RETI DEGLI ELABORATORI

CAPITOLO 1

1. Si discutano le differenze tra rete a circuito e a pacchetto

I commutazione di pacchetto non ha risorse riservate, la velocità dipende dalla qualità del collegamento e la trasmissione è del tipo store and forword. Mentre il commutazione di circuito richiede l'utilizzo di una linea dedicata dove alloca risorse sulla rete e rimane attivo per tutto il tempo.

2. Discutere l'impatto che la lunghezza di un pacchetto ha sulle prestazione del sistema discutendo l'effetto pipeline, il caso di un canale rumoroso ecc..funzionamento, le problematiche legate al formato dei messaggi, gli elementi di rete coinvolti

La lunghezza del pacchetto influisce sulle prestazioni, prendendo in esempio il commutatore di pacchetto abbiamo una trasmissione S-F quindi si deve memorizzare nel buffer tutto il pacchetto influenzando cosi anche i ritardi di accodamento. Prendendo in esempio il protocollo TCP avremo che può spedire allo stesso client più pagine web. Queste richieste di oggetti possono essere effettuate una di seguito all' altra senza aspettare eventuali risposte. In alcuni casi il mittente può essere obbligato a inviare soltanto determinati pacchetti (in quanto numerati) come avviene nella Ripetizione Selettiva

3. Quali livelli nella pila dei protocolli di internet vengono elaborati da un router? Quali da un commutatore a livello di collegamento? Quali da un host?

I router elaborano i livelli da 1 a 3. Gli interruttori di livello di collegamento elaborano i livelli da 1 a 2. Gli host elaborano tutti e cinque i livelli.

4. Quali sono i vantaggi di avere uno Stack protocollare basato sulla stratificazione? (Architettura a livello)

La stratificazione dei protocolli presenta vantaggi concettuali e strutturali. La modularità rende più facile aggiornare la componentistica. Un eventuale svantaggio legato alla stratificazione è la possibilità che un livello duplichi le funzionalità di quello inferiore. Un secondo potenziale svantaggio è che la funzionalità a un livello possa richiedere informazioni presenti solo in un altro livello.

5. Calcola: Ritardo di propagazione, ritardo di trasmissione etc..

RP: L/R

RT: d/v

Rete: d = N(d.ela + d.trasmi + d.prop)

6. Si descriva il funzionamento dell'applicazione Web (in quale livello e per cosa è usata? Descrizione del protocollo usato per scambiare i messaggi. Si spieghi cosa sono i cookies. Discutete anche come si possono migliorare le prestazione dell'applicazione web.

Un’applicazione Web si basa sul livello di applicazione un protocollo usato per scambiare i messaggi e include diversi protocolli come HTTP (che consente la richiesta e il trasferimento dei documenti web), SMTP (che consente il trasferimento dei messaggi di posta elettronica) e FTP (che consente il trasferimento di file tra due sistemi remoti).

CAPITOLO 2

1. **Si discuta il funzionamento di http, illustrando i vari passi necessari a scaricare una pagina web, e dettagliando l’impatto che può avere l’uso di un proxy.**
   HTTP è un protocollo a livello di rete e ha il ruolo di definire la struttura dei messaggi e la modalità di comunicazione tra il client e il server. HTTP non tiene memoria di stato e non si occupa di errori o eventuali dati smarriti . L’HTTP usa connessioni persistenti e non persistenti ovvero nel primo caso la connessione TCP rimane attiva e C-S usano la stessa connessione mentre nel secondo caso avremo una chiusura del TCP ad ogni invio dell’oggetto. Al fine di scaricare una pagina web il Client deve inizializzare una connessione TCP con il server tramite una socket, invierà cosi il segnale al server, a questo punto il server recupera l’oggetto, dopo aver inviato l’oggetto il server chiuse la sessione e infine il client estrae il file. L’RTT è il tempo necessario per trasferire un piccolo messaggio e viene anche chiamato handshack a tre vie. L’uso di un Proxy sono dei server in rete che permettono una maggiore velocità del trasferimento dati C-S perché agiscono come vere e proprie memorie cache.

2. **Cosa è una socket**

Una socket è un’interfaccia software che permette ad un processo di inviare e ricevere messaggi nella rete. Nello specifico una socket è l’interfaccia tra un processo applicativo e il protocollo a livello di trasporto

MAIL:

1. **Si descrivano tutti i meccanismi per la composizione, invio e corretta ricezione di un messaggio di posta elettronica tra due utenti. Si discutano i protocolli utilizzati per l’invio della posta elettronica e per scaricare messaggi di posta.**
   Quando X ha finito di comporre il messaggio, il suo user agent lo invia al server di posta, dove viene posto nella coda di messaggi in uscita. Quando Y vuole leggere il messaggio, il suo user agent lo recupera dalla casella di posta nel suo mail server. Esistono diversi protocolli che permettono il corretto utilizzo della posta elettronica come l’SMTP, un protocollo di posta elettronica asincrono che usa la codifica ASCII a 7 bit, è affidabile e persistente. Esistono anche altri diversi protocolli tra cui POP3 un protocollo di accesso semplice e di facile lettura e per questo motivo non viene usato particolarmente. Usa uno user agent, si affida al protocollo TCP e ciò che lo rende particolarmente usato è la sua modalità Scarica e cancella oppure Scarica e mantiene.

2. **Quale protocollo è utilizzato per la comunicazione tra mail server?**
   SMTP

DNS:
1. Si descriva il funzionamento del protocollo DNS:

Per DNS si intende il Domain Name System e ha il compito di risolvere i nomi degli host che sono identificati tramite degli indirizzi IP, ma per migliorare l'efficienza di identificazione vengono aggiunti degli Host Aliasing. Il DNS denota un protocollo, un programma oppure un server stesso. Lo si può vedere come un database distribuito con una forma gerarchica (esistono diversi modelli). Il caching dei nomi permette di migliorare le prestazione e il ritardo e viene usata una memoria cache con un TTL (time to live) importabile

1. **In quale strato della rete opera?**
   A livello applicativo

2. **Qual'è il suo compito e da quali protocolli è usato**
   Protocollo UDP

3. **Quali sono gli elementi di rete coinvolti nello scambio di messaggi e quale è il loro ruolo?**

4. **Come funziona in dettagli il protocollo**

La macchina dell'utente esegue il lato client dell'applicazione DNS
Il browser estrae il nome dell'host dall'URL e lo passa al lato client dell'applicazione DNS
Il client DNS invia una quei contenente l'hostname a un DNS server
Una volta ricevuto l'IP dal DNS, il browser può dare inizio a una connessione TCP verso il processo server HTTP

5. **Qual'è il formato dei messaggi scambiati**

Il formato dei messaggi di un DNS comprende un campo per l'identificazione composta da 16 bit per le query e le risposte alle query, un campo flag con una sezione delle domande consentente informazioni. Sulle richieste che stanno per essere effettuate, una sezione autoritaria contenete informazioni sui server autoritativi e una sezione aggiunta che racchiude un insieme di record utili.

6. **Quali ottimizzazioni sono possibili per migliorare l'efficienza del protocollo**

   Per migliorare un DNS è una sua implementazione distribuita e scalabile. Questo permette di non scaricare il singolo Point ma di gestire il carico in maniera più uniforme. Anche gli aggiornamenti e la manutenzione sono fattori determinanti per un DNS efficiente

2. Memorizzazione delle informazioni in DNS e i loro tipi (NS, A, etc...) 3. Quale livello di trasporto utilizza DNS e perché

Esistono diverse implementazioni del DNS:
Centralizzato: costituito da una facile implementazione ma che presenta problemi legati al single Point failure, volume di traffico incentrato in unico punto e il database centralizzato
DNS Gerarchico: composto da diversi server organizzati in modo gerarchico ed esistono 3 classi di DNS server: il root server, domini di primo livello è domini dei vari paesi, e DNS server autoritativi che associano host a indirizzi IP.
DNS locali: sviluppati nelle varie enti locali come uffici e università e possono essere configurabili in base alle necessità in modo manuale o automatico. Operano con un proxy che agisce come server intermedio

CAPITOLO 3

TCP:

1. **Discutere i meccanismi adottati da TCP per il controllo di congestione, le diverse soluzioni usate e le motivazioni che hanno portato ad introdurre soluzioni diverse**
   Il controllo di congestione attuato dal TCP si basa sulla comunicazione di ACK (o eventualmente NAK/ ACK duplicati) tra le due entità. In assenza di perdite di pacchetti, il tempo che intercorre tra l'invio di un segmento (dall'host A all'host B) e la ricezione del relativo riscontro (inviato dall'host B all'host A) definisce il cosiddetto Round Trip Time(o RTT). I meccanismi adottati per il controllo della congestione è EndToEnd, un approccio che viene controllato dai end system che forniscono informazioni riguardo eventuali perdite di pacchetti e ritardi. Mentre il controllo della congestione gestita dalla rete forniscono un feedback esplicito al mittente sullo stato della congestione

2. **Si discutano i concetti di protocollo di comunicazione, architettura di protocollo di**
   comunicazione, il principio di stratificazione, facendo un esempio di come tale principio trovi applicazione nell'architettura TCP/IP (ovvero si richiede di motivare la suddivisione in livelli delle funzionalità nella pila TCP/IP)
   L'architettura TCP-IP è stata pensata semplicemente come un'architettura gerarchica, in cui ogni livello intermedio può utilizzare il servizio offerto da uno dei livelli sottostanti per fornire a sua volta un servizio a un livello superiore. Il problema maggiore nasce con i protocolli della famiglia TCP-IP che risultano incapsulati in protocolli di pari livello gerarchico dove ogni livello è responsabile delle proprie funzioni

3. **Si discutano i protocolli per l'apertura e la chiusura di una connessione TCP, mettendo in risalto come e perché permettano un corretto svolgimento dello scambio dati - ad esempio successivo alla fase di apertura della connessione . Ed eventuali problematiche ad essi associate**
   Un handshake a tre vie (Three-way handshake) è un metodo utilizzato in una rete TCP/IP per creare una connessione tra un host/client locale e un server. Si tratta di un metodo in tre fasi che richiede sia al client che al server di scambiare i pacchetti SYN e ACK (riconoscimento-acknowledgment) prima dell'inizio della comunicazione dei dati. La chiusura della connessione quando riceve la conferma quella direzione della connessione viene chiusa. Il problema che può sorgere è dato dall'esempio dei due eserciti. Si entra in loop perché non si conosce lo stato del messaggio con l'orario di attacco.

4. **Si descriva nel dettaglio il meccanismo di trasmissione affidabile in TCP:**

   1. **Come sono calcolati i sequence number dei segmenti**
      I sequence number sono usati per numerare sequenzialmente i pacchetti di dati che fluiscono tra mittente e destinatario. Le discontinuità nei numeri di sequenza di pacchetti ricevuti consentono al destinatario di rilevare i pacchetti persi. I pacchetti con numero di sequenza ripetuto consentono al destinatario di rilevare pacchetti duplicati.
      Nel GBN (ricordiamo che il TCP ha un campo a 32 bit per i numeri di sequenza), i numeri di sequenza TCP contano i byte nel flusso dei dati anziché i pacchetti.

Detto k il numero di bit di tale campo, l'intervallo di possibili numeri di sequenza è [0 - 2^k-1]

Nel SR i pacchetti del sequence number saranno nell'intervallo
[rcv_base , rcv_base+N-1]

2. **Si dettagli i protocolli di ritrasmissione automatica dell'informazione**

GBN e SR

3. **Si chiarisca come è calcolato il ritrasmissione time-out**
TimeoutIntervall = EstimateRTT + 4 * DevRTT

   i. EstimateRTT = è una media ponderata dei valori di SampleRTT (intervallo di tempo che intercorre tra invio e ricezione del messaggio)

   ii. DevRTT =DevRTT è la deviazione standard del timeout di TCP

5. **Si descrivano i meccanismi per la trasmissione affidabile di PDU, spiegando il funzionamento di Stop&Wait, Go-Back-N, Selettive Repeat, e della soluzione adottata per la ritrasmissione affidabile in TCP.**
Il Stop&Wait è il più semplice dei protocolli in quanto il mittente invierà un frame alla volta al destinatario. Il mittente dovrà aspettare la conferma del destinatario. Questo intervallo di tempo che renderà a tutti gli effetti inattivo il mittente. Il riconoscimento verrà chiamato ACK.
GBN: il mittente può trasmettere più pacchetti senza dover attendere alcun acknowledgement, ma non può avere più di un dato numero massimo consentito N di pacchetti. Viene considerato un protocollo a finestra scorrevole e ritrasmette tutti i frame dopo il frame perso. Se un ACK viene perso allora si attende l'esaurimento del tempo (timeout).

   SR: evitano le ritrasmissioni non necessarie facendo ritrasmettere al mittente solo quei pacchetti su cui esistono sospetti di errore costringe il destinatario a mandare acknowledgement specifici per i pacchetti ricevuti in modo corretto. Tutti i pacchetti verranno inseriti in un buffer e non avranno un ordine di sequenza bensì verranno ordinati in un secondo momento.

6. **Come si identifica univocamente una socket TCP? E una UDP?**

   La socket UDP ha un numero di porta compresa tra 1024 e 65535, attua il sistema "Best Effort" ovvero non assicura la consegna dei segmenti ne l'ordine originario e non garantisce neppure l'integrità dei dati all'interno dei segmenti. Il segmento sarà composto dai dati, dalla sorgente e dalla destinazione. La socket TCP sarà composta da parametri tra cui la porta di inizio e di fine e da indirizzo di inizio e di fine. Anche se hanno indirizzi IP o porta diverse potranno avere la stessa destinazione

7. **Cosa si intende per slow start in TCP?**
Nel Slow Start avremo un cwnd (finestra di congestione) pari a 1 e il MSS che viene incrementato ogni volta di 1 ad ogni ACK ricevuto, raddoppiando la velocità trasmissiva. La velocità parte lentamente ma cresce in modo esponenziale. Se c'è

una perdita lo Slow Start ricomincia. SlowStart termina quando c'è una perdita. Oppure il ssthresh = cwnd oppure ci sono tre ACK duplicati ed entra in fast recovery

8. **TCP e gli ACK/NAK**
   Un ACK è utilizzato dal destinatario per comunicare al mittente che un pacchetto o un insieme di pacchetti sono stati ricevuti correttamente. Gli acknowledgement trasporteranno generalmente i numeri di sequenza del pacchetto o dei pacchetti da confermare. A seconda del protocollo, i riscontri possono essere individuali o cumulativi.

   Un NAK stato ricevuto correttamente. Gli acknowledgement negativi trasporteranno generalmente il numero di sequenza del pacchetto che non è stato ricevuto correttamente.

9. **La trasmissione affidabile dell'informazione in TCP avviene secondo un protocollo di AutomaticRepeatRequest ibrido. Il protocollo è un mix di quali protocolli?**
   (Quali caratteristiche ha di uno e dell'altro)
   Il TCP è un protocollo composto in parte da caratteristiche riprese da GBN e da una parte della Selective Repete. Nel primo caso memorizza il numero di sequenza più basso mentre nel secondo caso riprende la capacità di utilizzare pacchetti non in ordine

10. Cosa si intende per controllo di flusso?

Il controllo di flusso è un servizio di confronto sulla velocità, dato che paragona la frequenza di invio del mittente con quella di lettura dell'applicazione ricevente. Come notato in precedenza, i mittenti TCP possono anche essere rallentati dalla congestione nella rete IP

CAPITOLO 4

1. **Quali sono le due funzioni più importanti a livello di rete in una rete datagram? E le tre più importanti in una a commutazione di circuito?**

Le due funzioni più importanti sono il Forwording e il Routine. Il primo si occupa dell'assodamento dei pacchetti in entrata e in uscita, e si affida ad un Forwording Table usato come indice. Mentre il routine determina i percorsi dei pacchetti dalla sorgente alla destinazione

2. **Qual è la differenza tra instradamento e inoltro?**

L'inoltro consiste nello spostare un pacchetto dal collegamento di input di un router al collegamento di output appropriato. L'instradamento riguarda la determinazione dell'end-to-route tra sorgenti e destinazioni.

3. **I router nelle reti datagram e a circuito virtuale utilizzano tabelle di inoltro? Descrivete le tabelle di inoltro per entrambe le classi di reti.**

I router per inoltrare pacchetti si affidano all'indice del campo intestazione delle tabelle di inoltro. Il risultato indica a quale interfaccia di collegamento il pacchetto debba essere diretto. A seconda del protocollo, il valore nell'intestazione del pacchetto può rappresentare l'indirizzo di destinazione o la connessione cui appartiene.

4. Da quali parti interagenti è composto il livello di rete?

Il livello di rete è composto dal piano dei dati e il piano di controllo.
Il piano dei dati determina il modo di entrata e di uscita di un datagramma da un router e viene implementato a livello hardware.
Mentre il piano di controllo ha una logica globale sull'instradamento dei dataframmi su un percorso end-to-end tra sorgente e destinazione, in questo caso il piano di controllo viene implementato a livello software

5. Descrivi il servizio Datagram e Circuito Virtuale offerto dal livello di rete

Il servizio di Datagram è il percorso che viene modificato in base a determinati fattori e tutti possono arrivare a destinazione con un ordine non definito. Ogni pacchetto viene identificato con gli indirizzi IP.
Il servizio di Circuito Virtuale invece gli algoritmi creano un canale virtuale dove viaggiano i pacchetti. Si creano i circuiti virtuali e vengono identificati tramite un Id.

6. Cosa sono e quali sono i componenti dei router?

I router sono dispositivi a livello di rete e si occupano della commutazione di livello 3 nello Stack OSI. Sono comporti da porte di ingresso sa una struttura di commutazione, da porte di uscita e da un processore di instradamento.
Le porte di ingresso hanno un sterminatore elettrico ed elabora a livello di collegamento, determina la porta di uscita a cui dirigere il pacchetto e infine la tabella di inoltro è elaborata e aggiornata dal processore.
La struttura di commutazione connette le porte di ingresso e le porte di uscita tramite i bus o strutture di interconnessione.
Le porte di uscita invece hanno il computo di memorizzare i pacchetti e li trasmette in uscita.
Infine il processore di instradamento esegue i protocolli di instradamento e ha anche il compito di gestire ed elaborare le tabelle di inoltro.

7. Cosa sono e come sono ottenute le strutture di commutazione del livello di rete?

Le strutture di commutazione per definizione sono le modalità con le quali si commutano i pacchetti. Esistono diversi modelli tra cui commutazione in memoria, commutazione tramite bus e commutazione tramite rete di interconnessione.
La commutazione in memoria si basava sui router controllati direttamente dalla CPU, le porte agivano come normali dispositivi I/O e l'arrivo del pacchetto segnalava un interrupt per poi copiarlo in memoria. Anche in questo caso si preferì usare le tabelle di inoltre.
La commutazione tramite bus usava il bus stesso per il trasferimento senza l'utilizzo del processore. Si usava un'intestazione che indicava la porta locale. La larghezza di banda era limitata dal bus in quanto 1 bus = 1 pacchetto.
La commutazione attraverso una rete di interconnessione è realizzata come una vera e propria matrice con 2n bus con n porte di ingresso e n porte di uscita. Gli "incroci" che si vengono a creare vengono chiusi o aperti da un controller. Finalmente si è riusciti a inoltrare più pacchetti in parallelo. Al fine di gestire più pacchetti in uscita dalla stessa porta venne creata una coda di input. Le reti di interconnessione moderne più sofisticate usano tecniche per l'attraversamento simultaneo.

8. Come sono gestiti gli accodamenti e le perdite dei pacchetti tramite lo schedulatore?

Lo schedulatore di pacchetti stabilisce l'ordine di trasmissione dei pacchetti e offre cosi garanzie di qualità del servizio. In un primo momento era implementato con la tecnica FCFS ovvero il primo arrivato, il primo servito ma adesso esistono tecniche più sofisticate come WFQ che stabilisce un accodamento equo ponderato. Se ha poca memoria lo schedulatore stabilirà se scartarlo oppure rimuoverne uno. In alcuni casi può decidere se eliminarne uno prima che il buffer si riempia.

9. Descrivi l'IP Internet Protocol

E' un protocollo di interconnessione che attua il "Best Effort" non garantisce così il controllo sugli errori, sulla congestione e sull'affidabilità. Presenta due versioni IPv4 e IPv6.

10. Descrivi IPv4, la frammentazione, l'indirizzamento e infine la composizione dell'intestazione

L'IPv4 invia datagrammi composti da un header e una parte dati. I campi contengono la versione del protocollo, la lunghezza dell'header, il TTL, il protocollo usato se TCP o UDP, il campo chucksum, l'indirizzo di destinazione, un campo opzioni e un campo dati. La frammentazione dei datagrammi IPv4 si affidano al MTU ovvero il maximum trasmissione unit ma ogni protocollo avrà un valore del MTU diverso. I datagrammi verranno divisi in frammenti e riassemblati prima del livello di trasporto alla destinazione. L'ordine dei frammenti verrà determinato dai flag, dall'offset e dai campi di identificazione. L'indirizzamento IPv4 usa un'interfaccia che rappresenta il confine tra host e collegamento. L'host ha due interfacce e svolte il compito di inviare e ricevere datagrammmi. L'indirizzo IPv4 = 32 bit composto da due parti l'identificatore di rete e identificatore di host.

11. Cos'è il NAT? Come funziona e dove è stato implementato

Il NAT è il network Address translation, viene implementato nei ruoter tra le reti private e internet. Permette ad una zona locale di avere degli IP privati nascosti dall'esterno mascherati da un unico indirizzo IP. Dovrà cosi avere una tabella di routine per gestire le connessioni tra host. Esistono di due tipi: Statico che associa un ip pubblico ad uno privato ma non risolve la scarsità. E infine esiste anche il NAT dinamico con i terminali che hanno virtualmente lo stesso IP visti dall'esterno. Si convoglia cosi tutti gli IP tramite il meccanismo di traslazione della porta e ogni porta sorgente sarà diversa ad ogni richiesta.

12. Cos'è il protocollo DHCP?

Il protocollo DHCP per definizione è il protocollo di rete di livello applicativo e permette agli host di ricevere una configurazione IP necessaria per stabilire una connessione. Il protocollo Client-Server prevede un lato client e un lato server DHCP e un agente di relay DHCP per inoltrare le richieste server. Una sessione DHCP tipica prevede l'individuazione del server DHCP, offerta del server DHCP, richiesta DHCP e la conferma DHCP. Lato sicurezza il client si identifica tramite un campo ID (campo MAC) e per evitare usi malevoli si è introdotto il DHCP snooping in grado di fermare i pacchetti non originati da server autorizzati.

13. Il protocollo ICMP?

Il protocollo ICMP viene usato per scambiare informazioni su errori, malfunzionamenti o info di controllo. Viene usato dentro l'IP e si basa sul protocollo "Best Effort".

14. Descrivi IPv6, la frammentazione, l'indirizzamento e infine la composizione dell'intestazione

IPv6 cerca di risolvere problemi quali lo spazio di indirizzamento, il routing, la sicurezza, permettere configurazione automatica e di facilitare i servizi in real-time. La lunghezza è di 268 bit, è formato da un insieme di interfacce dette "anycast". Ha un header semplificato formato dal header principale con una propria estensione. Sarà proprio questa estensione a permettere la gestione del routing, la frammentazione, l'autenticazione e la sicurezza. La frammentazione è in modalità ent-to-end con un header non frammentabile. I frammenti contengono una parte del payload relativo all'IP originale. Il fragment header permette di identificare tutti i frammenti appartenenti allo stesso pacchetto

15. Quali sono le differenze tra IPv4 e IPv6?

Non esiste il chucksum, alcuni campi sono stati eliminati o resi opzionali.

16. Com'è avvenuta la transizione IPv4 a IPv6?

Ci sono stati errori di compatibilità ma sono state create delle soluzioni tra cui il dual stack e la tecnica del tunneling.
La prima non risolve il problema dell'indirizzamento e prevede un utilizzo del doppio stack aumentando cosi la complessità-
Mentre la tecnica del tunneling offre un collgamento Point to Point e i pacchetti IPv6 sono incapsulati in pacchetti IPv4 nei host. Infine si avrà un decapsulamento