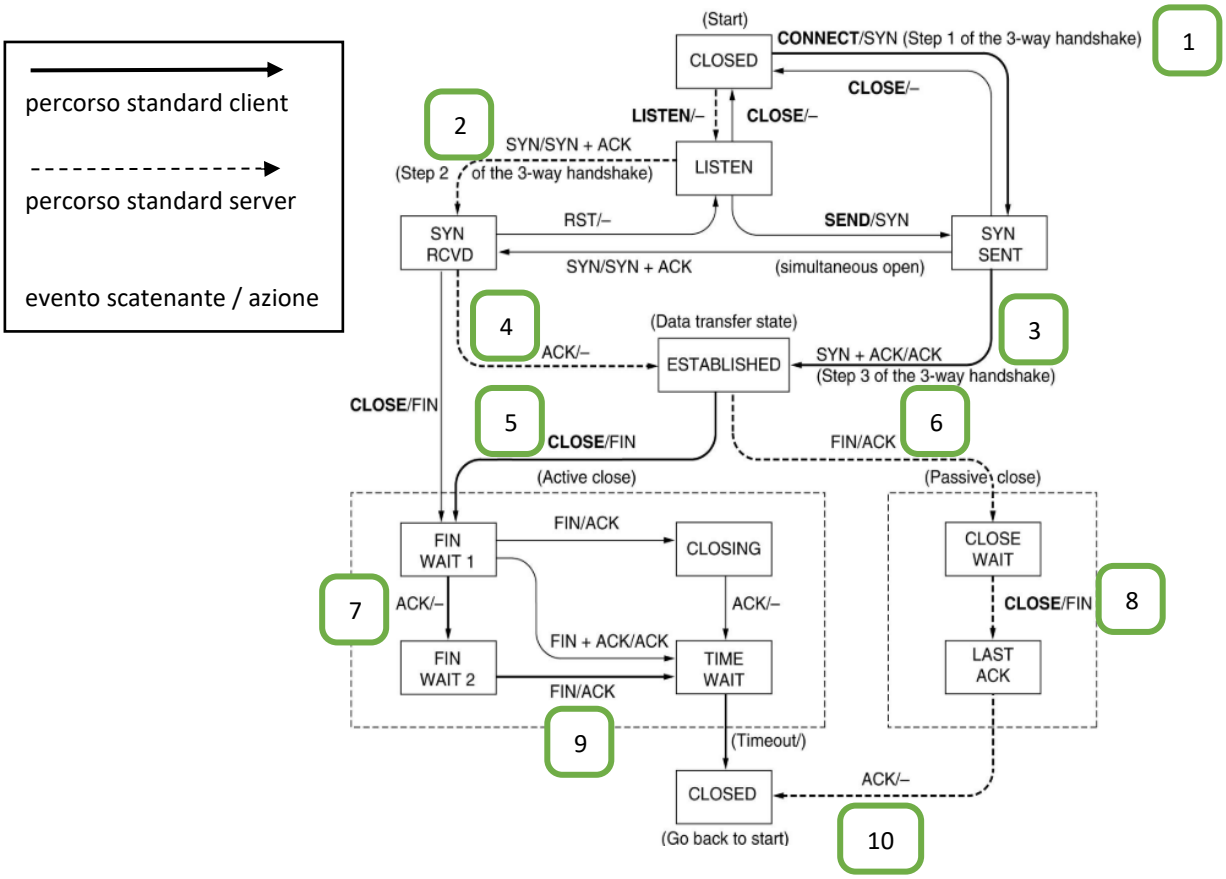
CONNESSIONE TCP



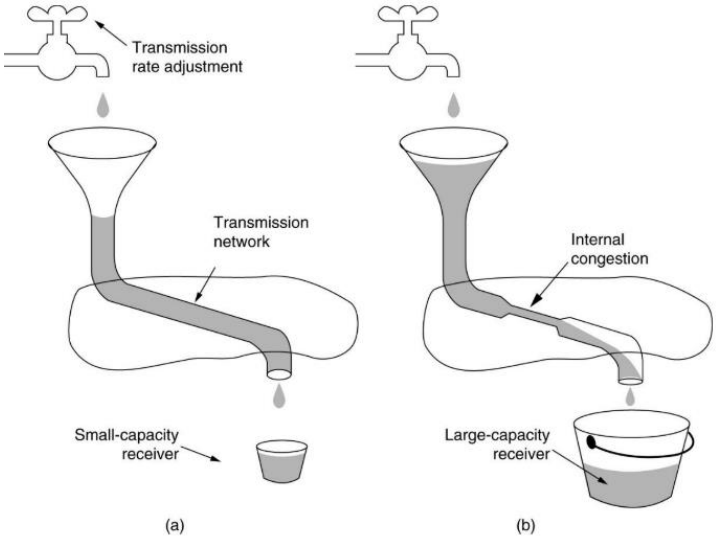
a) Stabilimento della connessione TCP nel caso normale
b) Chiamata collisione

Gli stati usati nella gestione della connessione TCP sono:

Stato	Descrizione
CLOSED	Non ci sono connessioni attive o in attesa
LISTEN	Il server è in attesa di chiamate
SYN RCVD	Una richiesta di connessione è arrivata, aspetta un ACK
SYN SENT	L'applicazione ha cominciato ad aprire la connessione
ESTABLISHED	Normale stato di trasferimento
FIN WAIT 1	L'applicazione dice che ha finito
FIN WAIT 2	L'altra parte ha accettato di terminare
TIMED WAIT	Aspetta che tutti i pacchetti muoiano
CLOSING	Entrambe le parti hanno provato a chiudere simultaneamente
CLOSE WAIT	L'altra parte ha cominciato la terminazione
LAST ACK	Aspetta che tutti i pacchetti muoiano



FINESTRE E VELOCITÀ DI TRASMISSIONE



(a) Una rete veloce alimenta un ricevitore con poca capacità (necessità di **controllo di flusso**).

(b) Una rete lenta alimenta un ricevitore con alta capacità (necessità di **controllo di congestione**).

W	Window, è il numero massimo di segmenti che possono essere spediti dopo l'ultimo confermato
Tx	Velocità di trasmissione
$cwnd$	Finestra di congestione
$rwnd$	Finestra del destinatario (controllo del flusso)

Nel caso in cui:

- $W = 1$: Invio un segmento e aspetto l'ACK prima di inviarne un altro
  $$Tx = \frac{1}{RTT}$$
- $W > 1$: Invio W segmenti, quindi alla ricezione del primo ACK ne invio un altro e così via, facendo scorrere la finestra (sliding windows).
  $$Tx = \frac{W}{RTT}$$

In generale:

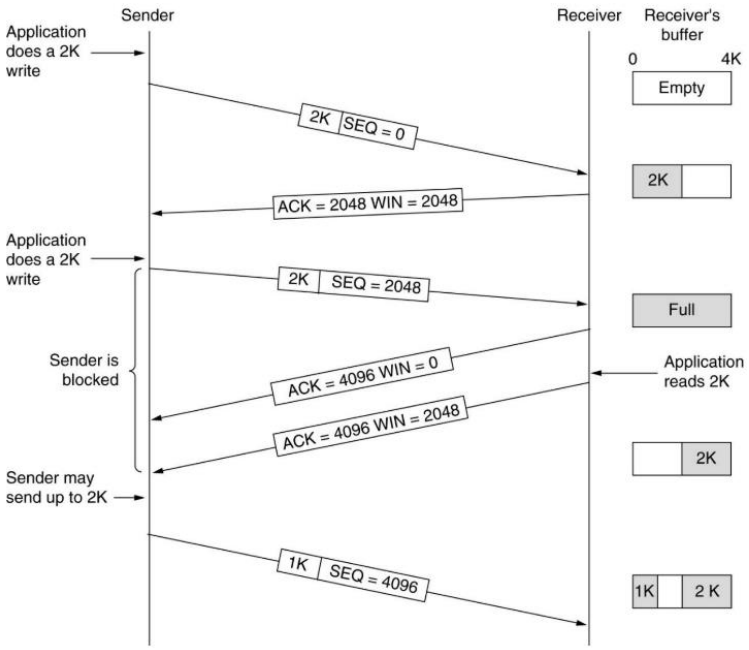
$$W = \min(cwnd, rwnd) \qquad \Rightarrow \qquad Tx = \min\left(\frac{cwnd}{RTT}, \frac{rwnd}{RTT}\right)$$

La velocità di trasmissione può essere limitata o dal controllo di flusso o da quello di congestione, tenendo presente che $cwnd$ e $rwnd$ variano nel tempo.

CONTROLLO DI FLUSSO

Receiver window ($rwnd$):

- Indica la quantità di nuovi dati che può essere inviata al destinatario
- È un parametro inviato dal destinatario ed è continuamente aggiornato
- Se $= 0$ significa che il mittente deve interrompere la trasmissione
- È opportuno aumentare il valore massimo (64kB) abilitando la TCP window scale option in presenza di elevati ritardi (RTT) e/o larga banda (default in Linux)



PERDITE

Si ritiene sia andato perso un segmento se:

- Scade l'**RTO** (Retransmission Time Out)
  ovvero se non sono arrivati ACK freschi (non duplicati) per un periodo più lungo di RTO (RTO è calcolato dinamicamante sulla base del RTT). Era l'unica condizione nelle prime versioni di TCP.
- Arrivano tre dupACK (Fast retransmit)
  questi sono generati alla ricezione dei segmenti successivi a quello mancante. Tale condizione è stata aggiunta in seguito.

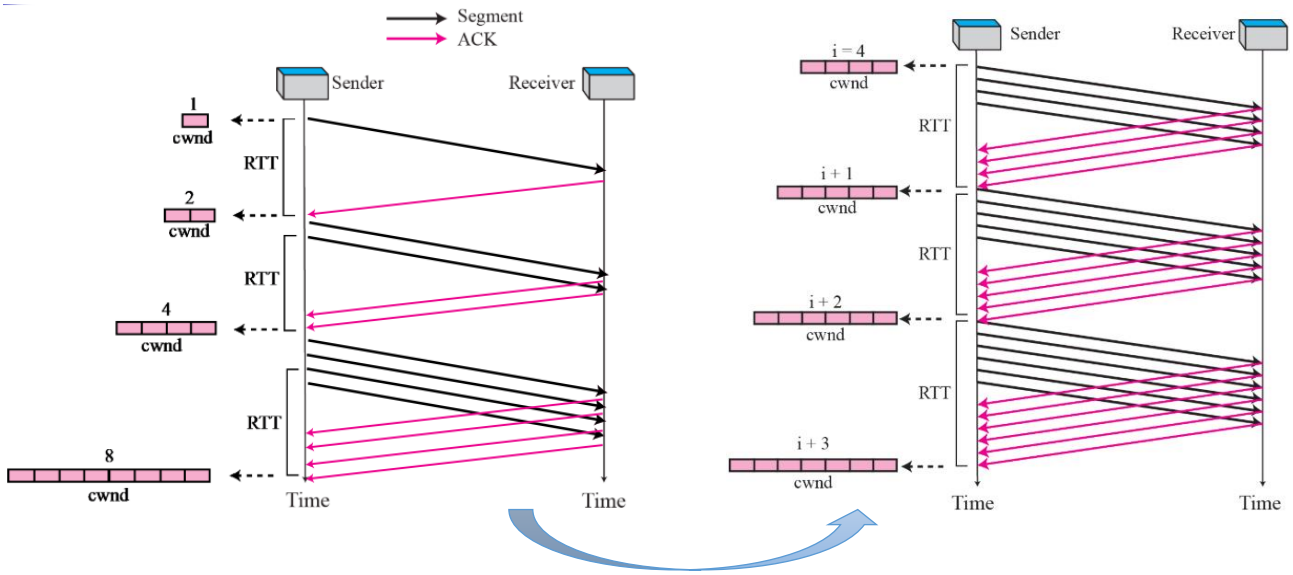
In entrambi i casi viene ritrasmesso il primo segmento non confermato

CONTROLLO DI CONGESTIONE

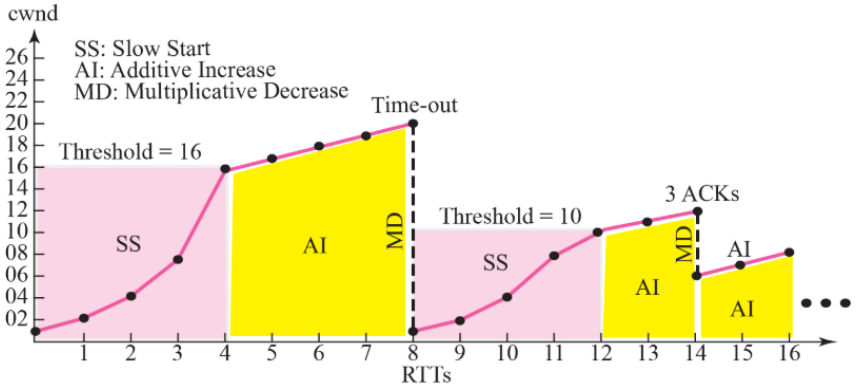
La finestra di congestione (cwnd) è il limite di quanti dati il mittente può inviare prima di ricevere un ACK.
La finestra del ricevente (rwnd) è il limite di quanti dati il ricevente può ricevere.
Il minimo tra le grandezze delle due finestre governa la trasmissione.

La finestra cwnd aumenta di uno ogni ACK ricevuto (sliding window) finché non raggiunge un valore di soglia (threshold) dopo di che incrementa di uno ogni volta che riceve tanti ACK quanto la grandezza della cwnd.

Slow Start, incremento esponenziale *Additive Increase, incremento additivo*



Nell'algoritmo per evitare le congestioni (congestion avoidance), la grandezza di cwnd aumenta esponenzialmente fino ad un valore soglia (**ssthresh**) nella fase di slow start (**SS**). Nella fase di additive increase (**AI**) la grandezza della cwnd aumenta di 1 MSS (Max Segment Size) finché una congestione non viene rilevata. In caso venga rilevata una congestione, e quindi in fase di multiplicative decrease (**MD**), se si tratta di RTO la finestra viene riportata a 0 e la soglia dimezzata, mentre nel caso di 3 dupACK vengono dimezzate sia la finestra che la soglia.
Il meccanismo AI/MD viene pertanto detto equo perché fa in modo che ci sia sempre una divisione equa della banda tra le due connessioni in caso le stesse abbiano RTT uguale. Se le due stazioni hanno invece RTT differente, il meccanismo non è equo poiché la finestra del dispositivo con RTT minore aumenta più velocemente dell'altra.



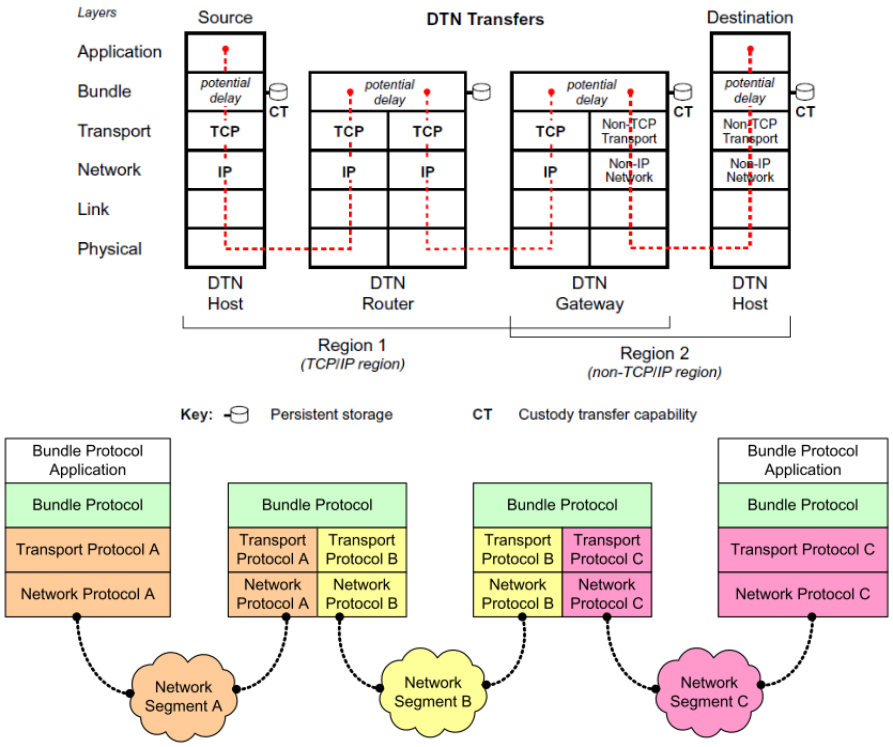
DELAY/DISRUPTION TOLERANT NETWORKING (DTN)

La **DTN** è una nuova architettura di rete per far fronte a nuove tipologie di network (challenged) che non rispettano anche solo una delle principali caratteristiche del TCP/IP:

- Connessione end-to-end (esiste sempre almeno un percorso tra mittente e destinatario)
- Round Trip Time (RTT) corto
- Poche perdite

Tale tecnologia è applicabile sia all'internet interplanetaria che per le reti challenged terrestri.
Nel 2002 parte la ricerca da parte dell'Internet Research Task Force DTN Research Group (IRTF DTNRG).

L'architettura è basata sull'inserimento del **Bundle layer** tra il livello di trasporto e quello applicativo. I pacchetti a questo livello sono detti bundles:



La connessione instaurata è una sorta di TCP/IP tra più dispositivi (hop-by-hop) resa però trasparente ai due dispositivi finali come una connessione end-to-end. È possibile che vengano usati diversi protocolli tra differenti DTN hops.
Inoltre le informazioni vengono memorizzate nella rete per due ragioni:

- Indispensabile nel caso non ci sia il nodo intermedio in maniera continua (esempio satelliti in movimento che ricevono ad intermittenza ogni tot minuti). Applicazioni in cui i dati viaggiano con il nodo intermedio sono dette "*data mule*".
- È più efficiente recuperare le informazioni con RTT lunghi.

I bundle vengono eliminati dal dispositivo corrente quando essi sono inviati al dispositivo successivo o scadono.