Domande sulla terza parte dei lucidi

1) In cosa consiste la funzione di frammentazione di IP?

Consiste nel suddividere il pacchetto IP in piu frammenti qualora il livello sottostante lo richieda per necessità fisiche della rete su cui si appoggia o per altri motivi. (Es.ethernet)

2) Come vengono usati i campi *Identification* e *Fragment Offset* dell'header IP?

Il campo idetification è lungo 16 bit ed è una sequenza casuale di bit decisa dall'ip sender che viene riprodotto uguale in tutti i frammenti del pacchetto ip.Questo per identificare tutti i frammenti di uno stesso pacchetto.
Il campo fragment Offset indica il byte nel quale il campo dati del frammento deve essere messo al momento della ricomposizione del pacchetto ip a destinazione.Esso è lungo 13 bit ed è espresso in multipli di 8byte.

3) Come sono usati i flag *D* ed *M* dell'header IP?

Il flag D è il flag di Do Not Fragment: esso deve essere posto a 1 quando non si vuole che il pacchetto ip venga frammentato lungo il percorso. Il flag M è il flag di more:esso viene posto a uno in tutti i frammenti del pacchetto ip tranne che nell'ultimo, ad indicare se il frammento corrente è seguito da qualche altro frammento o è il frammento ultimo del pacchetto ip.

4) A cosa serve e come viene usato il campo TTL dell'header IP?

Indica il numero massimo di hop attraversabili dal pacchetto. Ogni nodo decrementa questo valore ogni volta che processa un pacchetto e se questo campo viene posto a zero, si manda un messaggio di errore al mittente del pacchetto.

5) Come si calcola l'*Header Checksum* dell'header IP?

Il mittente del pacchetto calcola il Checksum dividendo il solo header in gruppi da 16 bit e complimentando la loro somma. Ogni nodo che processa il pacchetto invece divide in gruppi da 16 bit l'header somma questi gruppi al checksum del pacchetto ip. Poi complementa il risultato e se si ottengono tutti zeri, il pacchetto viene considerato come corretto, altrimenti viene scartato.

*6)* Quali nodi di rete verificano la correttezza dell'*Header Checksum?*

Ogni nodo sul percorso.

7) Come si verifica la corretta dell'*Header Checksum?*

Vedi domanda 5

8) E' necessario che ogni router attraversato ricalcali l'*Header Checkum* prima di inoltrare un pacchetto?Perché?

Altrimenti non potrebbe sapere se ritenere validi gli altri campi.

9) Cosa indica il campo *Protocol* dell'header IP?

Per specificare per quale protocollo viene mandato il pacchetto ip.
10) Quali opzioni devono essere necessariamente presenti nell'header IP?

Nessuna è obbligatoria.

11)Qual è la lunghezza massima dell'header IP?

60 byte

12) A cosa serve l'opzione Recorde Route?

Serve per scrivere nell'header del pacchetto ip gli indirizzi attraverso i quali un pacchetto è passato. Ce ne possono stare al massimo 9 nell'header ip.

13) A cosa serve l'opzione Strict Source Route?

Serve per specificare gli indirizzi che si vuole che il pacchetto segua. Se per caso uno degli indirizzi specificati non è raggiungibile, allora il pacchetto viene scartato e viene riportato un messaggio di errore al mittente.

14) A cosa serve l'opzione Loose Source Route?

Come la Strict source route, ma se uno degli indirizzi specificati non può essere raggiunto, il pacchetto non viene scartato.

15) A cosa serve l'opzione Time Stamp?

Per sapere a che ora un pacchetto è stato processato da un nodo. I tempi sono da prendere con le pinze perché possono non essere veritieri.

16) A cosa serve il protocollo ARP? Come funziona?

Il protocollo Arp serve per creare dinamicamente associazioni tra indirizzi ip e indirizzi fisici. Esso manda una arp request in broadcast contenente l'indirizzo ip del nodo di cu vuole sapere l'indirizzo mac. Se uno dei nodi riconosce il proprio indirizzo in quello specificato, invia al mittente della arp-request una arp-reply contentente il proprio indirizzo fisico.

17) Perché le righe (entries) della ARP Table hanno un timer di scadenza?

Perché le associazioni create una volta non valgono per sempre dato che alcuni host si possono disconnettere e la configurazione della rete può cambiare.

18) A cosa serve e come funziona il meccanismo di proxy ARP?

Il proxy arp serve in quelle situazioni in cui devono coesistere in un'unica rete piu sottoreti ad esempio a causa di una insufficienza di indirizzi per gli host. Tutti gli host della rete come conseguenza vengono configurati con una netmask pari a 0 e quindi tutti gli indirizzi vengono identificati come della stessa rete. Così una arp request se viene indirizzata ad uno degli host sulla

stessa rete locale, sarà l'host destinatario a rispondere con una arp reply, altrimenti sarà il proxy arp installato sul router a rispondere con l'indirizzo fisico dell'interfaccia del router.

19) A cosa serve il protocollo ICMP?

E' un protocollo che fa reporting di messaggi per errori nell'instraddamento del pacchetto.

20) A cosa servono i messaggi ICMP *Echo request* ed *Echo reply*?

Servono per sapere se un host è raggiungibile.

21) Come opera il comando di *ping* dei sistemi unix e dos?

Es: c:\ping 123.124.143.233

22) Da chi e quando viene generato il messaggio ICMP di *Destination Unreachable*? A chi è diretto il messaggio?

Il messaggio viene generato da uno dei nodi che processano il pacchetto ip.esso è destinato al mittente del pachetto. Viene generato quando la rete non è raggiungibile, quando l'host non è raggiungibile, quando è stato settato il bit di Do not fragment, ma la frammentazione è necessaria, quando uno dei nodi specificati nell'opzione nell'header non è raggiungibile.

23) Da chi e quando viene generato il messaggio ICMP di *Time Exceeded*? A chi è diretto il messaggio?

Il messaggio è diretto al mittente del messaggio.Viene generato o dal router che pone il ttl a 0 o dal destinatario che non si vede recapitare tutti i frammenti di uno stesso pacchetto entro un tempo massimo.

24) A cosa serve e come viene usato il messaggio ICMP di *Redirect*?

> Il messaggio viene utilizzato da un router quando si vuole che il pacchetto intraprenda una strada piu breve o meno congestionata.

26) Quando e perché gli indirizzi IP sono assegnati agli host in modo dinamico?

Sono assegnati in modo dinamico quando non si hanno abbastanza indirizzi per coprire gli host che magari non necessitano sempre di una connessione perché sono spesso inattivi.Inoltre uò essere comodo non configurare ogni volta gli host, ma avere un server che gestisca questa associazione.

27) Come avviene la configurazione di un host in modo dinamico mediante DHCP?

Avviene attraverso uno scambio di messaggi detto Four way handshake, dove l'host richiede al server dhcp di avere un indirizzo ip e il server ne propone uno secondo le sue disponibilità.In caso questo indirizzo andasse bene all'host allora il server crea un'associazione nelle sue tabelle interne tra l'host e l'indirizzo ip.

28) A cosa serve il DHCP relay?

Il dhcp relay serve quando abbiamo piu server dhcp interconnessi al fine di assegnare in modo dinamico un Ip agli hos

29) Con quali protocolli vengono trasportati i messaggi DHCP?

Con il protocollo udp che a sua volta si serve di ip e dei due livelli sottostanti.

30) Fino a quando non viene assegnato l'indirizzo IP che indirizzi IP di sorgente e di destinazione usa il client DHCP?

Indirizzo di sorgente 0.0.0.0 mentre indirizzo di destinazione 255.255.255.255.

31) A cosa servono i messaggi DHCP-Discover, DHCPOffer, DHCP-request, DHCP-ack e DHCP-release?

DHCP-Discover: Viene mandato al server dhcp dall'host quando questo vuole richiedere l'indirizzo ip. In questo messaggio è contenuto l'indirizzo fisico dell'host.

DHCPOffer: In risposta al messaggio precedente il server dhcp manda un indirizzo proposto al client insieme al proprio identificativo.

DHCP-request:In caso il client accettasse l'indirizzo proposto, allora comunica la decisione al. Server.In particolare il messaggio contiene tutte le informazioni necessarie come:gateway di default, indirizzo ip, netmask della rete e DNS server.

DHCP-release: Serve solamente in un ultima fase in quale il client abbandona l'indirizzo ip assegnatogli, comunicando la decisione al server, il  quale può liberamente assegnare lo stesso indirizzo ad un altro client.