Lo Strato di Trasporto

E' il primo strato che opera da estremo ad estremo (tra quelli visti fino adora).

Ha il compito di connettere applicazioni tra due host o tra host e un server. Queste applicazioni sono identificate da un indirizzo chiamato NUMERO DI PORTA. Di questi ne esistono vari, sono gestiti da IANA (assegna anche i blocchi degli indirizzi IP). Le prime 1023 porte sono usate da applicazioni "note" infatti si chiamano Well Known Port (es: 80→HTTP). Dalle 1024 in poi sono porte usate da applicazioni sconosciute o per stabilire delle comunicazioni (→vedi NAT, ma anche TCP). Queste ultime sono usate anche per stabilire più connessioni contemporaneamente. Ogni connessione è identificata da un SOCKET (IP destinazione + n° di porta destinazione se il segmento è UDP, IP DESTINAZIONE + n° PORTA DESTINAZIONE + IP SORGENTE + n° PORTA SORGENTE se è TCP), il n° di porta sorgente viene scelto tra i numeri > 1023, quindi la rende unica e riconoscibile. Questa tecnica rappresenta la multiplazione.

I protocolli che girano su questo strato sono

1. UDP (User Datagram Protocol)
2. TCP (Transport Control Protocol)

1. UDP:

E' un protocollo semplice, senza connessione. I segmenti possono essere perduti o consegnati fuori sequenza. E' molto usato, un esempio è il DNS.

Il segmento è molto semplice e composto da

- N° di porta origine
- N° di porta destinazione
- Lunghezza totale
- Checksum
- Dati

2. TCP

Molto più complesso, pretende di eseguire le seguenti funzioni:

× INDIRIZZAMENTO DI UN'APPLICAZIONE

× CONTROLLO DI SEQUENZA DELLE UNITÀ INFORMATIVE

× CONTROLLO E RECUPERO D'ERRORE

× CONTROLLO DI FLUSSO (regola la quantità di segmenti da mandare per non affaticare il ricevente)

× CONTROLLO DI CONGESTIONE (" " " " " " " " la RETE)

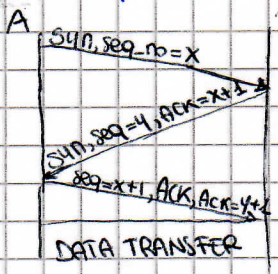
Il segmento TCP è più complesso e contiene i seguenti campi:

- PORTE DI SORGENTE e DESTINAZIONE
- IL NUMERO DI SEQUENZA DEL PACCHETTO
- IL NUMERO DI ACKNOWLEDGMENT
- LUNGHEZZA e BIT PER USI FUTURI
- FLAG → 6 bit, ognuno di essi ha un significato diverso (es il 5 è 1 → SYN se è il primo segmento di sincronizzazione)
- WINDOW → campo usato per il controllo di flusso
- Checksum
- Altri 3 campi (Urgent Pointer, Options e Padding)
- Dati

STABILIRE UNA CONNESSIONE

TCP è di Tipo "con connessione", quindi per stabilire una sessione due utenti prima devono sincronizzarsi. La Tecnica usata si chiama HANDSHAKE A TRE VIE

- PASSO 1 → host A invia un segmento SYN a B → A specifica il numero di sequenza iniziale e non invia dati
- PASSO 2 → host B risponde con un SYN ACK → specifica il numero sequenziale iniziale del server
- PASSO 3 → A risponde con un ACK che può contenere dati



Per chiudere una connessione: =D serve per liberare i socket

- Host A invia un segmento controllo FIN a B
- B risponde con un ACK
- B invia Fin
- A risponde con un ACK

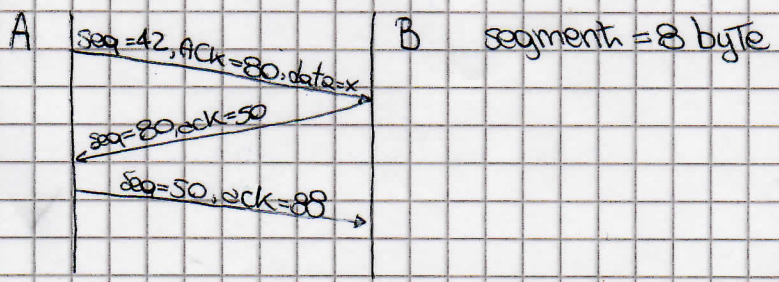
Funzioni:

- Controllo di Sequenza

Il numero di sequenza indica il primo byte del segmento nel flusso di byte. Quindi se il primo segmento ha numero 1 ed è lungo 8, il secondo sarà il 9.

L'ACK sarà il numero del prossimo byte atteso

Host A e B comunicano contemporaneamente quindi i segmenti avranno sia il nº di seq. sia e' ack [Tecnica del piggybacking].



- Controllo d'errore

Uguale al controllo del livello 2.

E' però interessante vedere il calcolo del Timeout, prima del rinvio. Il tempo viene stimato dinamicamente, in quanto dipende molto dalla situazione del traffico sul canale.

Sfrutta il Round Trip Time (RTT) e le sue oscillazioni nel tempo. Quindi

RETRASMISSION TIME OUT = RTO = RTT stimato x 4 deviazione RTT

- Controllo di Flusso

Cerca di affaticare il ricevente. Per far questo usa il campo Window, chi riceve scrive quanti segmenti è disposto a ricevere e il mittente aggiorna la propria finestra di trasmissione adattandosi alle esigenze, quindi quest'ultima è DINAMICA.

- Controllo di Congestione

TCP si preoccupa anche della RETE. Questo controllo si compone di due fasi:

1. Slow start: un host invia i segmenti con velocità sempre più alta per testare la rete. Fino a che riceve i riscontri la aumenta, altrimenti entra nell'altra fase.
2. Congestion Avoidance: i segmenti che non ha ricevuto riscontro indica che il protocollo ha superato la soglia di velocità consentita

Questo modo di "Testare" la rete è molto efficiente, statisticamente se ci sono più connessioni contemporanee, le riconoscerà suddividerà equamente.