Appunti di Sistemi Operativi e Reti

Domande e risposte – Parte di Reti (Network)

Capitolo 1 – Introduzione alle Reti

1) Cosa si intende per Rete di Elaboratori?

Una rete è un sistema di collegamenti che permette ai dispositivi di calcolo interconnessi di scambiare dati e condividere le risorse tra di loro. Questi dispositivi utilizzano un insieme di regole, chiamato protocollo di comunicazione, per trasmettere informazioni tramite tecnologie fisiche o wireless.

2) Quali sono gli elementi (o componenti) di una rete?

Gli elementi di una rete sono:

→ End Devices: chiamati anche "Host" e sono gli elementi di rete che inviano e/o ricevono messaggi, come ad esempio PC, smartphone, tablet, telefono IP, server ed ecc. Per distinguerli l'uno dall'altro, ogni dispositivo sul terminale viene identificato in rete mediante un indirizzo e quando un dispositivo terminale avvia la comunicazione utilizza l'indirizzo del dispositivo terminale di destinazione per specificare dove inviare il messaggio.

→ Dispositivi Intermedi: dispositivi che assicurano il flusso dati da un dispositivo all'altro, come ad esempio router, switch, modem, hub, bridge, access point, wireless access point ed ecc.

→ Collegamenti: elementi della rete che permettono la transizione dei pacchetti dal mittente (host che invia un messaggio) al destinatario (host che riceve un messaggio), come ad esempio cavi in rame (dati codificati mediante impulsi elettrici), fibra ottica (dati codificati mediante impulsi luminosi), cavo

seriale e wireless (dati codificati mediante onde radio).

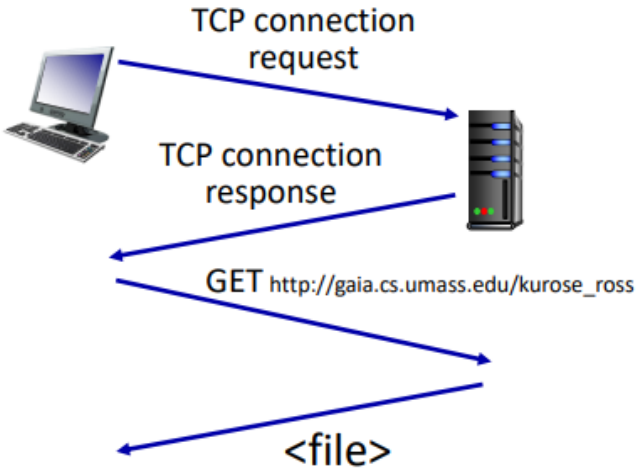
→ Servizi: varie applicazioni e/o protocolli di rete, come HTTP, HTTPS, FTP, FTPS, DNS, DHCP, TCP, UDP, IP, ARP.

3) Cosa si intende per rete Internet?

La rete Internet è una rete di telecomunicazioni che connette vari dispositivi o terminali in tutto il mondo, rappresentando dalla sua nascita uno dei maggiori mezzi di comunicazione di massa, grazie all'offerta all'utente di una vasta serie di contenuti potenzialmente informativi e di servizi. È una tipologia di rete informatica che utilizza il protocollo TCP/IP, per collegare tra loro più reti locali o geografiche.

4) Cosa si intende per protocollo di comunicazione?

Un protocollo di comunicazione è un insieme di regole che permettono la modalità di scambio di dati e informazioni tramite tecnologie fisiche o wireless.
Esempio:



5) Descrivere la funzione di invio dell'host

Il procedimento avviene nella seguente maniera:
→ accetta il messaggio relativo a tale applicazione;
→ divide tale messaggio in frammenti, chiamati pacchetti, con lunghezza L bit;
→ trasmette i pacchetti nel livello di accesso alla rete con velocità di trasmissione R;
→ il tempo necessario per trasmettere L – bit pacchetti è dato dal rapporto tra lunghezza di ogni singolo pacchetto L e la velocità di trasmissione R.

Formula: $T = L/R$

6) Descrivere il ruolo del livello di accesso alla rete

Il livello di accesso alla rete si occupa di recapitare i pacchetti prodotti dal livello superiore a questo, quindi al livello Internet.

7) Descrivere il ruolo del livello di Internet

Il livello di Internet ha il compito principale di spedire i pacchetti di informazione verso ogni nodo di destinazione presente in rete.

8) Quali sono le due funzioni del nucleo della rete?

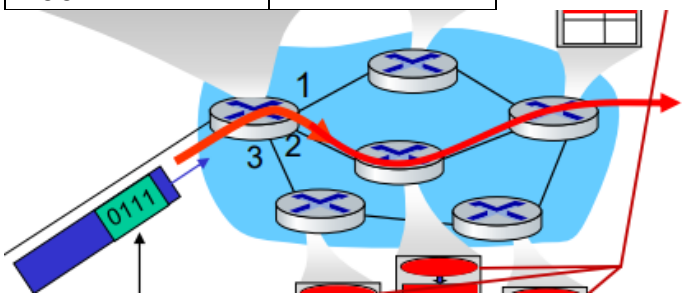
Le due funzioni del nucleo della rete sono:

→ Routing: L'instradamento (o routing) è il processo di selezione del percorso in qualsiasi rete. Una rete di elaboratori è composta da numerose macchine, chiamate nodi, e percorsi o collegamenti che li collegano e per questo motivo la comunicazione tra due nodi in una rete interconnessa può avvenire attraverso molti percorsi diversi.

→ Forwarding: è l'operazione che permette il trasferimento dei dati da un computer ad un altro mediante una specifica porta di comunicazione.

Esempio: tabella di inoltro locale

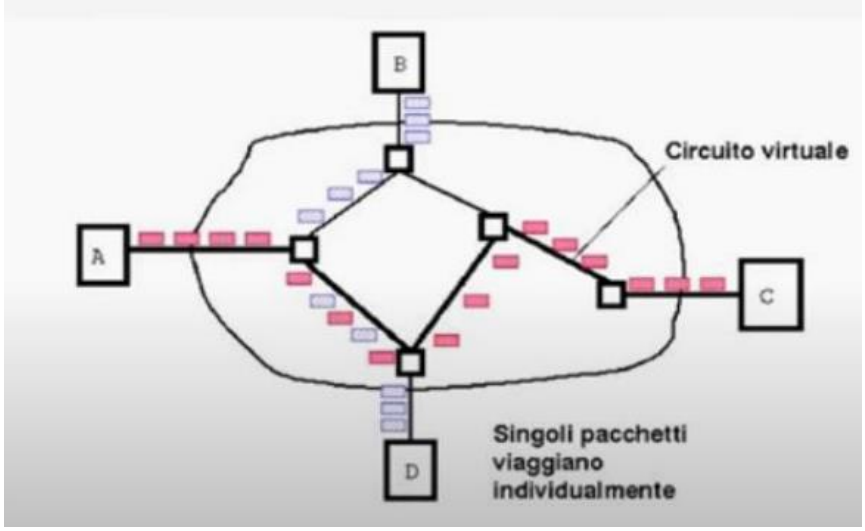
Header Value	Output Link
0100	3
0101	2
0111	2
1001	1



9) Definire la commutazione di pacchetto (packet switching). Quali sono i vantaggi e svantaggi di packet switching.

La commutazione di pacchetto prevede la suddivisione di un messaggio in più parti (pacchetto o frame) prima di inoltrarlo in rete attraverso un percorso non definito. Ogni pacchetto dati seguirà una propria strada, rimbalzando tra i nodi della rete prima di raggiungere il destinatario. Il nodo di destinazione ordinerà i pacchetti e ricostruirà il messaggio (grazie al protocollo TCP). Il vantaggio di tale tecnologia è la tolleranza ai guasti, in cui i router, grazie alle tabelle di routing, gestiscono le informazioni circa lo stato dei nodi: in base a queste

informazioni si può stabilire di volta in volta il miglior percorso da seguire nel minor tempo possibile. Grazie alla ridondanza se un percorso si guasta, i messaggi possono essere inviati su un percorso diverso. Gli svantaggi di tale tecnologia sono ritardo (dovuti al tempo di propagazione, di trasmissione, di elaborazione e alla latenza) e accodamento dei pacchetti (le code si verificano quando il lavoro arriva più velocemente di quanto possa essere servito).



10) Definire la commutazione di circuito (circuit switching). Quali sono i vantaggi e svantaggi di circuit switching.

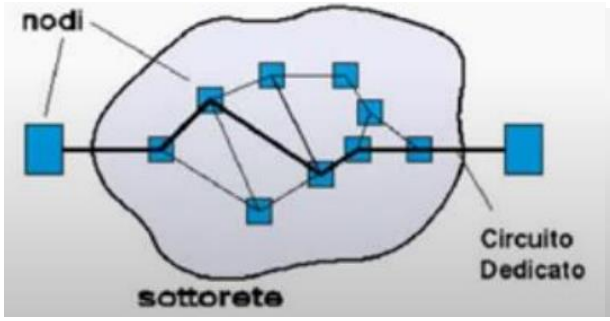
La commutazione di circuito è utilizzata nelle linee telefoniche analogiche e prevede una connessione tra due nodi tramite un percorso fisico scelto, nodo per nodo. I vantaggi di tale tecnologia sono:

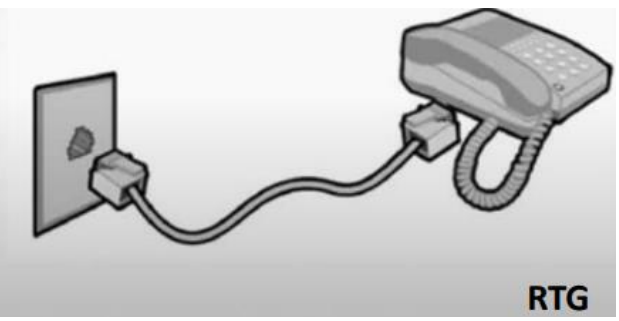
→ compattezza del messaggio che implica la riduzione degli errori;

→ circuito dedicato che garantisce affidabilità e sicurezza;

→ per tutta la trasmissione gode delle prestazioni fornite (come la banda).

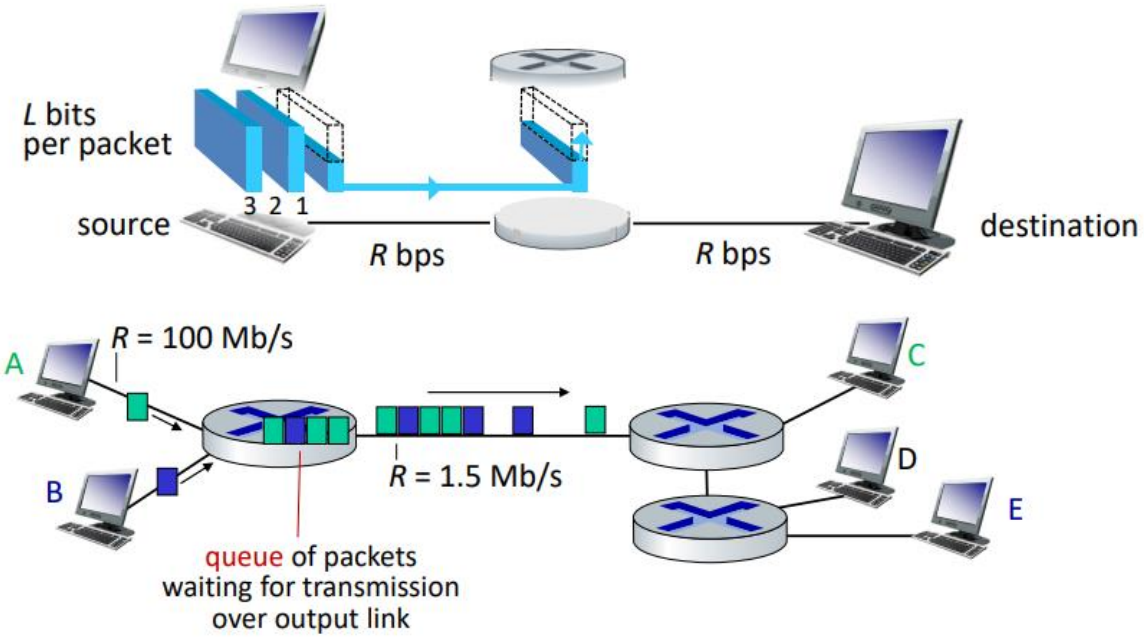
Lo svantaggio di tale tecnologia è che le parti di trasmissione non utilizzate sono perse.





11) Definire lo store and forward

Lo store and forward è una tecnica nella quale un pacchetto, nel suo percorso tra le singole stazioni della rete, deve essere totalmente ricevuto, prima di poter essere ritrasmesso nel collegamento in uscita.

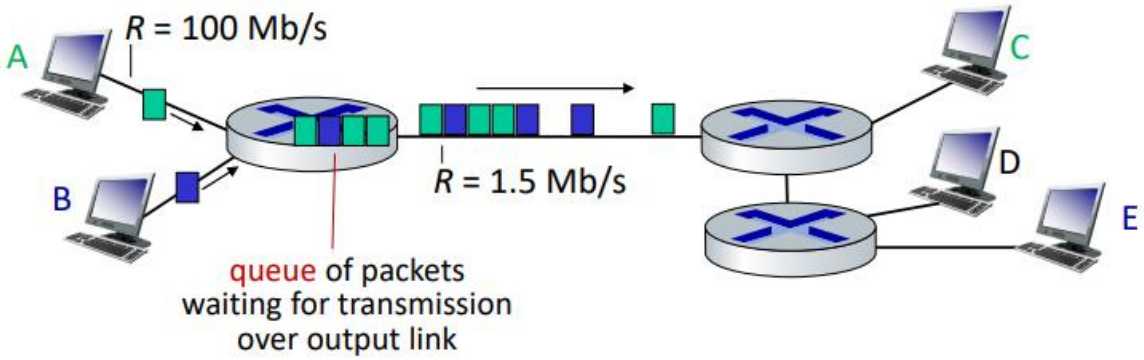


12) Descrivere il fenomeno di accodamento della commutazione di circuito

Se il tasso di arrivo (in bps) al collegamento supera la velocità di trasmissione (bps) del collegamento per un certo periodo di tempo:

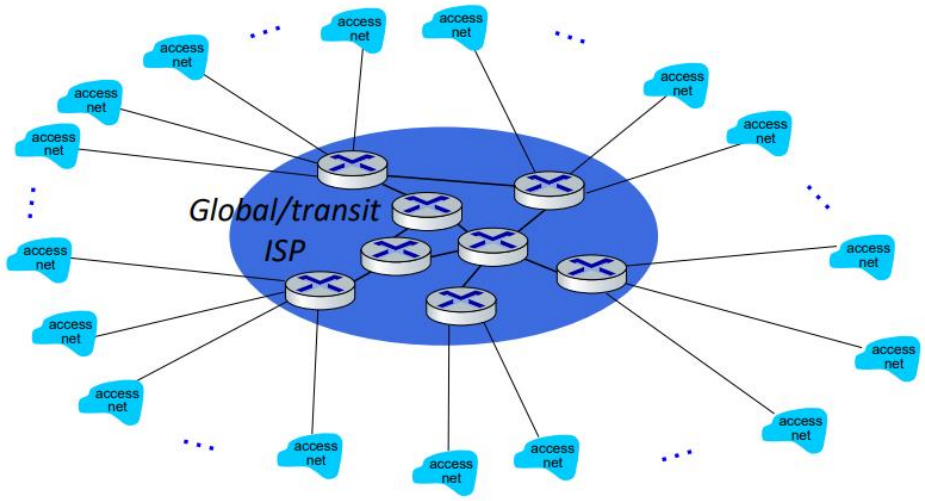
→ i pacchetti verranno messi in coda, in attesa di essere trasmessi sul collegamento di uscita;

→ i pacchetti possono essere eliminati (persi) se la memoria (buffer) nel router si riempie.



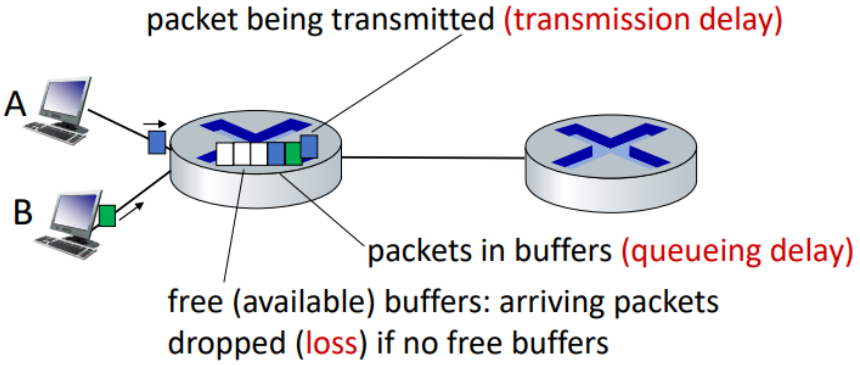
13) Che cosa si intende per ISP (Internet Service Provider)?

ISP (Internet Service Provider) è un'infrastruttura che offre agli utenti servizi inerenti ad Internet (principali World Wide Web, posta elettronica, ecc.).



14) Come si verificano il ritardo e la perdita dei pacchetti?

La perdita di pacchetti si verifica quando la memoria per contenere i pacchetti in coda si riempie, mentre la lunghezza della coda aumenta quando la velocità di arrivo al collegamento (temporaneamente) supera la capacità il collegamento di uscita.



15) Quali sono le quattro tipologie di ritardo dei pacchetti? Come viene calcolato l'end to end delay?

Le quattro tipologie di ritardo dei pacchetti sono:

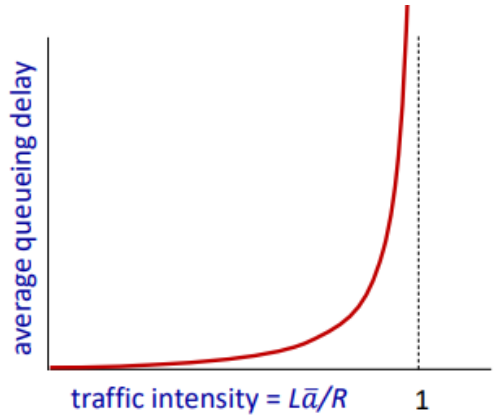
1 - elaborazione nodale (d_{proc}): in cui vengono verificati eventuali errori di codifica dei bit, determina il collegamento di uscita ed è tipicamente < microsecondi;

2 – ritardo di accodamento (d_{queue}): in cui il tempo di attesa al collegamento di uscita per trasmissione dipende dal livello di congestione del router ed è in ordine di millisecondi.

Siano a, la frequenza di arrivo dei pacchetti, L, la lunghezza dei pacchetti, e R, la larghezza di banda del collegamento.

L'intensità di traffico I viene calcolata mediante la seguente formula:

$I = (L * a) / R$

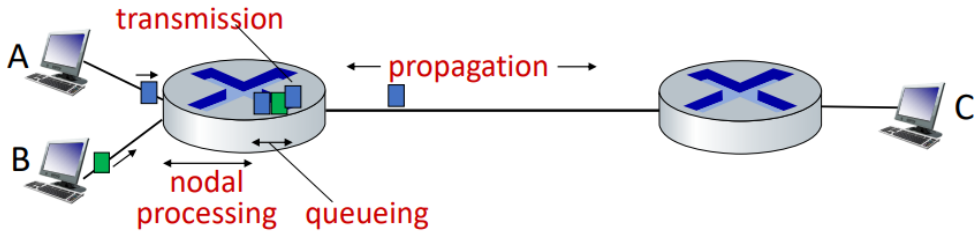


3 – ritardo di trasmissione (d_{trans}): in cui dati L, la lunghezza dei pacchetti e R, la frequenza di trasmissione (bps), il ritardo di trasmissione è il rapporto fra L ed R.

$d_{trans} = L/R$

4 – ritardo di propagazione (d_{prop}): in cui dati d, la lunghezza del collegamento fisico e s, la velocità di propagazione (sui $2 * 10^8$ m/sec), il ritardo di propagazione è il rapporto fra d ed s.

$d_{prop} = d/s$

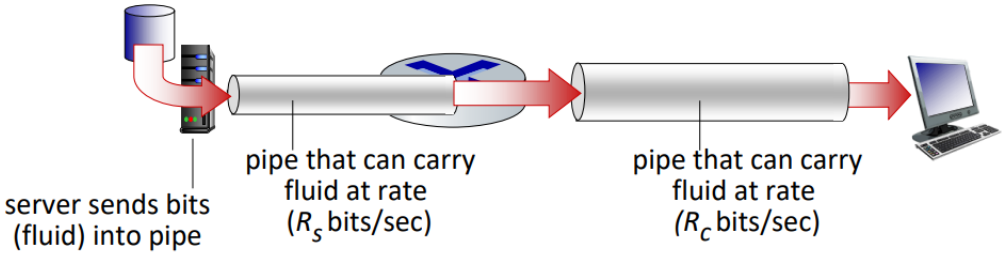


Il valore di end to end delay è la somma di tutti i ritardi

$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$

16) Cosa si intende per throughput?

Il throughput è la quantità effettiva di dati trasmessi in uno specifico periodo di tempo.

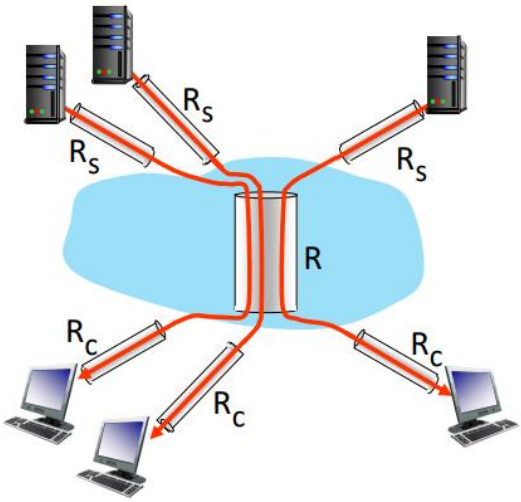


Rs < Rc → throughput medio: Rs

Rs > Rc → throughput medio: Rc

17) Cosa si intende per bottleneck link?

Il bottleneck link è il collegamento sul percorso end to end che limita il throughput end – end.



18) Cosa si intende per protocolli Internet?

I protocolli Internet sono insiemi di regole che controllano la comunicazione tra i computer di una rete. La condivisione di queste regole tra tutti gli host della rete garantisce il corretto funzionamento del sistema. All'inizio degli anni 80 l'ISO (International Standard Organization) iniziò un processo di standardizzazione proponendo un modello di riferimento OSI (Open System Interconnection) con l'obiettivo di definire regole comuni affinché sistemi diversi potessero comunicare tra loro.

19) Cosa si intende per modello ISO OSI?

Il modello ISO OSI è un'architettura a sette strati dove ogni livello può in generale comunicare solamente con il livello inferiore e fornisce servizi solo a quello superiore.

MODELLO ISO/OSI	LIVELLI	DESCRIZIONE
Applicazione	7	Responsabile dei servizi di rete per le applicazioni
Presentazione	6	Trasforma i formati dei dati per fornire un'interfaccia standard per il livello applicazione
Sessione	5	Stabilisce, gestisce e termina le connessioni tra l'applicazione locale e quella remota
Trasporto	4	Fornisce un controllo e un trasporto del flusso affidabili in una rete
Rete	3	Responsabile dell'indirizzamento logico e del dominio di instradamento
Collegamento dati	2	Si occupa di definire la struttura del messaggio dividendolo in frame individuando dove queste iniziano e dove finiscono
Fisico	1	Si occupa della gestione del mezzo trasmissivo (cavo coassiale, cavi STP o UTP, fibre ottiche) su cui avviene lo scambio di informazioni, della trasmissione dei singoli bit lungo la linea di trasmissione

20) Cosa si intende per modello TCP IP?

Il modello TCP/IP è un protocollo di collegamento dati utilizzato in Internet per consentire a computer e altri dispositivi di inviare e ricevere dati. TCP/IP sta per Transmission Control Protocol/Internet Protocol, cioè un sistema che consente ai dispositivi connessi a Internet di comunicare tra loro attraverso le reti. Il modello TCP/IP è l'unione di due protocolli:

→ TCP (Transmission Control Protocol): è responsabile della consegna affidabile di dati.

→ IP (Internet Protocol): è responsabile dell'aggiunta degli indirizzi sorgente e di destinazione ai dati.

MODELLO TCP/IP	LIVELLI	DESCRIZIONE
Applicazione	4	Dove operano i protocolli ad alto livello che permettono di risolvere i problemi relativi all'utilizzo della rete come SMTP e FTP
Trasporto	3	Specifica quale applicazione ha richiesto o riceve dati attraverso porte specifiche
Internet	2	Ha il compito principale di spedire i pacchetti di informazione verso ogni nodo di destinazione presente in rete
Accesso alla rete	1	Si occupa di recapitare i pacchetti prodotti dal livello superiore a questo, quindi al livello internet

Capitolo 2 – Livello Applicativo

21) Cosa si intende per DNS?

Il domain name system (DNS), serve per associare un host name ad un indirizzo IP, sfruttando gerarchie di nameserver, che sono suddivisi in:

→ root name server: lista di server contenenti correlazioni IP / root domain, sono 13 replicati nel mondo;

→ top level - domain TLD: responsabili dei top level (.com, .it, .net , .de, ecc.);

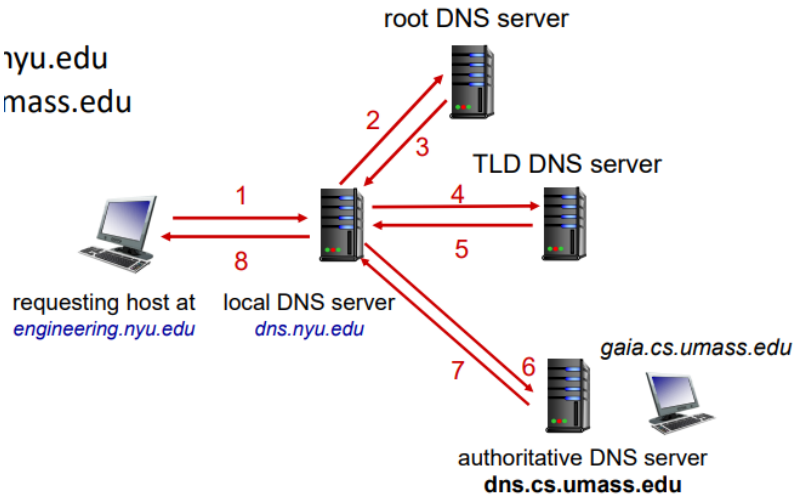
→ DNS di organizzazioni: come amazon, yahoo, unimib;

→ locali: cache di recenti collegamenti o name server locali.

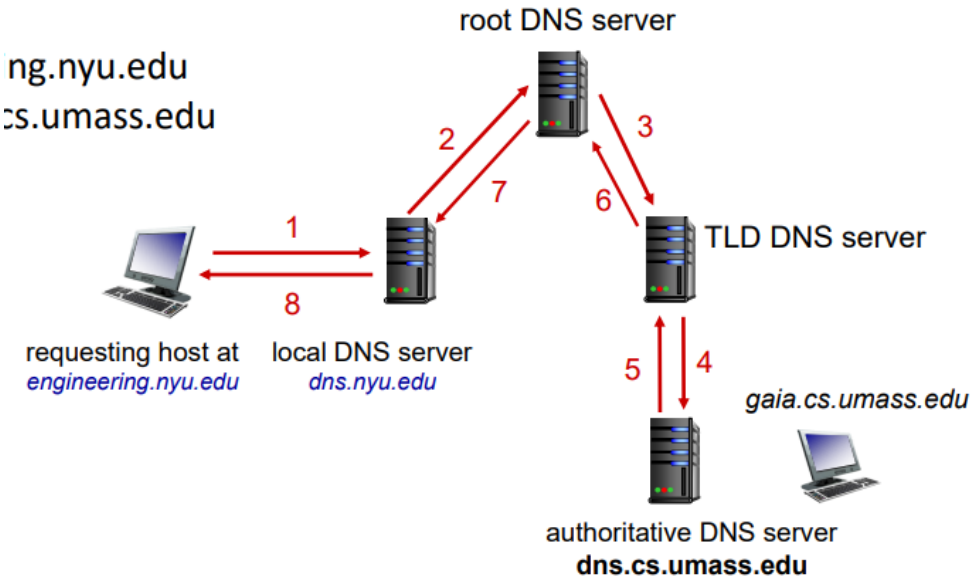
22) Quali sono le due tipologie di query DNS?

Esistono due tipologie di query:

→ query iterativa: la risposta proviene dal server contattato al server DNS locale con l'indirizzo IP del server a contatto;



→ query ricorsiva: pone l'onere del nome di risoluzione su nome contattato dal server (meno carico su server DNS locale) ma si ha carico pesante nella parte superiore dei livelli di gerarchia.



Capitolo 3 – Livello di Trasporto

23) Qual è il ruolo del livello di trasporto?

Il livello di trasporto fornisce una comunicazione logica tra applicativi, ovvero ci permette di far comunicare processi su macchine diverse come se fossero sulla stessa macchina.

Le azioni intraprese a questo livello sono:

→ sender: divide i messaggi in segmenti, passa al layer di rete (comunicazione logica tra host);

→ receiver: riassembla i segmenti, passa al layer applicazione.

24) Cosa si intende per socket?

Si dice socket, un'interfaccia che permette di far comunicare direttamente i processi che inviano e ricevono messaggi tramite il socket stesso.

Sender	Receiver
riceve un messaggio da applicazione, determina i valori dell'header, crea il segmento e lo passa ad IP.	riceve dal livello IP, controlla l' header, estrae il messaggio demultiplexa tramite il socket

25) Cosa si intende per multiplexing?

Il multiplexing è il meccanismo che permette di gestire dati da più socket, aggiungendo l'header di trasporto. Il mittente si occupa di ciò.

26) Cosa si intende per demultiplexing?

Il demultiplexing è il meccanismo che permette di utilizzare l'header per consegnare correttamente i socket. Il destinatario si occupa di ciò utilizzando IP e porte per indirizzare correttamente i segmenti ai socket.

27) Come può essere la connessione?

La connessione può essere:

→ connectionless: la creazione del socket avviene specificando (IP – porta di destinazione) e quando l'host riceve un segmento, lo reindirizza verso la porta specificata;

→ connection - oriented: i socket sono identificati da srcIP: srcPort e dstIP: dstPort, in questo modo il ricevente può supportare più socket contemporaneamente (ogni socket è connesso con un client);

28) UDP (User Datagram Protocol)

UDP (User Datagram Protocol) è un protocollo a livello di trasporto usato in applicazioni real-time non sensibili alla perdita di dati.

Esso ha le seguenti caratteristiche:

→ best - effort: non garantisce la consegna / consegna ordinata dei messaggi;

→ no congestion control: le congestioni fanno perdere pacchetti;

→ connectionless: non esiste handshake, garantendo setup più semplice e un header di minori dimensioni.

Non sono garantiti servizi su ritardi e latenza.

29) TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) è un protocollo a livello di trasporto usato in applicazioni dove il ritardo è irrilevante e la non perdita dei dati è importante.

Ha diverse caratteristiche:

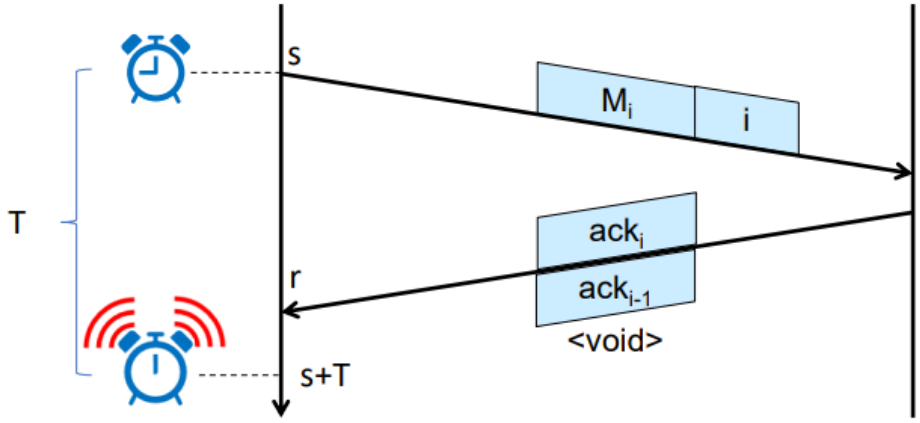
- point-to-point: un mittente e un destinatario;
- affidabile: consegna in - order;
- utilizza diversi meccanismi di controllo congestione e di flusso;
- necessita un handshake iniziale.

30) Principi di trasferimento affidabile

La complessità di un trasferimento dipende dalle caratteristiche del canale di comunicazione: mittente e destinatario devono comunicare per capire lo stato dell'uno e dell'altro.

Considerando che ack e nack sono soggetti ad errori, i protocolli di controllo dell'errore sono:

→ Stop and wait: tutti i segmenti sono numerati, aggiungendo un timer per gestire le perdite (capire quanto tempo farlo durare è difficile, inoltre potrebbe essere troppo lento);



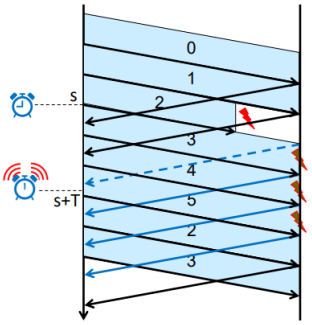
$$U = \frac{L/R}{RTT + L/R}$$

→ Sliding window: vengono inviati più pacchetti per volta e si aspettano ack in sequenza, condizione per una trasmissione continua è che la finestra non chiuda prima del primo ack.

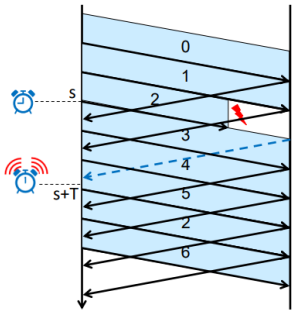
$$W \cdot L/R \geq RTT + L/R$$

$$W \geq \frac{RTT \cdot R}{L} + 1$$

Quando un segmento viene perso è possibile utilizzare i protocolli:
→ Go - Back - N: trasmette un pacchetto e passa a quello successivo dopo ogni ricevimento di ack, se a tempo S + T non arriva ack diamo pacchetto per perso, e il trasferimento ricomincia da dove il pacchetto è stato perso.



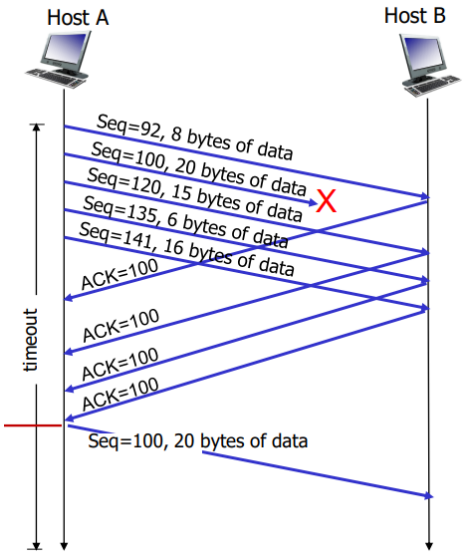
→ Protocollo Selective Repeat: uguale a quello sopra, ma viene rinviato solo il pacchetto perso in caso di errore.



→ Protocolli ibridi secondari.

31) Sequenza numerica TCP

Il controllo di sequenza avviene con due numeri:
• Sequence number: numero del primo byte nel segmento;
• Acknowledgements: numero del prossimo byte atteso dall' altro lato della comunicazione.



32) Cosa si intende per TCP Round Trip Time?

Il TCP Round Trip Time è l'unità di tempo che un pacchetto impiega per "viaggiare", utile per stabilire il valore di timeout che deve essere ponderato.
Per stimarlo si usano due parametri:

→ SampleRTT: tempo trascorso tra la trasmissione di un segmento e la ricezione dell'ACK;

→ EstimatedRTT: che si calcola mediante la seguente formula

$$\mathbf{EstimatedRTT = (1-\alpha)*EstimatedRTT + \alpha*SampleRTT}$$

→ TimeoutInterval: che si calcola mediante la seguente formula

$$\mathbf{TimeoutInterval = EstimatedRTT + 4*DevRTT}$$

→ DevRTT: che si calcola mediante la seguente formula

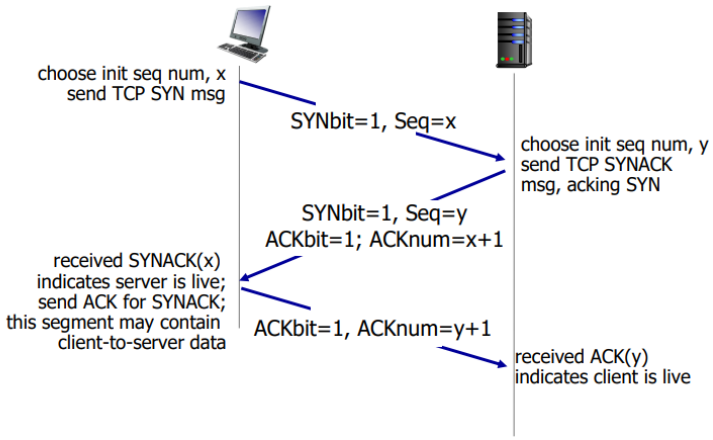
$$\mathbf{DevRTT = (1-\beta)*DevRTT + \beta*|SampleRTT-EstimatedRTT|}$$

33) Cosa si intende per TCP Fast Retransmit?

Proprietà di TCP in cui rinvia un pacchetto unack con il più piccolo sequence number se il mittente riceve 3 ack addizionali per lo stesso data.

34) Gestione della connessione: Handshake a tre vie

Prima di iniziare lo scambio di dati i due host effettuano un three -way handshake, nel quale concordano come stabilire la connessione e i parametri.



La chiusura di connessione tra client e server avviene impostando FINbit = 1 e rispondendo con un ACK.

35) Controllo di congestione

La congestione avviene quando più mittenti inviano dati che la rete non riesce a gestire. Più la rete si satura più si perdono pacchetti e aumenta il delay.
La congestione è gestita da:

→ end-to-end gestita dai due host (scelta del TCP);

→ network - assisted: gestita da dei feedback del router.

Una congestione viene gestita con:
→ AIMD additive increase moltiplicativa decrease: in caso di trasferimento di successo l'RTT viene incrementato. In caso di loss, la dimensione viene dimezzata.
→ Slow Start: all'inizio della connessione il cwnd = 1 MSS e aumenta esponenzialmente la quantità di dati trasmessa. Arrivato ad un valore prestabilito ssthresh viene impostato a $\frac{1}{2}$ del valore di cwnd. Implementato in TCP tramite TCP Reno: usa il Fast recovery dopo 3 acks duplicati: imposta cwnd a sstresh + 3*mss.

36) Controllo del flusso

Proprietà di TCP che controlla la velocità di trasmissione e la imposta di conseguenza, evitando di far andare in overflow il buffer del ricevente. Per permettere ciò il ricevente restituisce lo spazio libero nel buffer nel campo rwnd.
In particolare:
→ cwnd: gestisce la congestione;
→ rwnd: gestisce il flow.

37) Descrivere TCP Reno indicando i vantaggi e svantaggi

TCP Reno è una variante dell'algoritmo di controllo della congestione di TCP (Transmission Control Protocol), introdotta con lo scopo di migliorare la gestione della congestione nelle reti. Esso è stato sviluppato come miglioramento rispetto al TCP Tahoe, la prima implementazione del controllo della congestione in TCP e introduce meccanismi aggiuntivi per affrontare la congestione in modo più efficiente. Le caratteristiche principali di TCP Reno sono:
→ Slow Start (Inizio Lento): quando una connessione TCP viene avviata, Reno inizia con una finestra di congestione (cwnd) molto piccola e la finestra aumenta esponenzialmente con ogni ack ricevuto fino a raggiungere una soglia (ssthresh).
→ Congestion Avoidance (Evitamento della Congestione): dopo aver raggiunto la soglia ssthresh, la crescita della finestra di congestione diventa lineare anziché esponenziale, il che aiuta a prevenire il sovraccarico della rete.
→ Fast Retransmit (Ritrasmissione veloce): se il mittente riceve tre ack duplicati (segno che un pacchetto potrebbe essere stato perso), effettua una ritrasmissione del pacchetto mancante senza attendere il timeout del timer di ritrasmissione.

→ Fast Recovery (Recupero veloce): dopo un fast retransmit, invece di resettare la finestra di congestione come in TCP Tahoe, Reno riduce la finestra di congestione a metà del valore corrente (ssthresh) e poi entra direttamente in modalità congestion avoidance.
I vantaggi di TCP Reno sono:
→ maggiore efficienza: la combinazione di fast retransmit e fast recovery consente una gestione più rapida e meno distruttiva della perdita di pacchetti rispetto a TCP Tahoe;
→ riduzione del tempo di recupero: evitando il reset completo della finestra di congestione, TCP Reno riduce il tempo necessario per riprendere il trasferimento dati a piena capacità dopo una perdita di pacchetti.
Gli svantaggi di TCP Reno sono:
→ performance su reti con altra perdita di pacchetti: TCP Reno può non essere ottimale in reti con alta perdita di pacchetti o con ritardi significativi, poiché può ancora soffrire di riduzioni frequenti della finestra di congestione;
→ ignoranza della perdita non congestiva: TCP Reno presume che tutte le perdite di pacchetti siano dovute alla congestione, il che non è sempre vero.

38) Descrivere TCP Tahoe indicando i vantaggi e svantaggi
TCP Tahoe è un'implementazione iniziale del protocollo TCP (Transmission Control Protocol) con meccanismi di controllo della congestione introdotti per migliorare la gestione del traffico di rete e ridurre la probabilità di congestione. Le caratteristiche principali di TCP Tahoe sono:
→ Slow Start (Inizio Lento): quando una connessione TCP viene avviata, Tahoe inizia con una finestra di congestione (cwnd) molto piccola, generalmente impostata a un massimo di uno o due segmenti. La dimensione della finestra raddoppia ogni round trip time (RTT) fino a raggiungere una soglia predefinita (ssthresh).
→ Congestion Avoidance (Evitamento della Congestione): dopo aver raggiunto la soglia ssthresh, la crescita della finestra di congestione diventa lineare piuttosto che esponenziale. Questo approccio più graduale aiuta a prevenire la congestione della rete aumentando la finestra di un segmento per ogni RTT.
→ Fast Retransmit (Ritrasmissione Veloce): quando il mittente riceve tre ack duplicati per un particolare segmento, ritrasmette immediatamente il segmento mancante senza aspettare il timeout del timer di ritrasmissione. Questo riduce il tempo necessario per recuperare i pacchetti persi.
→ Timeout della Ritrasmissione: se un segmento non viene riconosciuto prima

che scada il timer di ritrasmissione, Tahoe riduce drasticamente la finestra di congestione (cwnd) a uno, e la soglia (ssthresh) è impostata a metà del valore di cwnd prima della perdita. Quindi, riavvia il processo di slow start.
I vantaggi di TCP Tahoe sono:
→ riduzione della congestione: l'introduzione di meccanismi di slow start e congestion avoidance contribuisce a ridurre la probabilità di congestione nella rete;
→ recupero più rapido dalla perdita di pacchetti: fast retransmit permette una ritrasmissione più rapida dei pacchetti persi, migliorando il tempo di recupero.
Gli svantaggi di TCP Tahoe sono:
→ efficienza subottimale: dopo una perdita di pacchetti e un timeout, TCP Tahoe riduce drasticamente la finestra di congestione a uno, il che può risultare in un periodo significativo di throughput ridotto mentre la finestra di congestione viene nuovamente aumentata;
→ reset completo della finestra di congestione: a differenza di TCP Reno, Tahoe non ha un meccanismo di fast recovery, quindi ogni perdita di pacchetti porta a un reset completo della finestra di congestione, riducendo l'efficienza del throughput.