TCP – Transmission Control Protocol

Mattia Pacchin – mattia@v-research.it

V-ReseΛrch Edu

TCP - liv. Trasporto

- Il protocollo TCP offre un trasporto affidabile in quanto consente il controllo dell'integrità dell'informazione contenuta nei pacchetti e il controllo sull'effettiva consegna del messaggio
- TCP è dunque un protocollo orientato alla connessione
- Il software di rete che implementa TCP deve assicurare due condizioni fondamentali:
  1. certezza che il programma applicativo destinatario sia attivo
  2. garanzia che tutti i pacchetti inviati dal mittente raggiungeranno la loro destinazione

TCP

- Elementi dell'intestazione TCP:
  1. Numero di porta sorgente TCP
  2. Numero di porta di destinazione TCP
  3. Numero di sequenza
  4. Numero di conferma di ricezione (ACK)
  5. Somma di controllo TCP (checksum)
  6. Dimensioni della finestra a scorrimento TCP
  7. Bit di segnalazione (FLAG)

TCP header

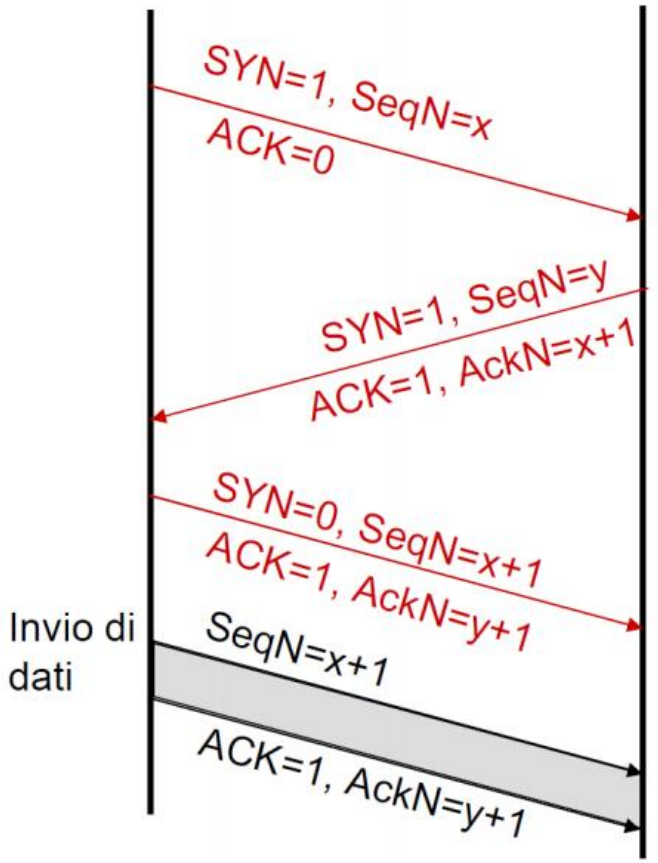
<table>
<tr><td colspan="3">Porta Sorgente(16)</td><td>Porta destinazione(16)</td></tr>
<tr><td colspan="4">Numero di Sequenza(32)</td></tr>
<tr><td colspan="4">Numero di Acknowledgement(32)</td></tr>
<tr><td>HLEN(4)</td><td>Riservati(6)</td><td>Flag(6)</td><td>Window(16)</td></tr>
<tr><td colspan="3">Checksum(16)</td><td>Urgent Pointer(16)</td></tr>
<tr><td colspan="3">Opzioni</td><td>Padding</td></tr>
<tr><td colspan="4">Dati</td></tr>
</table>

TCP

- Per capire il significato del numero di sequenza, bisogna ricordare che i segmenti TCP viaggiano in un ordine sequenziale numerato, all'interno di pacchetti IP. Il numero di sequenza nell'intestazione TCP stabilisce l'ordine che la destinazione deve usare per riassemblare i segmenti nell'ordine di partenza.
- Quando l'host ricevente ottiene un segmento TCP, risponde al mittente con un piccolo pacchetto di conferma detto ACK (ACKnowledgment). Il numero di ciascuna conferma di ricezione coincide con il numero di sequenza del pacchetto che è stato ricevuto, più uno.
- Il mancato ACK viene rilevato dal mittente: se non riceve una conferma di ricezione per ogni pacchetto che ha trasmesso, trascorso un tempo t di timeout, il mittente rimanda il pacchetto in questione.
- Nella pratica, per ridurre il numero di conferme (ACK) ed ottimizzare lo scambio dei dati, gli host scambiano anche un numero relativo alla dimensione della finestra (campo Window): questo numero indica quanti byte possono essere ricevuti e mantenuti nel buffer prima di inviare un nuovo ack. La finestra viene adattata in base alle condizioni del trasferimento (es. errori rilevati) regolando il flusso TCP.

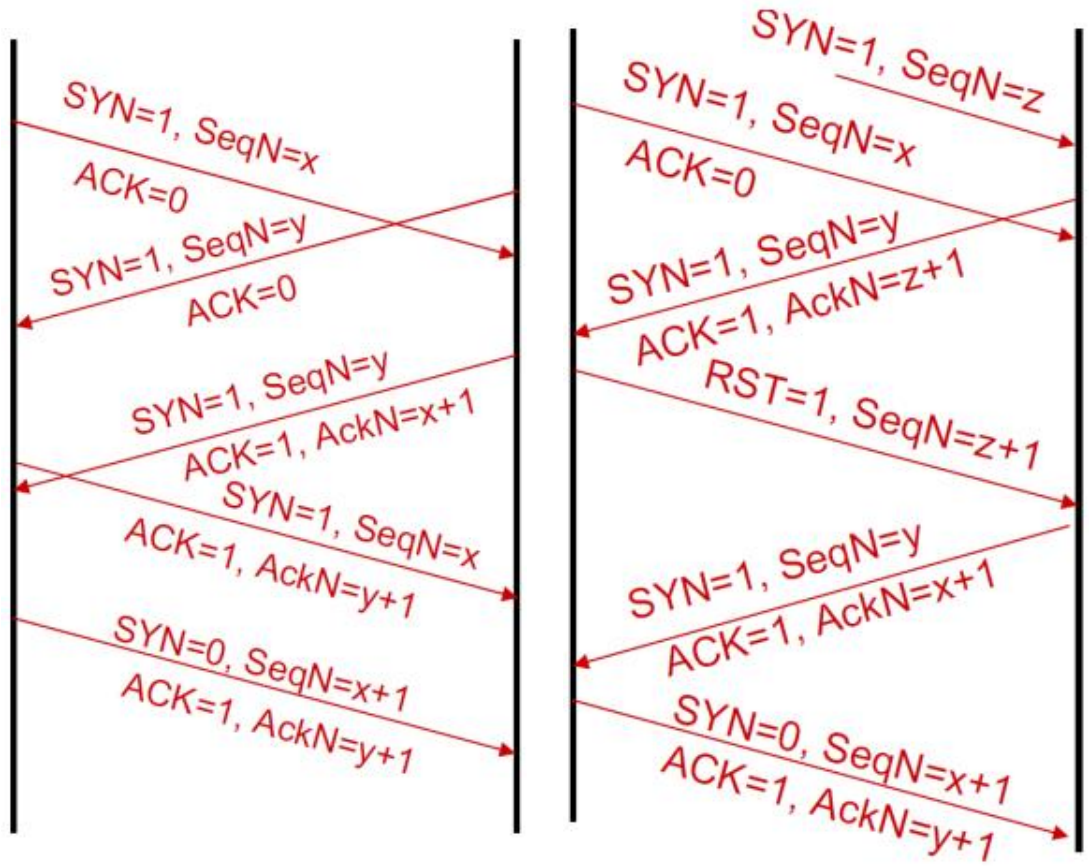
TCP – Three Way Handshake

- Il procedimento per avviare una connessione TCP può essere informalmente descritto come segue:
  1. "Iniziamo una connessione, fammi sapere se sei in linea e hai ricevuto questa richiesta"
  2. "Sì, io ho ricevuto la tua richiesta e sono pronto a stabilire il collegamento"
  3. "Va bene, ho ricevuto la tua conferma di ricezione; ecco i primi dati per te" (connessione stabilita)
- Il primo pacchetto dati ha numero di sequenza uguale all'ACK precedente



TCP – Three Way Handshake

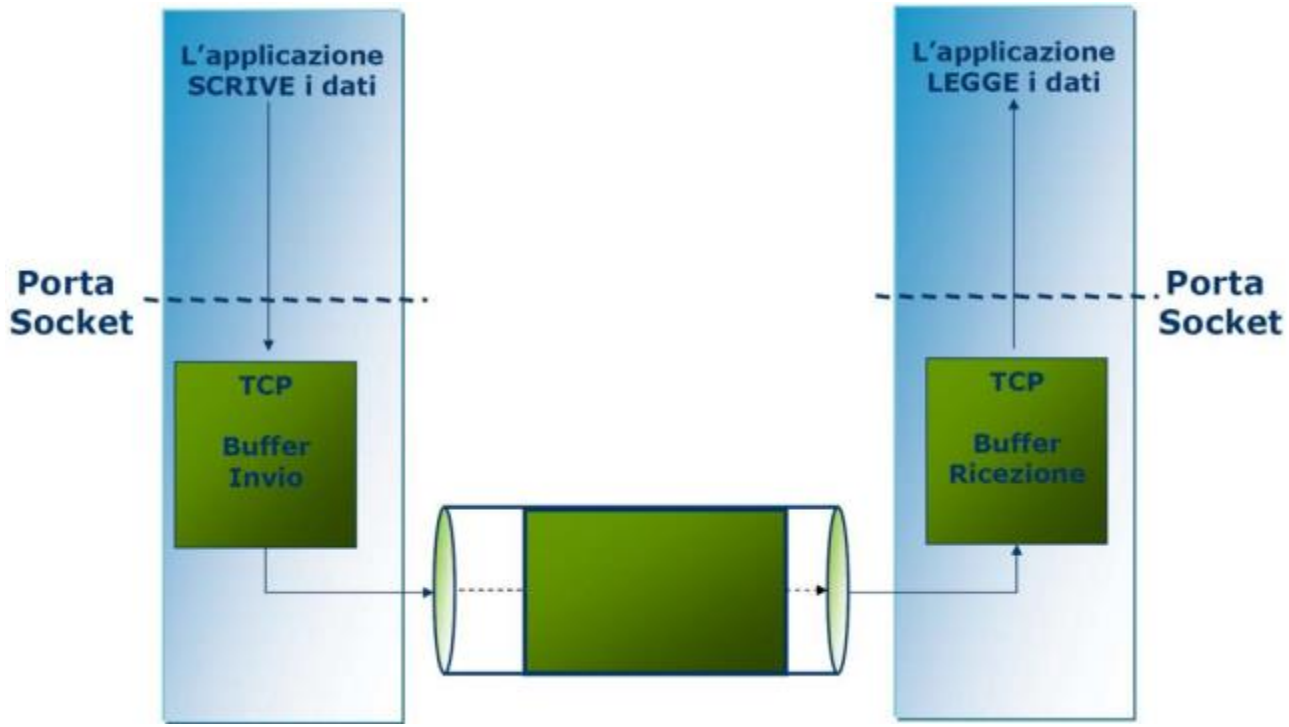
- Resiste alla instaurazione contemporanea di due connessioni
- Ignora pacchetti di apertura ritardatari
- Stabilita la connessione, il flusso dei dati è affidabile, in sequenza e bidirezionale
- Il flusso di pacchetti viene regolato tramite un buffer d'invio e uno di ricezione



V-ReseΛrch Edu

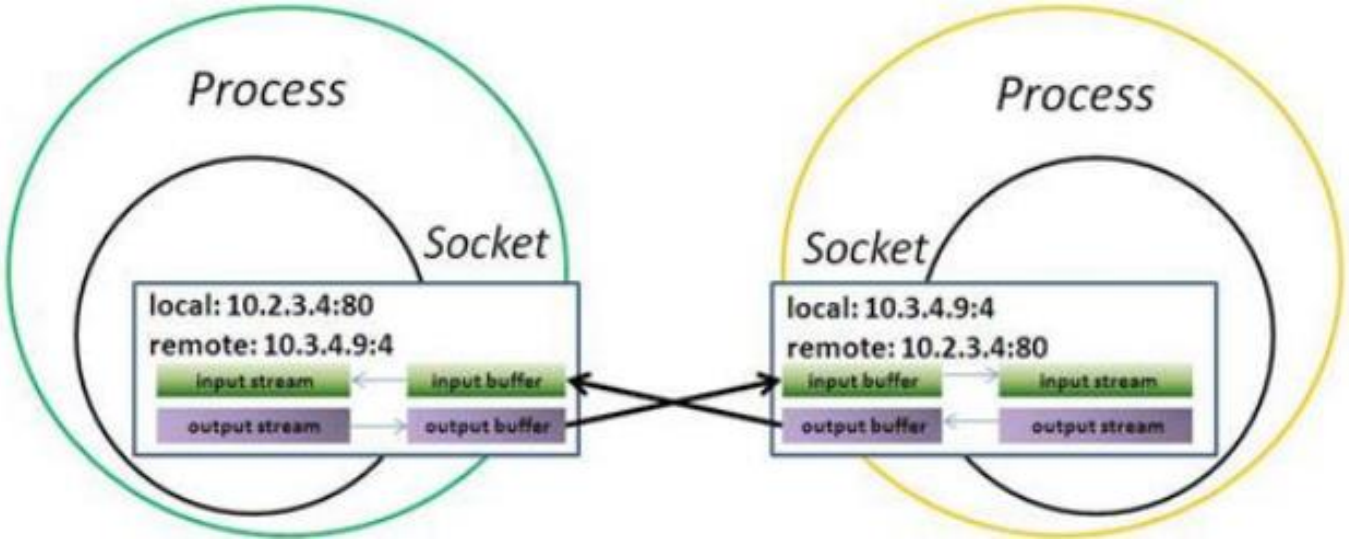
TCP - Socket

- TCP utilizza il protocollo IP per trasportare i messaggi ma, rispetto a quest'ultimo, distingue tra più destinazioni all'interno di uno stesso host mediante il meccanismo delle porte (socket)
- Socket: astrazione utilizzata per interfacciare i due terminali (endpoint) in gioco in una connessione tra due computer



TCP - Socket

- Una connessione TCP viene dunque identificata univocamente da una quadrupla:
  - <IP sorgente; porta sorgente; IP destinazione; porta destinazione>
- La notazione per esprimere la <IP, porta> è X.X.X.X:porta



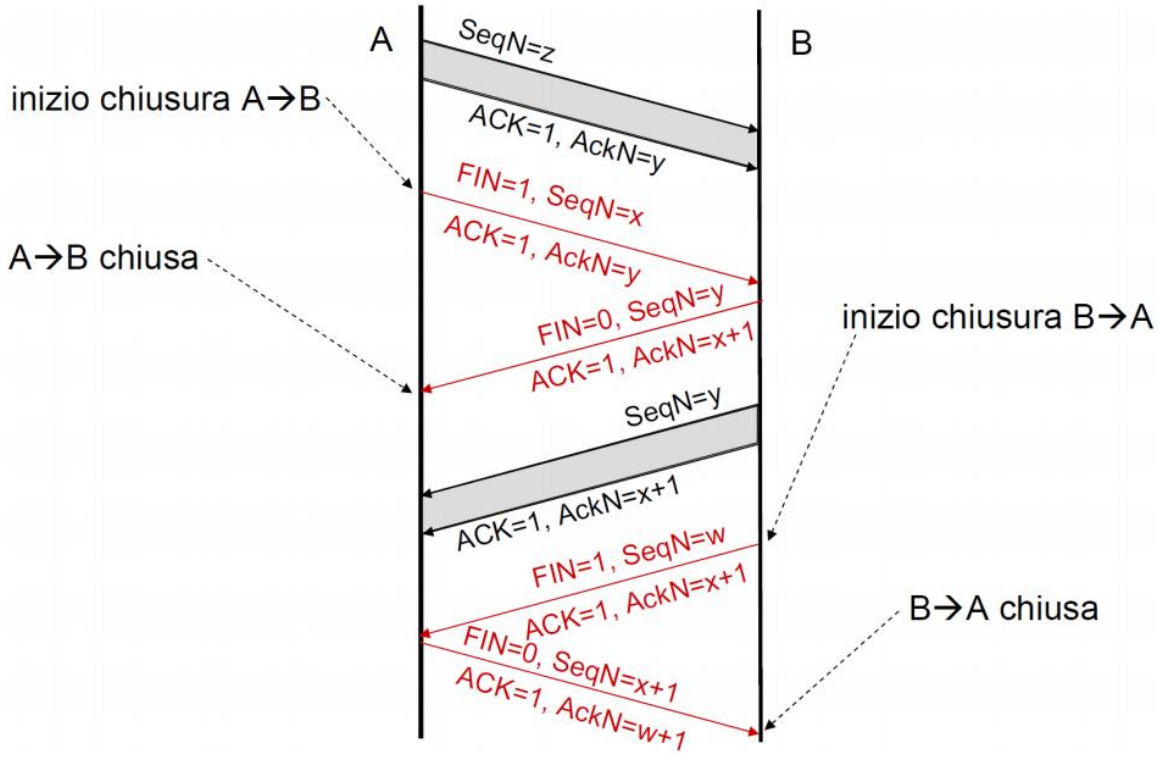
Well-known ports

- Le porte con numero inferiore a 1024 sono porte riservate per specifici servizi (well-known ports)

Port Number	Transport Protocol	Service Name	RFC
20, 21	TCP	File Transfer Protocol (FTP)	RFC 959
22	TCP and UDP	Secure Shell (SSH)	RFC 4250-4256
23	TCP	Telnet	RFC 854
25	TCP	Simple Mail Transfer Protocol (SMTP)	RFC 5321
53	TCP and UDP	Domain Name Server (DNS)	RFC 1034-1035
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)	RFC 2131
69	UDP	Trivial File Transfer Protocol (TFTP)	RFC 1350
80	TCP	HyperText Transfer Protocol (HTTP)	RFC 2616
110	TCP	Post Office Protocol (POP3)	RFC 1939
119	TCP	Network News Transport Protocol (NNTP)	RFC 8977
123	UDP	Network Time Protocol (NTP)	RFC 5905
135-139	TCP and UDP	NetBIOS	RFC 1001-1002
143	TCP and UDP	Internet Message Access Protocol (IMAP4)	RFC 3501
161, 162	TCP and UDP	Simple Network Management Protocol (SNMP)	RFC 1901-1908, 3411-3418
179	TCP	Border Gateway Protocol (BGP)	RFC 4271
389	TCP and UDP	Lightweight Directory Access Protocol	RFC 4510
443	TCP and UDP	HTTP with Secure Sockets Layer (SSL)	RFC 2818
500	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)	RFC 2408 - 2409
636	TCP and UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS	RFC 4513
989/990	TCP	FTP over TLS/SSL	RFC 4217

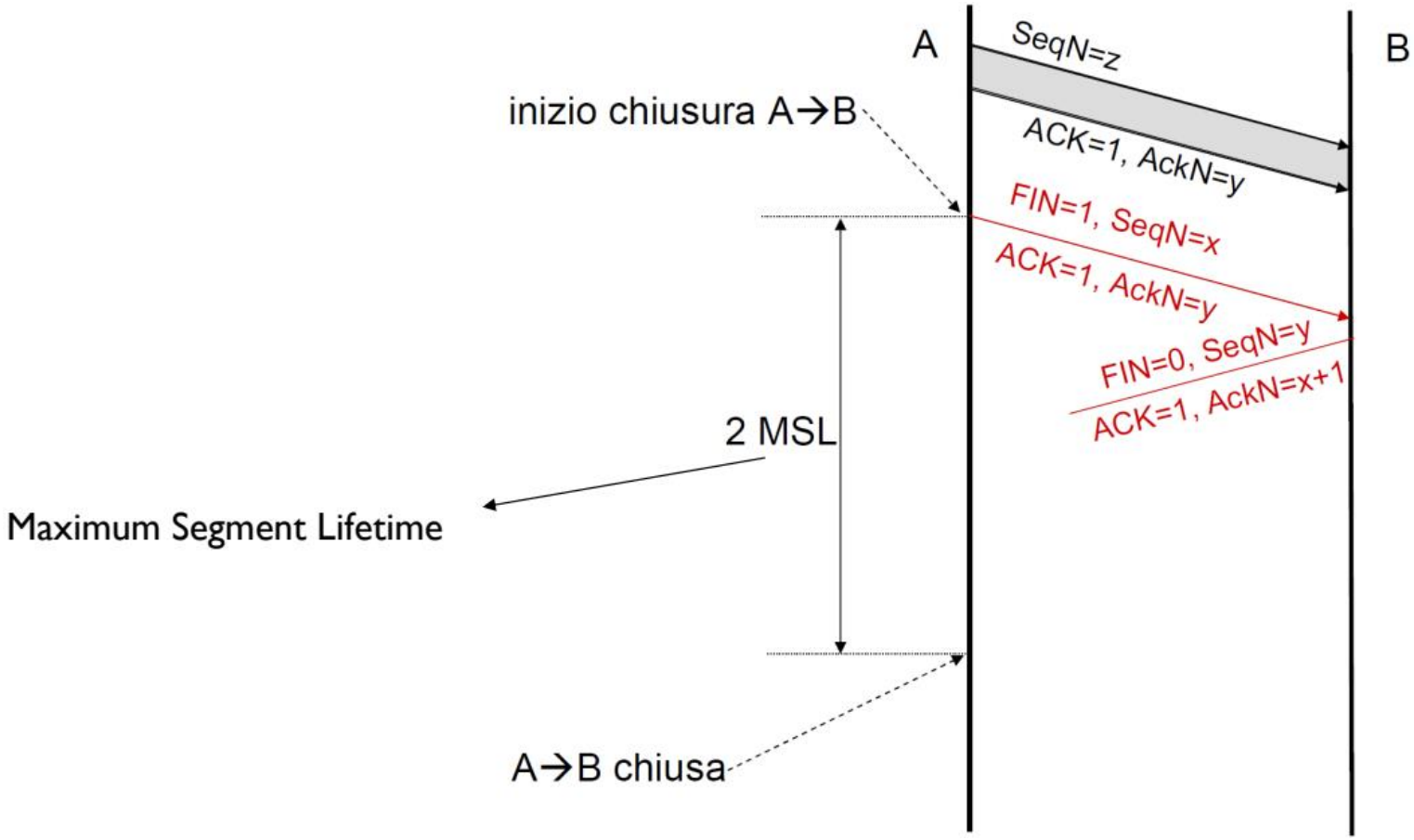
TCP – Chiusura normale

- TCP sceglie di realizzare la chiusura in modalità simplex
  1. le due direzioni vengono rilasciate in modo indipendente
  2. il TCP che intende terminare la trasmissione emette un segmento con FIN=1
  3. quando questo segmento riceve l'ACK la direzione si considera chiusa
  4. se dopo un certo tempo non arriva l'ACK, il mittente del FIN rilascia comunque la connessione, l'altra direzione può continuare a trasmettere dati finché non decide di chiudere

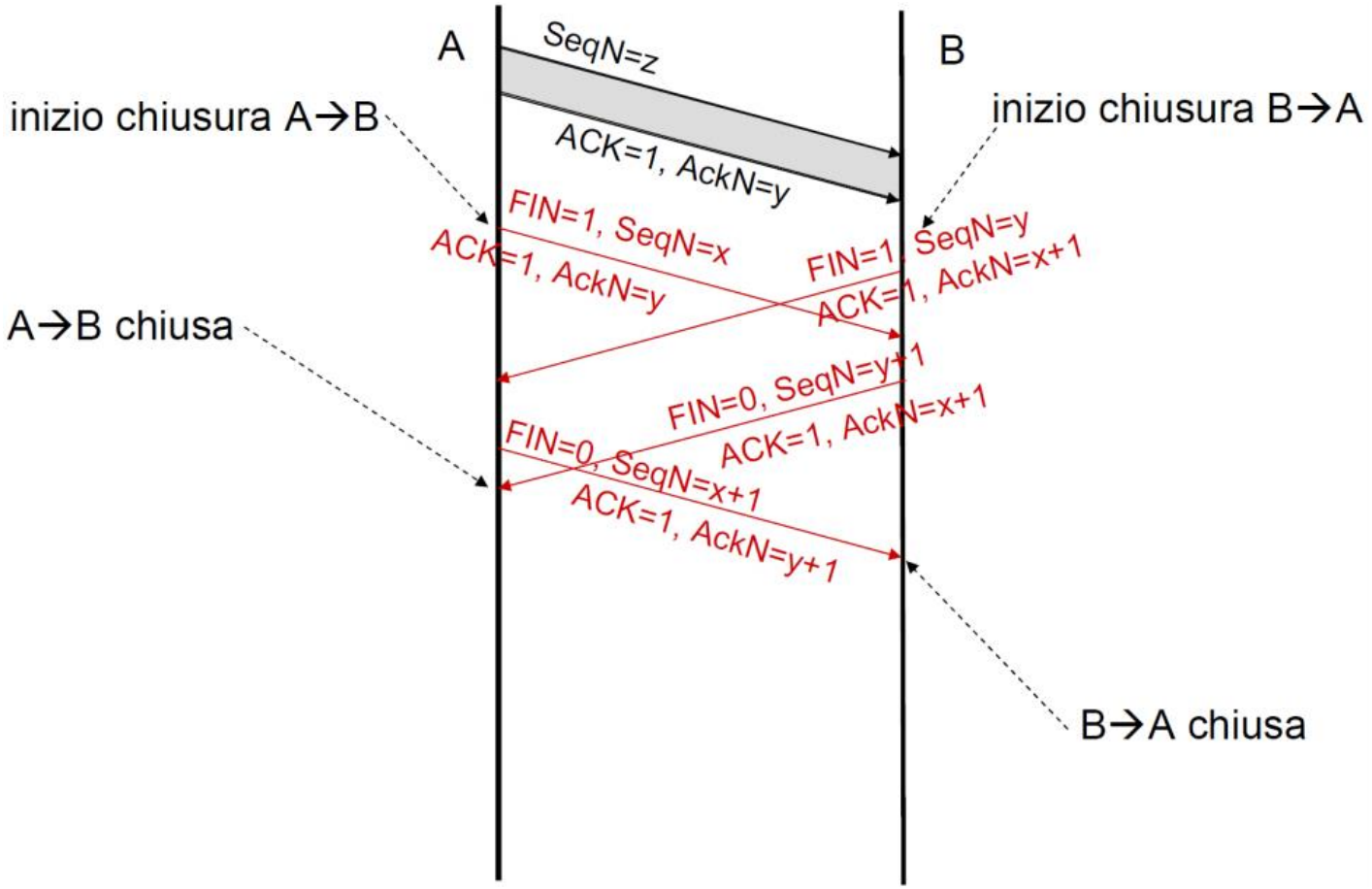


V-ReseArch Edu

TCP – Chiusura con ACK perduto



TCP – Chiusura contemporanea



TCP - Checksum

- Il checksum è un campo di controllo end-to-end: è calcolato dal mittente e verificato dal ricevitore del pacchetto che permette di capire se il contenuto del pacchetto è errato
- Aggiunge una pseudo-intestazione che contiene, fra l'altro, l'ip sorgente, l'ip destinazione e prende in considerazione i dati
- Per il TCP il calcolo del checksum è obbligatorio
- Se il pacchetto è errato, deve essere inviato nuovamente