Domande e risposte 2° parziale

Reti di Telecomunicazione

Differenza tra controllo di flusso e controllo della congestione.
Il controllo di congestione è legato alla capacità della rete di portare il traffico immesso ed è un problema globale che coinvolge gli host ed i router.
Il controllo del flusso è legato al traffico punto a punto tra un mittente ed un destinatario, deve fare in modo che un mittente veloce non trasmetta dati più velocemente di quanto il ricevente li possa gestire.

Subnetting di rete CIDR.
CIDR = ClassLess InterDomain Routing
E' una soluzione alla scarsità di indirizzi IP. Permette di dare a internet un po' di respiro per quanto riguarda la carenza di indirizzi allocando indirizzi senza badare alle classi. Questo richiede un forwarding più complicato.
C'è una routing-table unica che consiste in un array di indirizzi IP, subnet mask e linee d'uscita. Quando il pacchetto arriva si cerca con il suo indirizzo IP nella tabella alla ricerca di un riscontro, se se ne trovano diversi si prende la subnet più lunga. Con il vecchio sistema a classi quando un pacchetto arrivava si leggeva la classe e veniva indirizzato da un if a 16 uscite.

A cosa serve il protocollo ARP e come funziona.
ARP = Address Resolution Protocol
E' un protocollo importante che usa il broadcast, infatti ogni pacchetto ARP è mandato ovunque sulla sua rete. Se molte macchine sono attaccate su reti Ethernet che mandano e ricevono pacchetti con indirizzi Ethernet a 48 bit non sanno nulla degli indirizzi IP a 32 bit. Per mappare gli indirizzi IP su quelli MAC potrei tenere una tabella sempre aggiornata ma non è la soluzione giusta. Con ARP ogni macchina impara la configurazione della rete mandando una richiesta sulla rete di chi possiede un certo indirizzo IP, allora quando giungerà la risposta saprà sempre che si deve riferire a quella data macchina.

A cosa serve il NAT e come funziona.
NAT = Network Address Translation
È una soluzione molto poco elegante alla scarsità di indirizzi IP. Ad un ente od un privato viene assegnato un unico indirizzo IP oppure un range molto piccolo di numeri per il traffico internet. All'interno dell'ente ogni computer riceve un indirizzo IP univoco necessario per il routing interno. Quando un pacchetto deve uscire dalla subnet il suo indirizzo viene tradotto da privato (entro l'ente d'appartenenza) a pubblico (nella Internet).
NAT ha un problema, ovvero quando il pacchetto torna indietro non si sa a che macchina recapitarlo. Posso usare TCP o UDP, oppure delle porte numerate.
È abominevole perchè viola il principio dei layer per cui il layer k+1 deve essere ignoto al layer k; gli indirizzi IP dovrebbero essere univoci e se NAT cessa di funzionare si troncano tutte le connessioni che gestisce.

A cosa serve il campo TTL nell'header IP.
TTL = Time To Live.
È un contatore che limita la durata di vita di un pacchetto, dovrebbe contare in secondi con un massimo di 225 secondi ma richiede sincronia dei clock dei router. Invece viene decrementato ad ogni hop di una unità e decrementato più volte quando un pacchetto è accodato ad un router (in pratica conta gli hops). Il conto incomincia da 64 a dipende dal sistema operativo dell'host mittente.

Algoritmi dinamici di routing.
Gli algoritmi di routing servono per decidere quale strada far compiere ad un pacchetto nella rete, che si tratti di un protocollo connection oriented (con virtual circuit) o di uno connectionless (con datagram).
Sono detti algoritmi adattivi (o dimanici) gli algoritmi di routing che basano le proprie decisioni di azione su aggiornamenti continui delle proprie informazioni sullo stato della rete. I principali algoritmi dinamici sono il Distance Vector Routing ed il Link State Routing.

FARINELLI Agnese ~ http://thalionwen.altervista.org

Distance Vector Routing e Link State Routing.
Distance Vector Routing = è un algoritmo di tipo dinamico. Ogni router mantene una tabella con le migliori distanze note per ogni destinazione e quale linea usare. La tabella viene aggiornata scambiando informazioni con i vicini. Questo algoritmo è soggetto a conteggio all'infinito (se un router si spegne non lo si viene mai a sapere e le statistiche sulle distanze aumentano virtualmente fino all'infinito) e ci metteva troppo tempo a convergere.
Link State Routing = algoritmo dinamico che ha sostituito il precedente poiché non soffre di conteggio all'infinito e non ci mette troppo a convergere. L'algoritmo manda un pacchetto a tutti i suoi vicini per imparare il loro indirizzo IP e per misurare la loro distanza. Con i dati raccolti poi costruisce un nuovo pacchetto per raccontare cosa ha imparato a tutti gli altri router.

Descrivere il funzionamento dei comandi Ping e Traceroute e dire su quali protocolli si basano.
PING = è un programma diagnostico che è presente su ogni architettura. Serve a monitorare se esistono congestioni sulla rete a seconda di quanti pacchetti sono stati mandati e di quanti si sono ricevuti. Si basa sul protocollo ICMP. Il comando PING viene normalmente usato per testare la connettività e le funzionalità basiche della rete; in particolare per esempio può verificare l'esistenza di un indirizzo IP sulla rete.
TRACEROUTE = è un programma basato sul protocollo ICMP che manda pacchetti ICMP con TTL molto bassi bloccandosi al primo router che incontra. Programma che permette di verificare i punti da cui il pc deve passare prima di connettersi all'indirizzo desiderato dando come informazioni aggiuntive la nazione, il nome del provider, indirizzi IP, ecc.

Leaky Bucket e Token Bucket.
Leaky Bucket = tecnica per gestire le congestioni, che si ispira ad un secchio bucato per cui la coda si adagia nel secchio ma il flusso che esce dal buco è sempre costante a meno che non ci sia nessun pacchetto in coda allora si ferma. Se il pacchetto arriva che la coda è piena viene droppato. È implementato sia in hardware che nel sistema operativo. Produce un flusso di pacchetti costanti piallando il burst e riducendo le probabilità di congestione.
Token Bucket = il sistema precedente crea un pattern d'uscita rigidamente piatto sul livello medio per quanto il traffico sia intenso. Alcune applicazioni preferiscono velocizzare l'uscita quando arriva un grosso burst. In questo algoritmo nel secchio si mettono dei token generati da un clock ogni tot secondi.

Quando conviene usare UDP e quanto TCP come protocollo a livello di trasporto.
UDP = User Datagram Protocol
E' molto semplice perchè permette alle applicazioni di mandare datagram IP incapsulati sena stabilire una connessione. Non fa controllo del flusso e degli errori. Non garantisce che arrivino tutti i pacchetti e si usa quando non si ha tempo da perdere.
TCP = Trasmission Control Protocol
Progettato fin dall'inizio per fornire stream di byte, affidabile, end to end su una internet non affidabile. Sender e reciver creano una socket individuata da un indirizzo ed un numero di porta, ogni socket può gestire diverse connessioni.

Descrivere brevemente il protocollo HTTP.
HTTP = HyperText Transfer Protocol
E' il protocollo di lettura degli ipertesti HTML (HyperText Markup Language) sulla rete.

Descrivere come viene settata e come viene chiusa la connessione TCP (3-way-handshake).
Una connessione è settata da un primo host con una richiesta di connessione al secondo host con un numero di sequenza iniziale proposto. Il secondo host risponde con una accettazione di connessione dicendo che ha ricevuto il numero di sequenza, manda indietro una ricevuta ed un nuovo numero di sequenza. Il primo host riceve la ricevuta ed il nuovo numero di sequenza e manda una ricevuta nello stesso pacchetto del suo nuovo numero di sequenza consecutivo al primo.
La connessione si chiude con il primo host che manda una richiesta di chiusura, il secondo che l'accetta e rimanda la ricevuta (disconnettendosi poi) ed il primo host ricevendo la ricevuta si disconnette a sua volta (detta anche chiusura SIMMETRICA).
Three-Way-Handshake = non richiede che entrambi i lati usino lo stesso numero di sequenza, quindi

si può usare anche quando non c'è un clock globale.

Descrivere l'algoritmo slow start per la gestione della congestione.
È un algoritmo ideato per risolvere le congestioni, che fa crescere continuamente la finestra delle congestioni in modo esponenziale fino a quando non riceve un timeout o raggiunge la finestra del reciver. Tutte le implementazioni TCP lo devono supportare, di slow ha soltanto il nome perchè parte da valori molto bassi.
Partenza lenta (in inglese, slow-start), è una fase dell'algoritmo di controllo della congestione attuato da TCP.
Il mittente TCP inizia trasmettendo il primo segmento dati ed attende un riscontro. Ogni volta che un segmento trasmesso viene riscontrato (si riceve un ACK) il mittente incrementa la finestra di congestione CongWin di una quantità pari al MSS.
Quindi ad ogni RTT la CongWin raddoppia di dimensioni fino a raggiungere la metà della dimensione massima. Da questo punto in avanti l'aumento procede in maniera lineare fino a raggiungere il massimo. Questo valore viene mantenuto finché non si incorre in un evento di congestione, come ad esempio la perdita di un segmento dati, oppure quando la dimensione della finestra di congestione supera il valore della variabile SSTHRESH, evento che conduce alla fase di aumento additivo - diminuzione moltiplicativa (AIMD).