Domande IIW 2020-2021

Indice

Descrivere come viene realizzata la comunicazione affidabile nel protocollo TCP

Answer. La comunicazione affidabile del protocollo TCP permette di trasferire segmenti del livello di trasporto al protocollo HTTP senza errori e nel giusto ordine. Il protocollo TCP per creare un canale di comunicazione affidabile risponde a 3 tipi di eventi temporizzati:

- Quando TCP riceve un dato dal livello applicativo, lo incapsula in un segmento e lo passa al protocollo IP. Se il timer non è in esecuzione per qualche altro semgneto, TCP inizializza il timer e lo passa al protocollo IP.

- Quando TCP risponde ad un evento di timeout, il protocollo ritrasmette il segmento e reinizializza il timer;

- Quando TCP riceve un ACK dal destinatario. TCP confronta il valore dell'ACK y con la variabile *SendBase*(rappresenza il numero di sequenza del più vecchia byte non riconosciuto). Dato che gli ACK sono cumulativi, y equivale a riconoscere come ricevuti tutti i segmenti prima del numero di byte y. A questo punto si aggiorna la variabile *SendBase* e si reinizializza il timer se ci sono segmenti per cui non si è ancora ricevuto un ACK.

Una delle problematiche di regolazione delle ritrasmissioni in base ad eventi temporizzati è che può provocare grandi ritardi. Tuttavia, in generale, il mittente può rilevare la perdita del pacchetto prima che l'evento di timeout avvenga. Ciò è possibile tramite gli ACK duplicati che permettono di riconoscere nuovamente un segmento per il quale il mittente ha già ricevuto un ACK. Quando un segmento con un numero di sequenza è maggiore del prossimo numeri di sequenza atteso, dato che si vuole garantire l'ordinamento in sequenza dei pacchetti, si rileva un segmento mancante dovuto sia ad un riordino dei pacchetti nella cammino fra sorgente e destinatario, sia una effettiva perdita. Quindi, il destinatario, manda un ACK duplicato che corrisponde all'ultimo byte ricevuto in ordine. In una connessione, il mittente invia spesso un numero elevato di segmenti e, se uno di questi viene perso, ci saranno molti ACK duplicati. Se il mittente TCP riceve 3 ACK duplicati per lo stesso segmento, lo si considera come se il segmento seguente a quello degli ACK duplicati è perso. In questo caso il mittente effettua il FastRetrasmit, cioè invia il segmento prima che il timer scada. Inoltre, TCP offre un servizio di controllo di flusso per eliminare la possibilità del mittente di colmare il buffer del destinatario e quindi evidare la perdita di segmenti. In particolare si assegna al mittente una variabile receive window per ricevere informazioni sullo spazio libero all'interno del buffer al fine di poter regolare la velocità di invio dei segmenti in base alla spare room del destinatario. Infine si offre un servizio di gestione della connessione TCP in cui il TCP client per instaurare una connessione TCP con un server TCP deve effettuare un three-way handshake per garantire una connessione affidabile:

- Il client TCP, invia un segmento speciale contenente flag SYN=1. Sceglie un numero di sequenza e lo inserisce nel campo opportuno. Il segmento viene incapsulato in un datagramma IP ed inviato al server;

- Quando il segmento SYN arriva al server, viene estratto, si alloca il buffer TCP e le variabili di connessione. Il server, ora, invia un segmento con bit SYN impostato ad uno. Il campo ACK viene impostato a *client_ isn+1*. A questo punto il servere sceglie il proprio numero di sequenza e lo mette nell'header del segmento. Questo segmento è detto SYNACK segmenti.

- Alla ricezione dle semgento, il client alloca i buffer e le variabili di connessione. Invia al server un altro segmento SYN impostato a 0. Questo stato può contenere dati di livello applicativo.

Descrivere il protocollo BGP

Il protocollo BGP è un protocollo di tipo path-vector basato su prefissi e policy che permette di ottenere informazioni di raggiungibilità dei sistemi autonomi vicini, progazione delle informazioni di raggiungibilità a tutti i router interni di un sistema autonomo, conseguimento di buone rotte verso le sottoreti e di comunicazione ad ogni sottorete della proprie esistenza. Si definiscono:

- BGP peer: i router ai capi delle connesisoni TCP semipermanenti e la sua relativa connessione detta sessione BGP.

- La sessione BGP instaurata tra router dello stesso AS viene detta sessione interna BPG altrimenti sessione esterna BGP.

In particolare, i pacchetti non sono instradati verso uno specifico indirizzo di destinazione, ma invece verso prefissi CIDR rappresentanti una subnet o una collezione di subnets. Questo protocollo comprende due task:

- Per ogni AS, ogni router è sia un gateway che un router interno. UN router gateway p un router al confine di un AS che connette direttamente uno o più router all'intenro di un altro AS. UN rotuer interno connette solo gli host e i router all'interno della propria AS. I router inviano informazioni di raggiungibilità tra gli AS per conoscere il cammino dei sistemi autonomi che portano ad una certa destinazione. I rotuter scambiano queste informazioni su connessioni TCP semi permanenti dette BGP connection. Al fine di propagare l'informazione di raggiugibilità, si utilizzano sia iBGP che eBGP.

- Vi possono essere numero cammini da un certo router verso una subnet di destinazione. Quando un router segnale un prefisso lungo una connessione BGP, include nel prefisso gli attributi BGP: AS-PATH, NEXT-HOP. Il primo contiene la lista degli AS lungo i quali vengono passate le notifiche e viene aggiungo ogni volta che un prefisso viene passato tra AS. Questo attributo, inoltre, è utile per prevenire notifiche cicliche: s eun router ha il proprio AS già nella lista, scarterà la notifica. Il secondo attributo è l'indirizzo IP dell'interfaccia del router che inizia l'AS-PATH. Ogni rotta BGP è scritta come una lista di 3 componenti: NEXT-HOP,AS-PATH, prefisso di destinazione.

  Si sceglie la rotta che possiede meno AS.

Descrivere il protocollo ARP

Il protocollo ARP serve a tradurre gi indirizzi di rete in indirizzi MAC. Ogni router host e router possiede una tabella ARP nella sua memoria, il quale contiene un mapping degli indirizzi IP e indirizzi MAC. La tabella ARP, inoltre, contiene un valore di tempo di vita, che indica quando ogni mapping sarà cancellato dalla tabella.

L'host mittente ha bisogno di ottenere l'indirizzo MAC di destinazione dato l'indirizzo IP. Questo compito è facile s ela tabella ARP del mittente ha un'entry per il nodo di destinazione. Nel caso in cui tutto questo non è possibile, il mittente deve costruire un ARP packet che coniente l'indirizzo IP e MAC del mittente e del destinatario. L'obiettivo di questo pacchetto è di richiedere a tutti gli altri host e router nella subnet di determinare l'indirizzo MAC corrispondente all'indirizzo IP da risolvere. Quindi, l'adapter incapsula il pacchetto ARP nel frame, utilizza l'indirizzo broadcast per l'indirizzo di destinazione e lo trasmette nella subnet. Il frame contenente la richiesta ARP viene ricevuto da tutti gli altri adapter nella subnet e ogni adapter passa il pacchetto nel proprio modulo ARP. Ognuni di questi controlla se l'indirizzo IP è uguale all'indirizzo IP di destinazione del pacchetto ARP. Se il confronto ha successo, invia una risposta in pacchetto ARP conenente il mapping desideratro.È un protocollo particolare perché funziona solo nell'ambito della stessa rete LAN e non posso chiedere indirizzi MAC di nodi all'esterno della mia rete ed inoltre un messaggio ARP si limita solo a chiedere l'indirizzo MAC associato ad un preciso indirizzo IP. Per questi motivi lo si può pensare come un protocollo di livello due ma in realtà si considera come protocollo intermedio, ossia un protocollo di livello tre perché risolve indirizzi tre in indirizzi due ma limitato all'interno di una sottorete.

Illustrare e discutere le varie cause del ritardo a pacchetto

In generale un pacchetto parte da un host sorgente, passa attraverso una serie di router e arriva a destinazione. In ogni tappa, il pacchetto subisce vari tipi di ritardo in casciun nodo del tragitto. I principali ritardi sono:

- **Ritardo di elaborazione:** è il tempo richiesto per esaminare l'intestazione del pacchetto e per determinare dove dirigerlo. Questo ritardo può includere il tempo necessario per controllare errori a livello di bit.

- **Ritardo di accodamento:** è il tempo in cui il pacchetto rimane in coda in attesa della trasmissione sul collegamento. Questo ritardo dipende dal numero di apcchetti precedentemente arrivati, accodati e in attesa di trasmissione sullo stesso collegamento. Se la coda è vuota e non è in corso la trasmissione di altri pacchetti, allora il ritardo di accodemento è nullo. Questo ritardo viene modellato tramite concetti di multiplazione statistica e coda $M/M/n$.

- **Ritardo di trasmissione:** assumento che la trasmissione dei pacchetti sia di tipo FIFO; il pacchetto sarà trasmetto solo dopo la trasmissione di tutti i pacchetti che lo hanno preceduto nell'arrivo. Viene devinito come $\frac{L}{R}$ e coincide con il tempo necessario a trasmettere tutti i bit del pacchetto sul collegamento.

- **Ritardo di propagazione:** è il tempo che impiega il bit ad essere propagato. Dipede dal mezzo fisico (velocità della luce) e dalla lunghezza del collegamento.

In totale, il ritardo di un nodo è dato da:

$$d_{\text{node}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{transf}} + d_{\text{prop}}$$

Descrivere il funzionamento di un router NAT. Illustrare, con riferimento a Skype, come sia possibile realizzare connessioni tra client situati entrambi dietro dei router NAT.

I router NAT hanno il compito di gestire l'allocazione degli indirizzi.La prima operazione che deve svolgere un router NAT è quando riceve un pacchetto da un nodo interno alla rete e lo deve trasmettere verso l'esterno: modifica il campo sorgente di tutti i pacchetti, sostituisce al cammpo sorgente l'indirizzo IP della propria interfaccia e assegna un nuovo numero di porta. Così facendo, si utilizza un indirizzo IP per tutta la rete locale e,conseguentemente, gli indirizzi dei nodi interni non saranno più visibili dall'esterno aumentando la sicurezza della rete. Supponiamo che un nodo voglia mandare un pacchetto verso l'esterno, lo inoltra al router NAT che associa nella propria tabella l'indirizzo IP del nodo interno, il numero di porta e per l'indirizzo IP esterno un altro numero di porta e modifica la parte sorgente dell'indirizzo e del numero di porta. In seguito il pacchetto viene inviato all'esterno e il server ricevente invia la risposta al router che, dalla tabella, sostituisce i valori di indirizzo e porta del nodo interno e lo inoltra alla destinazione corretta. In tutto ciò, il client e il server non rilevano la presenza del router NAT. Nel caso in cui un pacchetto in arrivo non è presete nella tabella NAT, il pacchetto viene scartato per una questione di sicurezza. Lo svantaggio dei router NAT è che si limitato il numero di connessioni. I router NAT operano fino al livello 4 per modificare gli indirizzi. Una problematica dei router NAT è il cosiddetto attraversamento della NAT: se un utente vuole comunicare con un server dietro una NAT, non conosce l'indirizzo del server poiché è privato. Una possibile soluzione viene fornita dall'esempio di comunicazione di Skype: un client vuole contattare un altro client dietro un router NAT. A tale scopo, si utilizza un meccanismo che rende ogni client sia interno e esterno alla rete che si connette ad un server relay che gestisce il traffico P2P tra i due client.

Descrivere come viene realizzato il chaching nei sistemi Web

Una Web Cache (proxy server) è un'entità di rete che compie le richieste HTTP al posto del Web Server originale. Il browser di un'utente può essere configurato in modo tale che tutte le richieste HTTP vengano reindirizzate nella WebCache:

1. Il browser stabilisce una connessione TCP al WebCache e invia una richiesta HTTP per l'oggetto alla Web Cache;

2. La Web Cache controlla se la copia dell'oggetto è salvata localmente. Se lo è,il proxy server ritorna l'ogetto all'interno di un messaggio di risposta HTTP al browser del client

3. Se il proxy server non possiede l'oggetto, la Web Cache apre una connessione TCP al server originario. A questo punto, il proxy server invia una richiesta di connessione TCP con il server originario ed invia la richiesta dell'oggetto;

4. Quando la Web Cache riceve l'oggetto, si salva una copia locale e ne menda un'altra all'interno di un messaggio di rispsota HTTP al browser del client.

Questo meccanismo è utile poiché riduce il tempo di rispsota per una richiesta del client: il collo di bottiglia tra client e server di orgine è molto mino rispetto al colo di bottiglia del client e della cache. Inoltre, si ridue il traffico di un'accesos istutuzionale ad Internet e, riducendo globalmente il tempo di risposta, è possibile migliorare il traffico sull'interno Internet migliorando le prestazione di tutte le applicazioni.

Illustrare le differenze tra il controllo di congestione end-to-end e network assisted. Presentare esempi di controllo di congestione network assisted

Nel controllo di congestione End-to-End, il livello di rete non fornisce un supporto esplicito al livello di trasporto. Anche la presenza di congestione di rete deve essere risolta dagli end system basandosi solo sull'ossrvazione del comportamento della rete. In particolare, la perdita di un segmento TCP viene considerata come un'indicazione di congestionamento della rete e di conseguenza la finestra di trasmissione viene ridotta. D'altra parte nel controllo di congestione assistita dalla rete, i router fornisce un feedback esplicito al mittente /destinatario riguardo lo stato della rete. Questo feedback potrebbe essere anche un singolo bit per indiciare il link congestionato. Un esempio di controllo di congestione network assisted è il caso di ATM in cui un router informa il mittente sul massimo rate che il link può supportate.

Descrivere il meccanismo degli ack ritardati in TCP

Il meccanismo degli ACK ritardati fa parte delle funzionalità che il protocollo TCP utilizza per offrire un servizio affidabile di trasporto dati. Quando il destinatario TCP riceve un segmento con un numero di sequenza più grande del prossimo numero di sequenza atteso in ordine, rileva un segmento mancante. Il ricevitore cerca di non inviare ACK appena si riceve il segmento, ma di aspettare del tempo per inviare quell'ACK insieme ad un altro messaggio per minimizzare l'overhead della connessione. In particolare, questo meccanismo è detto piggybacking e, ogni volta che si riceve un segmente si fa partire un timer di 500 ms: se in questo tempo il ricevente deve inviare dati al mittente ingloba l'ACK nel segmento che avrebbe dovuto inviare al mittente. Possiamo distinguere delle casistiche:

- Se ho ricevuto un segmento, faccio partire il timer e ne arriva un altro,allora non facico finire il timer e mando ACK. Se la finestra è molto grande TCP manda un ACK ogni 2 segmenti;

- Se ho pacchetti fuori ordine,il ricevente non fa partire il timer poiché TCP utilizza ACK cumulativi e quindi si limita ad inviare lo stesso ACK relativo all'ultima sequenza di segmenti ricevuti in ordine. Quindi si riscontra molti ACK duplicati e si applica il fast retrasmistit.

Illustrare il funzionamento di uno switch Ethernet. Descrivere le differenze tra uno switch ed un hub

Un HUB è un dispositivo di livello di collegamento che agisce individualmente sul bit. Quando un bit, rappresentante zero o uno, arriva da una interfaccia,l'hub ricrea il bit, applifica la sua energia, e trasmetta il bit su tutte le altre interfacce. Nel caso in cui si ricevano due frame nello stesso istante, vi è una collisisone ed i nodi che sono entrati in collisione devono ritrasmettere. Uno switch p un dispositivo di livello di collegamento che si comporta come un hub, ma con la differenza che permette di evitare le collisioni ed implementa una tecnlogia store-and-forward. Uno switch comprende due funzioni: il forwarding e il filterning. La funzione di filtraggio permette di determinare quando un frame dovrebbe essere inoltrato verso qualche interfaccia o dovrebbe essere scartato. Il forwarding determina le interfaccie al quela il frame dovrebbe essere diretto e quindi si muove il frame verso quelle interfacce. Queste funzioni sono implementate in una switch table che contiene il MAC Address,l'interfaccia che porta verso quell'indirizzo MAC, il tempo di vita della entry. Lo switch aggiorna la propria tabella nel seguente modo:

- Non vi sono entri nella tabella con lo stesso indirizzo. In questo caso, lo switch inoltra delle copie del frame verso i buffer di uscite che precedono tutte le interfacce ad eccezzione dell'interfaccia di partenza;
- Se vi è un'entry nella tabella con la stessa interfaccia, non si ha necessitò di inoltrare il frame su qualsiasi altra interfaccia, si effettua il filtraggio e il frame viene scartato;
- Se vi è un'entry nella tabella con interfaccia diversa. Il fram ha bisogno di essere inoltrato verso il link collegato all'interfaccia nuova. Lo switch effettua la funzione di instradamento mettendo il frame nel buffer di uscita che precede l'interfaccia.

Una proprietà dello switch è il self learning che consente di costruire automaticamente, dinamicamente la tabella di swtich. Grazie a questa proprietà questi sono dispositivi plug-and-play poiché non richiedono nessuna configurazione.

Descrivere come viene realizzato il controllo di congestione TCP

TCP fornisce un servizio servizio di trasporto affidabile tra due processi in esecuzione su differenti host. Al fine di garantire questo servizio, il meccanismo di controllo di congestione è un componente essenziale. In particolare, la velocità limite di ogni mittente che invia traffico sulla propria connessione diventa una indice di congestione della rete aumentando e diminuendo il rate in base alla congestione percepita lungo il cammino. A tale scopo, si usa una variabile congestion window che impone il vincolo di velocità massima del mittente TCP. Inoltre, definiamo un evento di perdita come la frequenza di timeout o di ricezione di 3 ACK duplicati e quindi, quando vi è congestione, uno o più buffer dei router del cammino va in overflow causando lo scarto del datagramma e questi verrano percepiti come loss events. Nel controllo di congestione si tengono presenti i sequenti principi:

- Un segmento perso implica che il rate del mittente TCP dovrebbe essere diminuiti;
- Un ACK ricevuto indica che la rete non è congestionata e il rate può essere aumentato;
- *Bandwidth probing:* si aumenta il rate di invio finché non si verifica un evento di perdita. Nel caso in cui si verifica una perdita, il rate viene diminuito.

Gli algoritmi di controllo di congestione sono i seguenti:

- Slow Start: si inizia il valore della congestion window di 1 MSS ogni volta che si riceve un ACK per un segmento. Il rate iniziale sarà quindi impostato a $\frac{\text{MSS}}{\text{RTT}}$. In seguito ad ogni ACK ricevuto si aumenta la finestra di 1 MSS per ogni semgento riconosciuto, raddoppiando così il rate ad ogni RTT. Questo tipo di crescita è esponenziale e termina quando si verifica un evento di perdita.A questo punto imposta il valore della congestion window a 1MSS

e la variabile sstresh a $\frac{\text{cwnd}}{2}$. La variabile ssthreh è utile per fermare la fase di crescita di slowstart e quando la finestra di congestione è ugulae alla sstresh termina e si va nello stato di congestion avoidance. Se si ricevono 3 ACK duplicati, si effettua il fast retrasmit e si entra nello stato di fast recovery.

- Congestion Avoidance: Quando si entra in questo stato il valore della congestion window è uguale a sstresh. In questa fase asi aumenta la finestra di convesione di $\frac{\text{MSS}}{\text{cwnd}}$ ogni volta che arriva un nuovo ACK o un timeout. Quando si verifica un evento di perdita, cioè si ricevono 3 ACK duplicati e si entra nello stato di fast recovery;

- Fast Recovery: Il valore della finestra di congestione viene aumentato di 1MSS per ogni ACK duplicato che viene ricevuto per il segmento che ha causato questo evente. Eventualmente, qunado arriva un ACK per il segmento mancante, TCP rientra nello stato di congestion avoidance dopo aver diminuito cwnd. Se vi è un timeout, si passa nello stato slowstart dopo avere effettuato le aazioni percedenti,

Descrivere gli algoritmi di routing distance vector

Gli algoritmi distance-vector sono algoritmi di routing decentralizzati in cui il calore del cammino a minor costo viene effettuato in maniera asincrona, iterativa e distribuita nei router. Nessun nodo possiede le informazioni complete sul costo di tutti i link della rete, ma solo di quelli che gli appartengono. Scambiando informazioni con i nodi vicini è possibile calcolare la rotta a minor costo verso la destinazione. I costi vengono espressi tramite l'equazione di Bellman-Ford la cui soluzione fornisce le entry nel nodo x nella tabella di routing. In una rete, si invian ad intervalli di tempo, una copia del proprio vettore delle distanze ad ogni suo vicino. Quando un certo nodo riceve un nuovo vettore, questo viene salvato ed aggiorna il proprio vettore risolvendo l'equazione di Bellman. Dopo l'aggiornamento, il nodo invierà il suo nuovo vettore ad ogni suo vicino che, a loro volta, aggiorneranno i propri valori di conseguenza. Iterando questo procedimento, ogni stima dei costi convergerà al valore vero. Questi tipi di algoritmi soffrono del problema count-to-infinity. In pratica il costo aggiornato potrebbe aumentare se si verifica un routing loop cioè che un pacchetto rimbalza all'infinto tra due nodi a causa dell'aggiornamento delle distanze. Per risolvere questa problematica, si utilizza la tecnica poisoned reverse: se il vicino del vicoino attraversa il nodo vicino per arrivare a destrinazione, allora il vicino dei vicini avvertirà il suo vicino che la sua distanza dalla destinazione è infinito finché non raggiunge la destinaizone. Dato che il vicino crederà che il suo vicino non ha un cammino a destinazione non proverà mai a raggiungere la destinazione attraverso il nodo di routing loop.

Descrivere come viene realizzato il controllo di flusso in TCP

Il protocollo TCP fornisce un servizio di controllo di flusso alle sue applicaizone per eliminare la possibilità di colmare i buffer del destinatario TCP. L'obiettivo è quindi quello di far combaciare la velocità con cui si inviano i dati a quella a cui vengono letti. Si assegna una variabile receive window per dare informazione al mittente sullo stato del buffer del destinatario. Supponiamo un host A stia inviando un file di grandi dimensioni ad un host B su una connession TCP. L'host B alloca un buffer di ricezione nella sua connessione, definendo la dimenzione *RcvBuffer*. In qualche istante di tempo, il processo dell'applicazione del destinatario legge dal buffer. Occorre devinire due variabili

- *LastByteRead:* è il numero dell'ultimo byte nel flusso dei dati letti dal buffer da parte del processo dell'applicazione B;

- *LastByteRcvd:* è il numero dell'ultimo byte nel flusso dati che è arrivata dalla rete ed è stata salvata nel buffer di ricezione.

La relazione che lega le tre variabili è la seguente: *LastByteRcvs-LastByteRead*$\leqslant$*RcvBuffer*.Inoltre, definiamo la receive window come la dimensione rimanente nel buffer:

$$\text{rwnd} = \text{RcvBuffer} - [\text{LastByteRcvd} - \text{LastByteRead}]$$

Questa variabile è dinamica nel tempo e l'host B dice all'host A quanta spare room possiede nel buffer della connessione salvando in ogni segmento la variabile rwnd. Inzialmente è impostato come *rwnd = RcvBuffer*. L'host A deve prendere in considerazione: *LastByteSent* e *LastByteAcked*. Mantenendo la quantità dei dati ancora non ricevuti minore di *rwnd*, l'host A si assicura che il buffer non sta in overflow.

Descrivere le caratteristiche principale dell'applicazione di Posta Elettronica. Si illustrino, inoltre i protocolli di livello applicativo in tale applicazione

Il servizio di posta elettronica è composto da tre componenti: l'userAgent che permette all'utente di leggere,rispondere,inoltrare,salvare e comporre i messaggi, il mailserver che rappresenta il nuclo dell'infrastruttura delle email che garantisce ad ogni utente una mailbox che mantiente e gestisce i messaggi in arrivo e il SMPT, un protocollo client/server che mette in comunicazione utenti tramite i mail server. Quest'ultimo può essere sostituito dai protocollo: POP3,IMAP,HTTP. Il protocollo SMTP utilizza un servizio di trasferimento dati di TCP per inviare dal server le email del mittente e alla mailbox del destinario. Si utilizza la porta 25 e i messaggi sono 7-bit ASCII. Inoltre, è composta da un lato client e un lato server in esecuziione sul server. Il server quindi si può comportare sia come client che come server. In questo protocollo si alternano tre fasi:hanshaking, trasferimento di messaggi, chiusura della connessione. Nel protocollo POP3 l'userAgent apre una connessione sulla mail server nella porta 110. Una volta stabilità, si haq la fase di autorizzazione, in cui si inviano in chiaro username e password per essere autenticato, transazione in cui l'useragent si prelevano i messaggi e si può effettuare la cacellazione. In risposta a quest'ultimo tipo di evento, POP3 restituisce un messaggio di OK o di ERR. Nella fase di transizione si può impostare la modalità download and delete o download and keep che consente, rispettivamente, di scaricar e salvare l'intera posta ed eliminarla una volta terminata la connessione o di ternerla in memoria. L'ultima fase è quella di Update in cui si cancellano i messaggi segnati come tali. Un altro protocollo è l'IMAP che aggiunge delle funzionalità a POP3. In particolare, si associa ad ogni messaggio una cartella INBOX o in altre cartelle definite dall'utente. Infine, l'ultimo protocollo di posta elettronica è HTTP in cui l'utente si connette al mail server tramite una richiesta HTTP e al momento di invio di un messaggio esso passa prima per il browser, poi nel mail server ed infine si utilizza il protocollo SMTP per consegnare il messaggio al destinatario.

Descrivere il meccanismo di ritrasmissione rapida in TCP, evidenziandone i relativi vantaggi e svantaggi.

Una delle problematica delleritrasmissione azionate da timeout è che il periodo di timeout potrebbe essere molto lungo. Quando un segmento è perso, questo lungo periodo di timeout forza il mittente a ritardare il reinvio del pacchetto perso, aumentando conseguentmente il ritardo. L'evento di perdita che fa scattare il timeout può essere causato sia da una perdita del segmento sia da un ordine dei segmenti che non corrisponde all'ordine in cui sono stati inviati. Poiché il mittente generalemtne invia spesso un grande numero di segmenti, se uno di questi viene perso, ci saranno molti ACK duplicati che identificano la presenza dle segmento perso. Quindi, se il mittente riceve 3 ACK duplicati per lo stesso dato, si considera il segmento come perso e quindi TCP attua il fast retrasmist: cioè si ritrasmette il segmento prima che il timer scada.

Descrivere il meccanismo dell'avvelenamento del percorso inverso "poisoned reverse"

Il meccanismo dell'avvelenamento del percorso inverso entra in gioco nell'istante in cui si determina la rotta a minor costo e vi si presenta un routing loop. In particolare, se z percorre y per giungere alla destinazione x, allora z avvertirà y che la sua distanza da x è infinito. Quindi z continuerà a aggiornare questa informazione per y fino a che non si sia determinata la rotta che porta da x verso y. Dato che y crede che da z non si ha un cammino verso x, y non proverà mai a giungere ad x attraverso z. Anche se questo meccanismo risolve il problema del routing loop, in realtà non è così poiché se vi sono loop da tre o più nodi, il poisoned rever non li rileva.

Descrivere il funzionamento del protocollo di accesso al mezzo (protocollo MAC) nelle reti Ethernet

Il protocollo MAC specifica le regole per trasferire un framse su un link. Per i link punto punto si ha un singolo mittente e destinatario agli estremi della rete. Invece, per i link broadcast in cui un utente può potenzialmente accedere al mezzo insieme a tanti altri si ha necessità di coordinare gli accessi al mezzo. I protocolli che rendono possibile l'accesso al canale possono essere suddivisi in tre categorie:

- Protocolli di partizione di canle in cui si partizione il canale in frequenza FDM o in tempo TDM. Nel secondo, si suddivide il canale in frame temporale ognuno dei quali composto da N slot. Ad ogni slot si associa uno degli N nodi e quando deve inviare un pacchetto, quest'ultimo viene inviato nell'intervallo di tempo assegnatogli. Questa tecnica elimina le collisioni, ma si limita la velocità di trasmissione. Nel primo metodo, si dive il canale in differenze frequenze dedicate ad un solo degli N nodi e si hanno gli stessi vantaggi di TDF. Un altro protocollo a suddivisione di canale è il CDMA in cui si assegna ad ogni nodo un codice utilizzato per cripare i bit che invia. Se il codice è ben posto è possibile trasmettere contemporaneamente evitando le collisioni.

- Protocolli ad accesso casuale: un nodo trasmette sempre alla velocità massima del canale. Quando vi è una collisione, ogni nodo coinvolot nell'evento di collizione ritrasmette ripetutamente il suo frame finché non arriva senza coolizione. Tuttavia, quando un nodo riscontra una collsione, la ritrasmissione avviene con un appropriato ritardo scelto indipendentemente dagli altri nodi. Ne sono un esempio Slottet ALOHA,ALOHA protocol,CSMA/CD;

- Protocolli a turnazione: si suddividono in due sotto-categorie.

    - Nel protocollo di polling si richiede che uno dei nodi sia progettato come nodo master. Il nodo master interpella ogni nodo in maniera round-robin. In particolare, il nodo master prima invia un messaggio al nodo 1 dicendo che può trasmettere un certo numero di frame. Dopo di che passa al nodo 2 e cosi via. Questo protocollo permette di eliminare le collisioni,ma si aggiunge un ritardo dovuto all'interpellamento dei nodi. UN altro protocollo a turnazione è il protocollo Token-passing in cui non vi è un nodo master, ma si ha un frame detto token che viene scambiato tra tutti i nodi in ordine fissato. QUando un nodo riceve il token, lo maniente solo se ha qualche frame da trasmettere altirmenti lo inoltra immediatamente al prossimo nodo. Quest'ultimo protocollo è decentralizzato e altamente efficiente. Ma lo svantaggio è che il fallimento del nodo può causare un crash dell'intero canale.

Descrivere il funzionamento del protocollo HTTP

Il protocollo HTTP definisce come i client web richiedono le pagine web ai web servers e come i server trasferiscono le pagine web ai client. Quando un utente richiede la pagina Web, il browser invia al server messaggi di richiesta HTTP per gli oggetti nella pagina. Il server, quindi, riceve la richiesta e risponde con un messaggio di risposta HTTP contenente gli oggetti richiesti. Il protocollo HTTP utilizza il protocollo TCP come il suo protocollo di livello inferiore. Infatti, il client HTTP instaura una conessione TCp con il server nella porta 80 e una volta stabilità la connessione, i processi del browser e il server accedono a TCP attraverso le proprio socket. Una volta che il chient invia un messaggio nella sua interfaccia socket, quest'ultimo passa al protocollo TCP che garantisce un servizio affidabile di trasgferimento dati ad HTTP. QUesto implica che ogni messaggio di richiesta HTTP inviato da un processo client arriva intatto al server e viceversa. Il protcollo HTTP è detto protocollo stateless poiché non maniente informazioni sui client. Vi sono delle versioni differenti dal protcollo HTTP 1.0/1.1 in base, rispettivamente, alla persistenza o meno della connessione.

Descrivere e motivare le differenze principali di routing intra-AS e inter-AS

La rete è una collezzione di router interconnessi. Per promuovere la scalabilità e l'autonomia amministrativa si è scelto di organizzare i router in sistemi autonomi (AS), ognuno di questi costituito da un gruppo di router con lo stesso controllo amministrativo. I router all'interno dello stesso AS (intra-AS) eseguono lo stesos algoritmo di routing. i router che eseguono algoritmi di routing diversi vengono detti inter-AS. Un esempio di protocollo intra-AS p il protocollo OSPF. Questo è un protocollo link-state che utilizza il flusso delle informazioni dello stato dei link per implementare l'algoritmo di Dijkstra. In particolare, ogni router costruisce una mappa topologica dei router all'interno dell'AS ed ognuno di questi esegue localmente l'algoritmo di Dijkstra per determinare un albero di cammini più corti verso tutta la subnet con se stesso come nodo radice. Inizialmente i costi individuali dei link sono impostati dall'amministratore di rete. OSPF include, inoltre, le seguenti funzionalità:

- Sicurezza: fornisce un servizio di autenticazione tra router;
- Multipla same-costs path: si mette a disposizioni molteplici path, se esistono, a minor costo;
- Supporto routing multcast e unicast;
- Supporto per la gerarchia in un intra-AS.

I protocollo inter-AS coinvolgono la coordinazione di molteplici AS e quindi deve essere esguito in parallelo con il protocollo OSPF. Uno degli algoritmi di routing utilizzati è il BGP. In particolare, i pacchetti non sono diretti verso uno specifico indirizzo di destinazione, ma invece verso dei prefissi CIRD ognuno dei quali rappresenta una subnet o una collezione di subnets. BGP fornisce un mezzo ad ogni router per:

- ottenere informazioni sulla raggiungibilità di un prefisso degli AS vicini;
- determinare la rotta migliore verso i CIDR. UN router potrebbe imparare su 2 o più rotte versono uno specifico prefisso e per determinare la migliore rottam il router, localmente, eseguirà la procedura di selezione della rotta tramite GBP in base alla policy ottenuta dalle informazioni di raggiungibilità.

Ne dettaglio il protocollo di routing BGP si articola di due fasi:

1. Avvertimento sulle informazioni di rotta: ogni router viene considerato sia gateway che router intern e i router di gateway scambiano informazioni di raggiungibilità tra AS per conoscere i cammini che portano verso la destinazione.
2. Calcolo della rotta migliore: Si utilizzano gli attributi AS-PATH,NEXT-HOP per scegliere la rotta da prendere.

Descrivere il funzionamento del DNS

Il DNS-domain name system serve ad identificare gli host Intentet. Un identificatore per un host è detto hostname e da informazioni sulla posizione dell'host in Intenet. Poiché gli hostname,a lfanumerici e di lunghezza variabile, non sono adatti al routing si introduce l'indirizzo IP. Il DNS fornisce un mapping tra hostname ed indirizzo IP. Il DNS è un database distribuito, che utilizza il protocollo UDP in una gerarchiad i DNS servers e un protocollo di livello applicativo che permette agli host di esefuire query al database distribuito. La traduzione tra hostname ed indirizzo IP segue:

1. L'utente esegue il lato client dell'applicazione DSN;

2. Il browser estrae l'hostname e lo passa alla parte client dell'allicazione DNS;

3. Il client DNS invia una query contenente l'hostname al DNS server;

4. Il DNS client riceve na risposta che include l'indirizzo IP per l'hostname;

5. Una volta che il browser riceve l'indirizzo IP dal DNS può iizia una connessione TCP con il processo server HTTP localizzato dall'indirizoz IP.

In aggiunta, fornisce i seguenti servizi:

- Host Aliasing: un host con un nome complicato può avere uno o più nomi che riferiscono allo stesso indirizzo IP;

- Mail server aliasing: il protocollo DNS può essere invocato da un'applicazione mail per ottenre dall'hostname l'indirizzo IP;

- Load distribution: DNS è utilizzato anche per implementare una distribuzione di carico lungo i server replicati.

Per gestire problemi di scalabilità DNS utilizza una struttura gerarchica composta da tre classi di indirizzi sever:

- root DNS server: forniscono gli indirizzi IP per i server TLD;

- TLD: (es.com,.uk) forniscono l'indirizzo IP ai server autoritari;

- DNS server: sono utilizzati per gli enti pubblici.

In generale una query al DNS non permette di ottenere l'indirizzo IP del server autoritario, ma si può ottenere interpellando i server intermediari tramite query ricorsive, in cui si richiede la risoluzione del nome per conto sle server, o query iterativi, in cui il serrver contattato risponde con un nome di srver da contattare per risolvere il nome che si cerca. Quindi, la query dall'host richiedente al server DNS è ricorsiva e le rimannenti sono iterative.

Descrivere le caratteristiche principali del protocollo HTTP 1.1

Il protocollo HTTP 1.1 definisce come i client web richiedono le pagine web ai web server e come i server trasferiscono le pagine web ai clients affidandoti al protcollo TCP. La particolarità del protocollo HTTP 1.1 è quella di utilizzare connessioni HTTP persisenti: il server lascia la connessione TCP aperta dopo aver inviato la rispsota HTTP e le successive richieste e risposte tra i due possono essere inviati lungo la stessa connessioni. Questo permette di inviare una intera pagina Web su una singola connesisone TCP. Possonoe ssere di due tipologioe:

- Connessioni persistenti senz apipeling: questi tipi di connesisone non conentono l'invio incontrollato di richieste e quindi di risposte tra client e server. In particolar,e il client deve aspettare la rispsota del server per effettuare la nuova richiesta mantenendo la stessa connessioni;

- Connessioni persistenti con pipeling:; questi tipi di connesisoni consentono l'innvio e la ricevizioni di richieste e risposte HTTP in congtemporanea, senza dove aspettare la rispsota dle server.

Descrivere come viene effettuata la demultiplazione del protocollo TCP

La demultiplazione TCP serve al protocollo TCP per trasportare il segmento in arrivo dal livello di rete al livello superiore ed in particolare serve ad indirizzare il dato verso la socket corretta. La socket TCP è identificata da quattro valori: indirizzo IP sorgente, numero di porta sorgente, indirizzo IP di destinazione, numero di porta di destinazione. Quando un segmento TCP arriva dalla rete ad un histm l'host utilizza tutti e quattro questi valoir per demultiplare il segmento alla socket corretta.

Descrivere le caratteristiche del protocollo OSPF

OSPF è un protocollo link-state che utilizza il flusso dell einformazioni dello stato del link e l'algoritmo di Dijskstra per fornire moltelici rotte a mino costo. Ogni router determinare un albero di cammini costruisce una mappa toèpologia dell'intero AS. Ogni router, quindi, esegue localmente l'algoritmo di Dijikstra per determinare un albero di cammini più corti verso tutta la subnet con se stesso come nodo radice. I costi inviduali del link sono configurati dall'amminisratore di rete: nel caso in cui li impostasse as 1, si ottiene il routing a minimo hop.

OSPF fornisce meccanismi per detemrinare il cammino a minor costo per un dato insieme di pesi dei link. Un router invia in broadcast le informazioni di routing verso tutti gli altri router nel sistema autonomo ogni qual volta che percepisce un cambiamento dello stato dei link. Questo stambio di informaizoni può avventire anche dopo un certo intervallo di tempo. OSPF fornice:

- Sicurezza: gli scambi di informazioni tra router possono essere autenticati;
- Fornisce moltreplici cammini a minor costo se possibile
- Multicast OSPF che, tramite un database dei link, si determina la rotta migliora
- Si possono scegliere dei router che hanno il compito di comunicare con gli altri AS.Quindi si può instaurare una gerarchia all'intenro dell'AS.

Descrivere le differenze tra le versioni 1.0 e 1.1 del protocollo HTTP

Il protocollo HTTP definisce come i client web richiedono le pagine web ai web server e come questi trasferiscono le pagine wei a clients. Questo è un protcollo che si appoggia sul protocollo TCP per gestire le richieste e le risposte HTTP e, al momento della progettazione, occorre decidere se adottare il protocollo HTTP 1.0 con connessione non persistente o il protocollo HTTP 1.1 con connessione persistente.

Nel primo il client deve avviare una connessione ogni qual volta deve richeidere un oggetto al server avviando una connessione TCP, inviando una richiesta HTTP ed aspettare una sua risposta. Possiamo definire l'RTT Round Trip Time come il tempo necessario per un pacchetto a viaggiare dal client al server e viceversa. Questo parametro prende in considerazione il ritardo di propagazione, di accodamento, trasmissione e processamento. Il difetto di questo tipo di connessione è che per ogni oggetto si deve aspettare 2*RTT, si consumano molte risorse le connessioni in parallelo sono limitate. Nella seconda tipologia il server lascia la connessione TCP aperta dopo aver inviato la rispsota HTTP. Le successive richieste e risposte tra i due possono essere inviati lungo la stessa connessione. In aggiunto, possono essere divise in due categorie: le connessioni persistenti senza pipeling in cui non si consente l'invio incontrollato di richieste e di risposte tra client e server, ma si deve aspettare la riezione della risposta per avanzare nuove richieste; le connessioni persistenti con pipeling che ocnsentono l'inzio e la ricezione di richieste e risposte HTTP in contemporanea senza dopver aspettare la risposta dle server.

Descrivere il funzionamento del protocollo ALOHA

Il protocollo ALOHA è un protocollo decentralizzato ad accesso casuale del livello di collegamento che consente di definire delle regole per l'accesso al mezzo. Questo protocollo richiedere che tutti i nodi del canale broadcast siano sincronizzati nelle trasmissione per consentire la trasmissione all'inizio di uno slot. Quando arriva un frame, il nodo trasmette immediatamente il frame interamente nel canale broadcast e se subisce una collisione con una o più trasmissioni, il nodo sarà immediatamente ritrasmesso con probabilità p. Altrimenti, il nodo aspetta un tempo di trasmissione di un frame e, trascorso questo tempo, il nodo ritrasmette il frame con probabilità p o aspetta per un altro tempo di frame con probabilità (1-p). Le sue prestazioni sono molto minori rispetto a Slotted Aloha che ha un'utilizzazione del canale del 37% a fronte del 18% di Aloha. La differenza risiede nel fatto che in slotted Aloha si dedicano slot in cui poter inviare frame alla massima velocità e se vi è una connessione, la ritrasmissione non avviene immediatamente, ma solamente all'inizio dello slot successivo.

Illustrare le caratteristiche principali dle protocollo RIP

Il protocollo RIP è un protocollo che si basa sull'algoritmo Distance Vector, la cui metrica è il numero di hops cioè il numero di hops da effettuare per arrivare a destinazione. Per avere la rotta a minor costo e quindi a minor numeor di hops occorre inizializzare il coto dei collegamenti ad 1. Questi costi vengono calcolati trai router sorgente e la sottorete di destinazioni.

A differenza degli OSPF, il protocollo RIP permmette di scambiare il vettore delle distanze ai router adiacenti tramite un particolare messaggio detto RIP advertisements. I messaggi RIP contengono un'intestazione, il tipo di comando e la versione. Ogni destinazione cotiene il tipo di famiglia di indirizzi.

Descrivere il funzionamento di uno switch. Motivare inoltre perché la topologia "attiva" di una rete LAN non possa avere dei cicli

Gli Switch sono dei dispositivi del livello 2 con il compito di ricevere i frame ina rrivo del livello di colelgamento e inoltrari sul link di ushita. Il lavoro dello switch è trasperente agli host e ai router. Si compone di due funzioni il filtering e il forwarding implementate entrambi nella switch table dello switch. Questa tabella è composta da tre campi: indirizzo MAC, interfaccia che porta verso quell'indirizzo MAC e il tempo in cui è stata inserita la entry (aging-time).Supponiamo che un frame arrivi in una certa interfaccia x, possono verificarsi le seguenti casistiche:

- Non vi sono entry nella tabella con los tesso indirizzo di destinazione. In questo caso, lo swtich inoltra delle copie del frame verso i buffer di uscita che precedono tutte le interfacce ad eccezione dell'intervaccia x;

- Vi è un'entry nella tabella con stessa interfaccia. In questo caso, il frame sta arrivando da un segmento LAN che contiene l'adapter .Non vi è necessità di inoltrare il frame su qualsiasi altra interfaccia; quindi lo switch effettua la funzione difiltraggio scartando il frame;

- Vi è un'entry nella tabella, con una nuova interfacca. In questo caso, il frame ha bisogno di essere inoltrato verso il segmento LAN collegato all'interfacciay. Lo switche ffettua la funzione di forward mettendo il frame nel buffer di uscire cheprecede l'interfaccia y.

Uno switch ha la proprietà che la sua tabella viene costruita automaticamente, dinamicamente e autonomamente senza qualsiasi intervento dall'amministratore di rete o da un protocollo di configurazione. Ed infine possiede permette di eliminare le collisioni,di mantente link eterogenei, gestire la sere.

Nella topologia attiva, anche detta la topologia ad anello, si implementa il protocollo token passing. Questo protocollo è un protocollo a turnazione basato su frame speciale detto token che viene inviato a tutti i nodi della node Ring e, a turno, abilita il possessore del toker l'invio dei dati a massima velocità. Non si può avere i cicli poiché equivarrebbe, al massimo, a mantenere il token senza non volerlo mai cedere e a quel punto si avvia una qualche procedura di ripristino per correggere il guasto.

Illustrare la gerarchia dei server DNS e la differenza tra query DNS iterative e ricorsive

Il DNS ha il compito di fornire un mapping tra l'hostname e l'indirizzo IP. Per motivi di scalabilità si è scelto di organizzare il DNS tramite un database distribuito gerarchicamente in cui possiamo identificare tre classi di indirizzi: rott DNS server che fornisce l'indirizzo .com/.uk e forniscono l'indirizzo IP dei server autoritati, DNS dei server autoritari che vengono utilizzati per gli enti pubblici e i server DNS locali che non fanno necessariamente parte della gerarchia ma sono forniti dagli ISP per velocizzare il servizio. In generale una query al DNS non permette di ottenere l'indirizzo IP del server autoritario, ma si può ottenere interpellando i server intermediari tramite query ricorsive, in cui si richiede la risoluzione del nome per conto sle server, o query iterativi, in cui il serrver contattato risponde con un nome di srver da contattare per risolvere il nome che si cerca. Quindi, la query dall'host richiedente al server DNS è ricorsiva e le rimannenti sono iterative.

Commutazione a circuito

Nella commutazione a circuito le risorse richieste lungo un percorso per consentire la comunicazione tra sistemi periferici sono riservate per l'intera durata della sessione di comunicazione. Questa è una connessione end-to-end con servizi dedicati e si riservano velocit di trasmissione e buffer di comunicazione. Una volta che la comounicazione è stata istanziata le prestazioni sono garantiti e viene fornito un servizio affidabili. Comprende 3 fasi: call setup, trasferimento dati, call teardown.

Dato che le risorse sono condivise, si deve allocare la capcaità trasmissiva tramite la FDM o TDM. Nel primo metodo si suddividono le frequenza disponibili del link di comunicazione in base agli utenti attivi nella rete e nel caso in cui tutte le frequenze siano occupate, la comunicazione viene scartata. Nel secondo metodo, si suddivide la capacità del link nel tempo. Ad ogni slot di un frame si inserisce una chiamata che verrà riassegnata al frame successivo. Questo contente un'assegnazione di chiamate del tipo Round-Robin. Il grande svantaggio di questa tecnica è che l'assegnazione viene fatta ad ogni frame e quindi si pososno riscontrare periodi di silenzi.

Commuatazione a pacchetto

Le applicazioni scambiano informazioni che vengonod divisi in pacchetti contentente dati. Nelle reti LAN le risorse vengono condivise ed ogni pacchetot utilizza il massimo della capacità dle link. La commutazione di pacchetto è una commutazione di tipo store-and-forward cioè il commutatore deve ricevere l'intero pacchetto prima di poter cominciare a trasmettere sul collegamento in uscita il primo output. Il router è un disposiitivo dotato di molti collegamenti e la sua funzione è quella di instradare un pacchetto in entrata su un collegamento in uscita e non può trasmettere i bit che ha ricevuto finché non ha immagazzinato nel suo buffer tutti i bit del pacchetto in arrivo. In una rete a più collegamenti, il commutatore deve mantenere per ogni collegamento un buffer di output per conservare i acchetti che sta per inviare su quel collegamento. Se un pacchetto richiede l'invio su un collegmaneto, ma questo è occupato da un'altra trasmissione, quello in arrivo deve attendere nel buffer di output e quindi si può formare del ritardo di accodamento. Questi ritardi dipendono dal livello di traffico nella rete e si possono verificare perdite di pacchetti. A causa di questa variabilità di ritardo e della perdita di pacchetit in base al traffico, la commutazione a pacchetot viene detta multiplazione statistica e può essere modellata tramite code M/M/n.

UDP

Il protocollo UDP è un protocollo di trasporto leggero dotato di servizi minimalisti. Infatti, è senza connessione, non necessità di handshaking (a differenza del protocollo TCP) e fornisce un servizio di dati inaffidabile. UDP prende i messaggi dal processo dell'applciazione, allega i campi di numeri di porta sorgente e destinazione necessari per multiplazione (incapsulmanente dei dati in un segmento UDP) e la demultipklazione con due cami aggiunti e lo invia nel livello sottostante di rete. Il livello di rete incapsula il segmento del libvello di trasposrto in un datagramma IP ed efetuta una consegna best-effort a destinazione. Se il segmento arriva all'host di destinazione, UDP utilizza il numero di porta di destinazione per consegnare il dato del segmento al processo dell'allicazione. UDP è un protocollo connectionless poiché non si effettua l'handshaking, ma fornisce un servizio di controllo degi errori tramite il campo checksum: in cui si effettua una somma a complemento ad 1 di i bit e il risultato viene messo in questo campo. A questo punto il destinatario effettua il checksum del segmento e lo controlla con quello del segmento UDP.

User-Server Interaction: Cookies

I server HTTP sono stateless, cioè non mantengono informazioni sul client una volta che la connesisone è terminata. Spesso i siti Web necessitano di identificare gli utenti, limitare le attività di altri utenti o di personalizzare i contenuti presenti nella pagina Web. A tale scopo, si utilizzano i coockies. Questi sono formati da quattro compoentni: header di risposta HTTP, header di richiesta HTTP, file mantenuto sul sistema dell'utente e gestito dal browser, file mantenuto sul database del sito. La prima volta in cui l'utente visita il sito, fornisce un identificativo. Durante le successive sessioni, il browser trasferisce un cockie header al server per permettere la sua identificazione nel server.Inoltre, sono usati per creare un livello di sessione utente sul protocollo HTTP stateless, inviando in ogni interazione le informazioni per autenticare automaticamente l'utente.

FTP

Il protocollo FTP è un protocollo di trasferimento file, in cui l'utente utilizza un host locale per trasgerire file da o verso un host remoto. L'utente interagisce con il protocollo FTP tramite un FTP user agent fornendo inizialmente il nome dell'host remodo, in modo che il processo FTP client nell'host locale stabilista una connessione TCP con il processo FTP dell'host remoto e, inoltre fornisce nome identificativo e password e quindi è un protocollo che deve mantenere lo stato dell'utente a differenzza di HTTP. Dopo di che è possibile inviare file da un host locale a quello remoto. In particolare, si utilizzano due connessioni: la connessione di controllo sulla porta 21, utilizzatta per inviare informazioni di controllo, e la connessione dati in cui si inviano effettivamente i dati sulla porta 20. Questo protocollo è detto fuori banda poiché utilizza una connessione aggiuntiva per scambiare dati. Nel caso in cui si volesse inviare più di un file con il protocollo FTP, la connessione di controllo rimane attiva, mentre quella dati verrebbe chiusa e riaperta.

P2P File Distribution - Bit Torrent

In una architettura P2P, non vi è garanzia di prescenza di server sempre accesi, ma si hanno coppie di host connessi detti peer che comunica direttamente tra di loro. Ognuno dei peer può ridistribuire qualsiasi porzione del file che ha ricevuto da qualsiasi altro peer permettendo, quindi, di svolgere funzioni di server.

In BitTorrent, la collezzione di tutti i peer che partecipano nella distribuzione di un file è detto torrent. I peer in un torrent scaricano chunk (porzioni) di file da un altro peer. Quando un peer is unisce ad un torrent, non possiede chunks, ma li accumula durente il tempo,scaricandoli e mettendoli a disposizione del torren e, una volta acquisito l'intero file, ha la possibilità di lasciare il torren o continuare a contribuire all'upload del file. In particolare, ogni nodo pssiede un nodo detto tracker che ha il compito di registrare e di mantenere traccia dei peer che partecipando la torrent. A questo punto il nuovo peer prova a stabile delle connessioni TCP concorrenti con tutti i peer, detit peer vicini, dalla lista dei peer che ha ricevuto dal tracker. In un dato istante, ogni peer avrà quindi un sottoinsieme di porzioni di file e, periodicamente, chiederà ad ogni peer vicino la lista dei chuk che possiede. A questo punto per decidere quali chunk richiedere si utilizza la tecniche del più raro prima al fine di velocitzzare la distribuzione del file. Per decidere quali richiede i peer devono rispondere si utilizza un algoritmo di trading in cui si da la priorità ai vicini con cui si sta scaricando alla velocità massima: per ogni vicino,ogni 10 secondi, si misura il rate di ricezione dati e si determinano i 4 peer con il rate massimo e, ogni 30 secondi, si sceglie un vicino aggiuntivo casuale ed invia i chunk. Se i due peer sono soddisfatti con lo scambio, si metteranno a vicende nella top quattro peer e continueranno a scambiarsi i chunk finché saranno incompatibili.

Architettura di un Router

Un router è responsabile del trasferimento effettivo dei pacchetti tra i link. Un router è compsoto da quattro componenti:

- Porta di ingresso: effettua varie funzioni tra cui terminare un link di ingresso a livello visico e al livelo di collegamento fa intergire due link diversi. Inoltre determina la porta di uscita in cui un pacchetto in arrivo sarò instradato dalla switch fabri.

- Switching Fabric: è la fabbrica di coommutazione che connette le porte in ingresso alle porte di uscita;

- Porte di uscita: ha il compito di salvare i pacchetti ricevuti dalla fabbrica di commutazione e li trasmette sul link di uscita sfruttando le funzionalità del livello di colelgamento e fisico;

- Routing Processor: è il processore del router e si eseguono i protocolli di routing, si mantengono le tabelle di routing e si allegano le informazioni dellos tato del link.

Queste quattro componeneti sono realizzati via hardware.

Switching

La switchin fabri ha il compito di commutare da una porta di input ad una porta di output. Può essere realizzata nei seguenti modi:

- Switching attraverso la memora: si commuta attraverso la CPU. In particolare, una porta di input con un pacchetto in arrivo, attraverso un interrupt, segnala il processore. Quindi, il pacchetto viene copiato dalla porta di ingresso nella memoria del processore e il routing processor estra l'indirizzo di destinazione e cerca la porta di uscita nella tabella di forward, copia il segmaneto nel buffer di uscita.

- Switchin attraverso un bus: una porta di ingresso trasferire un pacchetto direttamente nella porta di uscita su un bus condiviso senza intervento del processore. Viene effettivamente implementato tramite una switch-internal label che inca la porta di uscita locale a cui si sta trasferendo e trasmettendo il segmento sul buts. Tutte le porte di uscita ricevono il macchetto, ma solo la porta corrispondente manterrà il pacchetto.

- Switching via interconnection network: è una commutazione a crossbar cioè un'interconnessione di rete costituita da 2*N bus che connettono N porte di ingresso ad N porte di uscita. Ogni bus verticale interseca ogni bus orizzonale. Quando arriva un pacchetto che ha bisono di essere inoltrato, il controller chiude il punto di incrocio nell'intersezione dei due bus e quindi invia il segmento solo ad una porta di uscita. L'unico ritardo si può verificare quando le porte di ingresso sono differenti ma quella di uscita è una.

CSMA e CSMA/CD

Sia che in slotted ALOHA che in ALOHA, la decesione di un nodo di trasmettere è presa indipendenmtente dall'attività degli altri nodi collegati al canale broadcast. In particolare, un nodo non presta attenzione ne a cosa accade ad un altor nodo ne ferma la trasmissione se un altro nodo invia a interferire con la propria trasmissione. Per prendere in conderazione questi due aspetti sono stato introdotti i protocollo carrire sense multiple access e carrire sense multiple accesse with collision detection.

- CSMA: se un frame di un altro nodo è in trasmissione nel canale, un nodo aspetta finché non rileva nessuna trasmisisone per un piccolo intervallo di tempo;

- Nel CSMA/CD: quando un nodo effettua il CSMA, cessa la trasmissione appena rileva una collisione. Questo aiuta le performance del protocollo non trasmettendo un frame corrotto nella sua interezza. In particolare:

    - L'adapter ottiene un datagramma di livello di rete, prepara il frame di livello di collegamento e lo mette nel buffer;

    - Se l'adapter perscepisce il canale vuoto, trasmette. Altrimenti, aspetta finché non perscepisce nessun segnale di energia e trasmette;

    - Mentre trasmette, l'adapter controlla la presenza di segnali di energia in arriva dagli altri adapter sul canale broadcast. Se non trova questi segnali, trasmette il frame; altrimenti, scarta la trasmissione;

    - Se rileva segnali di energia nella trasmissione aspetta un tempo casuale dettato da un algoritmo di backoff esponenzione che calcola il tempo di attesa prima di effettuare CSMA in base al numero di collisione che si sono percepite durante la trasmissione del frame. A 10 collisioni, il frame viene scartato.

SSL

La crittografia può essere usata per arricchire TCP dando luogo ad un protocollo detto SSL, unaversione arricchita di TCP con servizi di sicurezza, tra cui la riservatezza, l'integrità dei dati e l'autenticazione del client e del server, intermedio tra l'applicazione e TCP (protocollo intermedio di livello tra il 4 e il 5). È caratterizzato da diversi passi. Nella fase di handshake: una volta inizializzata la connessione TCP, il client invia un messaggio e il server risponde con il proprio certificato firmato con la chiave pubblica. Il client allora genera la chiave master e la invia, tramite la chiave pubblica, al server, il quale la decifra. Nella fase di derivazione delle chiavi: tramite la chiave master vengono generate 4 chiavi, due per la cifratura (una per i dati da client a server e un'altra per il viceversa) e due per la parte di integrità (MAC). Nella fase di trasferimento dati: il flusso di dati viene suddiviso in record, ne viene calcolato il MAC insieme alla chiave, ottenendo il messaggio e la firma. Oltre a questi passi, c'è una fase di negoziazione, in cui viene deciso che tipo di algoritmo di cifratura usare.

E-mail Sicura

Un'entità vuole inviare una e-mail ad un destinatario. Si usa un meccanismo a chiave simmetrica dove la chiave viene scamviata usanto la chieve pubblica del destinatario, la quale si ottiene dalla CA,certificato di autorità. Per combinare sia confidenzialità, autenticazione e integrità è il seguente:il mittente prende il messaggio, si calcola l'hash e applica la firma digitale sul digest del messaggio. Il mittente genera una chiave simmetrica, la cifra con la chiave pubblica del destinatario e invia un messaggio con la chiave simmetrica cifrata e un messaggio cifrato che contiene il messaggio originario con la firma digitale. Il destinatario usa la sua chiave privata per estrarre la chiave simmetrica, la usa per decifrare il messaggio, applica l'hash al messaggio, applica la chiave pubblica del mittente così autentica il messaggio per estrarre (H(m)) e fa il confronto. Così so che il messaggio è stato inviato proprio dal mittente che mi aspettavo, sono sicuro della sua identità e so che il messaggio non è stato modificato. Un protocollo che funziona come sopra riportato è il PGP, il quale permette la sicurezza della posta elettronica ed usa crittografia a chiave simmetrica, a chiave pubblica, funzione hash e firma digitale.

Firma digitale

La firma digitale è una tecnica crittografica simile alla firma a mano. Chi invia un documento può firmarlo in modo da certificare la sua provenienza ed è verificabile e non può essere alterato. L'idea è che quando un mittente scrive un documento, solo lui lo può firmare usando la sua chiave privata e cifralo. Quando un destinatario riceve un messaggio firmato, per verificare che effettivamente è stato inviato e firmato da un certo mittente e non è stato firmato da nessun altro, applica la chiave pubblica del mittente e verifica l'autenticitò. L'uso della chiave pubblica per le firme digitali ha il problema per cui la cifratura e la decifratura risultano essere complicati e onerosi ed è per questo che viene usato un approccio più efficiente che consiste nll'introduzioni delle funzioni hash nella firma. In pratica, il mittente non firma l'intero documento ma soltanto una sua impronta ottenuta applicando al messaggio una ufunzione hash che genera una sequenza di lunghezza minore. Se si combinano le due cose, un mittente invia un messaggio, si calcola con la funzione hash il digst $H(m)$ e lo firma con la chiave privata, in modo che il destinatario riceva il messaggio originario e il digest criptato. A questo punto, il destinatario prende il messaggio, ci applica la funzione hash, calcola $H(m)$, usa la chiave pubblica del mittente per decifrare la firma e confronta se questi due digest sono uguali.

Crittografia a chiave simmetrica

La crittografia a chiave simmetrice si basa sull'esistenza di una chiave che cambia a seconda del meccanismo usato per la cifratura. Esistono più tipologie di algoritmi:

- Cifrario di cesate: si basa sulla sostituzione di ogni letta del messaggio ordinale con una lettera sfasata alla prima di k posizione. La chiave è k;
- Cifrario monoalfabetico: si sostituisce ogni lettera del messaggio originale con una lettera in uno schema regolare. La chiave è il cifrario;
- Metodo a più associazioni: si intercambiando cifrari senza un pattern preciso e la chiave corrisponde agli n cifrari e al pattern usato per la cifratura;
- Cifrari a blocchi: si divide il messaggio da cifrare in blocchi di k bit ed ogni blocco viene cifrato in maniera indipendente. I diversi blocchi vengono riassemblati e mescolati alternandone così l'ordine per poi ripetere questa procedura più volte.
- Cifrari a blocchi concatenati: ogni messagio, prima di cifrarlo viene compinato tramite uno XOR tra la sequenza di bit in ingresso e il codice i-esimo utilizzato per cifrare il blocco precedente. Ogni codice cifrato, dipende da tutta la sequenza in ingresso. Ne è un esempio il DES e AES per maggiore sicurezza.

Crittografia a chiave pubblica

La crittografia a chiave pubblica permette di usare chiavi diverse e quindi non devon esere scambiate. L'idea è quella di non avere una chiave comune segreta, ma due chiavi per ciasuna rete: K^+ pubblica e K^- privata. Conoscere la chiave pubblica non da informazioni sulla chiave privata anche se queste siano correlate. Applicando la chiave pubblica e poi la privata di ottiente il messaggio. L'algoritmo principale è RSA che utilizza nozioni di algebra per calcolare la chiave pubblica e privata per un messaggio: (n,e) è la chiave pubblica e (n,d) chiave privata. L'algoirtmo è il seguente:

Per generare le chiavi vengono eseguiti i seguenti passi:

1. Vengono scelti due numeri primi p e q dell'ordine di 1024 bit e maggiore è il loro valore più sara sicura RSA, ma sarà più complicata la cifratura e la decifratura;
2. Viene calcolato $n = pq$ e $z = (p-1)(q-1)$
3. Viene scelto un numero e minore di n, diverso da 1 e che non abbiamo divisori comunic con z;
4. Viene scelto un numero d tale che $ed-1$ sia divisibile per z
5. La coppia (n,e) è la chiave pubblica e la coppia (n,d) è la chiave privata.

Ora per cifrare un messaggio m vuol dire:

1. Calcolare $x = m^e \bmod n$ ossia il messaggio cifrato;
2. Calcolare $m = c^d \bmod n$, il messaggio decifrato, utilizzando la chiave segreta.

Firewall

Il firewall è una combinazione di hardware e software che separa una rete privata da Internet e permette di controllare il traffico tra la rete e le risorse interne. Il firewall ha l'obiettivo di impedire gli attacchi SYN flooding, cioè un attacco di tipo DOS nel quale un intruso invia una serie di richieste SYN-TCP riempendo la struttura dati del server, prevenire modifica dei dati interni alla rete, impedire gli accessi dall'esterno della rete. Si possono dividere in tre categrie:

- Firewall stateless che eseguono azioni di filtraggio di pacchetti. Si analizza il traffico in entrata e uscita e si decide se farlo passare o meno in base ai cambi del segmento/frame. Per effetuare i controlli del segmento/frame si implementano delle regole nella lista di controllo di accesso: se un pacchetto non rispetta determinate regole non viene fatto passare;

- Firewall con stato che filtrano i pacchetti: si tiene traccia della connessioni TCP in modo da vedere se determinati pacchetti hanno senso in quel momento. In questo caso le liste di controllo di accesso hanno un controllo sullo stato della connessione in quel momento;

- Firewall di tipo applicativo gateway: questi firewall effettuano il filtraggio dei pacchetti unito ad un gateway a livello applicativo che prende decisione in base ai dati applicativi. Ci sono delle limitazioni dovute ai nodi che possono cambiere il proprio indirizzo IP.

IPsec

I servizi offerti da IPsec sono la cifratura a livello di datagramma, l'integrità dei dati, l'autenticazione dell'orgine del datagramma, evitare attacchi di replay e confidenzialità dei dati. Esistono due principali protocolli:

- AH: fornisce solo l'autenticazione della sorgente e l'integrità dei dati;

- ESP: fornisce autenticazione della sorgente,integrità dei dati e riservatezza.;

IPsec ha due modalità di funzionamento: transport in cui solo il paylod del datagramma è cifrato e autenticato e il tunnel in cui l'intero datagramma viene cifrato e autenticato e questo viene incapsulato in un nuovo datagramma con un nuovo indirizzo IP, inviato a destinazione. Per inviare i datagrammi, l'host sorgente e destinatario creano un canale logico a livello di rete detto associazione di sicurezza. Essendo unidirezionali, se i due host vogliono scambiarsi datagrammi in modo sicuro devono esistere due associazioni di sicurezza. Le entità che si scambiano traffico devono mantenere le informazioni sulle SA(security autority) e per garantire la comunicazione sicura si ha bisogno di una coppia di SA per ogni coppia di entità che vogliono comunicare tra loro. Tutte queste informazioni vengono salvate nel loro database di associazione di sicurezza SAD. Infatti, servono ogni volta che si deve scambiare traffico poiché ogni pacchetto da inviare da un router. Quindi un intruso non riesce ad accedere al conenuto dei pacchetti poiché sono cifrati, non riesce a vedere le sorgenti e le destinazioni poiché queste informazioni fanno parte del payload che viene cifrato, non può usare l'indirizzo IP come indirizzo IP sorgente per sostituirsi ad esso poiché la cifratura usa una chiave nota solo al router e non può fare reply attack per i datagrammi vengono numerati e la numerazione è protetta con l'integrità.

Esercizio RSA

- Calcola la chiave pubblica (n, e) e privata (n, d) dati $p = 7, q = 13, e = 11$

$$\begin{aligned} n &= p \cdot q = 91 \\ m &= (p-1) \cdot (q-1) = 72 \\ \text{MCD}(e.m) &= 1 \longrightarrow \text{Vera} \\ d \cdot e &= m \cdot k + 1 \rightarrow d = \frac{(m \cdot k + 1)}{e} \end{aligned}$$

- Date le seguenti chiavi:
  - Chiave pubblics $(5, 35)$
  - Chiave privata $(5, 35)$

  Volendo trasmettere $m = 2$, cifrare e decifrare m utilizzando RSA.

$$\begin{aligned} \text{codifica} &\rightarrow m_{\text{cifrato}} = m^e \bmod n \\ \text{decodifica} &\rightarrow m_{\text{chiaro}} = \text{cod}^d \bmod n \end{aligned}$$