Descrivere l'algoritmo CSMA 0-Persistent (non persistente)

Il CSMA 0-persistent (non persistente) è un algoritmo di accesso al mezzo condiviso che prevede che:

1. quando una stazione ha delle trame da trasmettere, ascolta il canale per verificare se c'è una collisione in corso
2. se il canale è libero trasmette, altrimenti rimanda la trasmissione ad un nuovo istante scelto in modo casuale
3. se si verifica una collisione, la stazione aspetta un tempo casuale e poi ritrasmette.
4. il procedimento si ripete fino a quando la trama non viene trasmessa con successo

Il CSMA 0-persistent permette di desincronizzare la trasmissione ma introduce maggiori ritardi.

Descrivere l'algoritmo CSMA 1-Persistent

Il CSMA 1-persistent è un algoritmo di accesso al mezzo condiviso che prevede che quando una stazione ha delle trame da trasmettere, ascolta il canale per verificare se c'è una trasmissione in corso

1. se il canale è libero trasmette, altrimenti aspetta che il canale si liberi e poi trasmette.
2. se si verifica una collisione, la stazione aspetta un tempo casuale e poi ritrasmette.
3. il procedimento si ripete fino a che la trama non viene trasmessa con successo.

Si descriva l'algoritmo CSMA P-Persistent

Il CSMA p-persistent è un algoritmo di accesso al mezzo condiviso che prevede che quando una stazione ha delle trame da trasmettere, ascolta il canale per verificare se c'è una trasmissione in corso.

1. se il canale è libero trasmette con una probabilità p.
2. se la stazione ha deciso di non inviare, attende un intervallo di tempo e trasmette con probabilità 1-p
3. se il canale è occupato, attende un intervallo di tempo e poi ascolta il canale. Se si verifica una collisione, la stazione aspetta un tempo casuale e poi ritrasmette.

4. il procedimento si ripete fino a che la trama non viene trasmessa con successo

Il CSMA p-persistent diminuisce i ritardi rispetto alla variante non-persistent.

Si illustri la variante del CSMA chiamata CSMA-CA usata nelle WLAN

CSMA-CA è un algoritmo di accesso al mezzo condiviso che prevede che quando una stazione ha delle trame da trasmettere, ascolta il canale per verificare se c'è una trasmissione in corso.

1. se il canale è libero, continua ad ascoltare il canale per un intervallo pari a DIFS (slot temporale più piccolo + 2 slot temporali). Se il canale è ancora libero, la stazione trasmette la trama.

2. se il canale è occupato, fin da subito o durante il DIFS, allora continua ad ascoltare il canale fino a quando non si libera

3. quando il canale si libera, la stazione ascolta per un intervallo pari a DIFS. Se il canale torna ad essere occupato, allora si torna al punto 2.

4. se il canale rimane libero per un DIFS, la stazione estrae un numero casuale uniformemente distribuito tra [0, CW-1] (contention window). Fintantoché il canale rimane libero, la stazione decrementa il contatore di backoff (numero di slot che deve attendere prima di trasmettere).

   (a) Se il contatore arriva a 0 la stazione trasmette.

   (b) Se il canale torna ad essere occupato prima che il contatore arrivi a 0, congela il contatore e si torna al punto, ma al punto 4 non si deve estrarre un nuovo contatore, ma si userà il contatore congelato. Se c'è collisione si estrae un tempo casuale e si inizia il processo di trasmissione in cui si raddoppia il CW.

Tra le stazioni che generano una trama mentre il canale è occupato, la stazione con il numero di SIFS più piccolo sarà la prima a trasmettere.

Si descriva, ad esempio in pseudo-codice, corredata da commenti, l'algoritmo CSMA nella sua variante Collision detection (CSMA-CD), indicando il motivo che ha portato all'introduzione di tale variante

Il CSMA-CD è un algoritmo di accesso al mezzo condiviso che prevede che quando una stazione ha delle trame da trasmettere, ascolta il canale per verificare se c'è una trasmissione in corso.

1. se il canale è libero trasmette, altrimenti aspetta che il canale si liberi e poi trasmette

2. se si verifica una collisione, la stazione interrompe la trasmissione, invia un segnale di disturbo (jamming signal) alle altre stazioni per avvisarle che si è verificato una collisione, e aspetta un tempo casuale e poi ritrasmette

In questo modo non si spreca tempo a trasmettere trame già corrotte.

L'header IP contiene un campo chiamato "Time to Live" (TTL), si spieghi come viene utilizzato tale campo e perché è stato introdotto

Il campo Time To leave (8 bit) specifica un valore inizializzato dalla sorgente che viene decrementato da ogni router attraversato dal datagramma. Se il valore raggiunge lo zero, il datagramma viene scartato e viene inviato un messaggio di errore alla sorgente. Questo meccanismo impedisce ai datagrammi di rimanere bloccati in un ciclo di routing infinito.

Si descriva la fase di chiusura della connessione TCP indicando i messaggi scambiati e i principali campi dell'header utilizzati

Dato che la connessione TCP è bidirezionale, la chiusura della connessione deve avvenire in entrambe le direzioni.

1. la stazione A che non ha più dati da trasmettere e decide di chiudere la connessione invia un segmento FIN, che è un segmento con il campo FIN posto a 1 e il campo dati vuoto.

2. la stazione B riceve il segmento FIN, invia un ACK e indica all'applicazione che la comunicazione è stata chiusa nella direzione entrante

Se questa procedura avviene solo in una direzione (half close), nell'altra direzione il trasferimento dati può continuare (gli ACK non sono considerati come traffico originato ma come risposta al traffico). Per chiudere completamente la connessione, la procedura di half close deve avvenire anche nell'altra direzione.

In relazione al livello di Trasporto, si spieghi cosa sono le "Porte Note" ed il motivo per cui sono state introdotte

Una porta è un codice identificativo (16 bit) utilizzato per identificare una determinata applicazione. Nell'header TCP i campi source port e destination port specificano l'indirizzo della porta sorgente e quello della porta di destinazione. Le porte possono essere statiche o dinamiche

- le porte statiche, dette porte ben note, sono identificativi che vengono associati ad applicazioni largamente utilizzate o definite dallo standard. Le porte statiche sono tutte quelle porte comprese tra 0 e 1023.

I numeri di queste porte vengono assegnati dalla IANA (Internet Assigned Numbers Authority). Grazie a questa standardizzazione il client non deve specificare la porta quando vuole accedere a uno di questi servizi standard. In questo modo un client che vuole accedere a un server HTTP sa a priori che deve collegarsi alla porta TCP numero 80.

- le porte dinamiche sono identificativi che vengono assegnati direttamente dal sistema operativo al momento dell'apertura della connessione tra host.

Per consentire il risparmio di energia nelle WLAN le stazioni usano il "Network Allocation Vector": si spieghi cos'è e come viene utilizzato

Il NAV, nello standard 820.11 per le WLAN, è una funzione software che fornisce una tecnica di ascolto virtuale nel canale di trasmissione. Dato che la maggior parte delle trame 802.11 contengono anche un campo che indica la lunghezza della trama stessa, i nodi che la percepiscono possono impostare il NAV al tempo in cui prevedono che il mezzo verrà liberato. Se il NAV > 0, il mezzo è considerato occupato e le stazioni non trasmettono. Non dovendo rimanere in ascolto costante le WLAN possono risparmiare energia.

In riferimento al livello di Rete si spieghi, anche attraverso un esempio, cos'è il NAT, spiegando perché tale funzionalità è stata introdotta

Il NAT (network address translation) permette agli host di una sottorete con indirizzi privati di inviare e ricevere pacchetti attraverso Internet. Al router di bordo che si trova tra la rete ad indirizzamento privato e la rete ad indirizzamento pubblico, viene assegnato un indirizzo pubblico, in questo modo il route rdi bordo viene visto come un host con indirizzo IP dal mondo esterno (router abilitato al NAT).

Il router abilitato al NAT sostituisce l'indirizzo sorgente di ogni pacchetto in uscita con il proprio indirizzo pubblico e sostituisce l'indirizzo di destinazione di ogni pacchetto in entrata con l'indirizzo privato dell'host corretto. Il router NAT mantiene al suo interno una tabella NAT che contiene la corrispondenza tra l'indirizzo privato sorgente e l'indirizzo pubblico della destinazione.

I record della tabella NAT vengono creati in modo dinamico ogni volta che il pacchetto diretto verso l'esterno attraversa il router e vengono cancellati con un meccanismo di time out. Per permettere a diversi host privati di connettersi contemporaneamente allo stesso host pubblico è necessario tradurre sia l'indirizzo IP sia l'indirizzo TCP/UDP, che è l'identificativo del processo coinvolto nella comunicazione (NAPT).

Si spieghi il funzionamento del protocollo ARP, spiegando il motivo per cui è stato introdotto

L'ARP (address resolution protocol) è un protocollo che fornisce una corrispondenza tra l'indirizzo IP e l'indirizzo MAC di un host. Ogni host possiede una tabella (cache ARP) che contiene le corrispondenze tra gli indirizzi IP e gli indirizzi MAC che sono stati richiesti. Quando un host vuole inviare un pacchetto ad un altro host

1. controlla la propria cache ARP, per verificare se possiede già la corrispondenza indirizzo IP - indirizzo MAC
2. se non è presente invia un messaggio ARP in broadcast a tutti gli host della rete, contenente l'indirizzo IP della destinazione
3. l'host che ha quell'IP invia un messaggio di risposta alla sorgente contenente il proprio indirizzo MAC, dopodiché aggiorna la propria cache ARP
4. se la destinazione non appartiene a quella rete, l'host invia un messaggio ARP per ottenere l'indirizzo MAC del router di default, il cui indirizzo IP è fornito dal protocollo DHCP.

L'header del protocollo IPV6 contiene il campo "Extension Header", si spieghi come viene utilizzato e perchè è stato introdotto

Il campo next header è lungo 8 bit e specifica il tipo di informazione che segue l'header di base: se il datagramma include un extension header, il campo specifica il tipo di extension header, se invece il datagramma non include un extension header, il campo specifica il protocollo del payload. Gli extension header sono degli header, di dimensione variabile, che si trovano all'interno del datagramma tra l'header principale e l'header del livello di trasporto, e forniscono informazioni relative al routing, alla frammentazione, all'autenticazione e alla sicurezza. I router possono ispezionare rapidamente l'header iniziale e tralasciare le informazioni di cui non hanno bisogno.

L'header del protocollo UDP contiene solo 4 campi: Source Port, Destination Port, Length e Checksum, si spieghi a cosa servono

il campo source port (16 bit) specifica il processo sorgente, il campo destination port (16 bit) specifica il processo destinazione, il campo length (16 bit) specifica la lunghezza totale, espressa in byte, del datagramma, compreso l'header UDP, e il campo checksum (16 bit) viene usato per sapere se il datagramma corrente contiene errori nel campo dati.

Si dia una definizione di Periodo di Vulnerabilità per una rete ad accesso multiplo con mezzo condiviso

Il periodo di vulnerabilità è l'intervallo di tempo in cui la trama può subire collisioni che invalidano la trasmissione. Se T è il tempo di trama e t_0 è l'inizio della trasmissione da parte di una sorgente, il periodo di vulnerabilità è pari al doppio della trama. Nel momento in cui inizia a trasmettere (t_0), nessun'altra sorgente deve aver iniziato la trasmissione dopo l'istante di tempo $t_0 - T$ e nessun'altra sorgente deve iniziare la trasmissione fino a $t_0 + T$.

Si spieghi attraverso un esempio come viene utilizzato il campo "Fragment Offset" dell'header IP

Il protocollo IP usa 3 campi dell'header IP per riassemblare i frammenti: il campo identification, il campo fragment offset e il flag more fragment. Il campo fragment offset è lungo 13 bit e specifica l'offset di un frammento relativamente all'inizio del datagramma IP originale. Il campo fragment offset viene misurato in blocchi di 8 byte.

- se il frammento ha l'offset $\neq 0$ e il flag MF $= 0$, allora è l'ultimo frammento
- se il frammento ha l'offset $= 0$ e il flag MF $= 1$, allora è il primo frammento
- se il frammento ha l'offset $\neq 0$ e il flag MF $= 1$, allora è un frammento intermedio

Ad esempio, un datagramma di 3999 byte, se viene trasferito in una rete con MTU = 1400 byte, verrà diviso in 3 frammenti: il primo con offset = 0, il secondo con offset = $\frac{1400}{8} = 175$ e l'ultimo con offset $\frac{2800}{8} = 350$.

Si dia la definizione di Dominio di Collisione e Dominio di Broadcast

Il dominio di broadcast, chiamato anche segmento data-link, è una porzione di rete in cui se una stazione trasmette un frame all'indirizzo broadcast, tutte le altre stazioni ricevono il frame. Il dominio di collisione è una porzione di rete in cui se 2 stazioni trasmettono contemporaneamente, si verifica una collisione. Le stazioni che appartengono alla stessa rete di livello 2 condividono lo stesso dominio di broadcast, e gli apparati che estendono le LAN possono influire soltanto sul dominio di collisione.

Dare una definizione di indirizzo privato ed indirizzo pubblico spiegando come vengono utilizzate le due diverse tipologie di indirizzo

Gli **indirizzi IP pubblici** identificano un host nella rete Internet e sono univoci. Gli indirizzi IP pubblici sono forniti dagli ISP quando un host stabilisce una connessione. Non è possibile avere 2 host connessi a Internet con lo stesso indirizzo IP.

Gli **indirizzi IP privati** identificano un host in una rete locale e sono univoci all'interno della stessa rete. Gli indirizzi privati non vengono usati dai router per l'instradamento dei pacchetti in Internet ma servono per la comunicazione tra gli host all'interno della stessa rete. Quando un host di una LAN, che utilizza un indirizzo privato, deve collegarsi ad Internet, dove è richiesto un indirizzo IP pubblico, ricorre al NAT. Il NAT permette di mappare più indirizzi privati su un solo indirizzo pubblico visibile all'esterno della rete locale e utilizzabile per accedere ad Internet.

Si spieghi l'utilizzo dei quattro principali indirizzi IP speciali

Gli indirizzi speciali sono indirizzi IP che non possono essere assegnati agli host e sono:

- l'indirizzo di rete è un indirizzo in cui i bit del suffisso sono posti a 0 e indica una rete
- l'indirizzo di directed broadcast è un indirizzo in cui i bit del suffisso sono posti a 1. Quando un pacchetto con indirizzo di broadcast diretto raggiunge la rete specificata, viene consegnato a tutti gli host di quella rete
- l'indirizzo di limited broadcast è un indirizzo in cui tutti i bit sono posti a 1. Il pacchetto con indirizzo di broadcast limitato viene inviato a tutti gli host che fanno parte della rete a cui appartiene l'host che ha inviato il pacchetto
- l'indirizzo "questo host" è un indirizzo in cui tutti i bit sono posti a 0 e viene usato durante lo startup quando l'host non ha ancora un indirizzo IP corretto
- l'indirizzo di loopback (127.0.0.0) è un indirizzo usato per testare le applicazioni di rete. Il programmatore fa girare 2 programmi sullo stesso host e comunicano usando questo indirizzo. La comunicazione tra i programmi avviene attraverso lo stack protocollare di rete.

Si spieghi cosa si intende, quando si parla di funzionalità di Livello 2, per Framing e si descriva una delle possibili tecniche con un esempio

Il framing è una funzione che rende distinguibile una trama dall'altra attraverso l'utilizzo di certi codici all'inizio e alla fine della trama, che fungono da delimitatori. per implementare il framing è possibile marcare l'inizio e la fine di ogni trama con il metodo del character count o del bit stuffing.

- il metodo del character count consiste nell'indicare nell'header del frame il numero di caratteri del frame
- il metodo del bit stuffing consiste nell'inserire all'inizio e alla fine del frame uno speciale pattern di bit 011111110, chiamato byte di flag. Per evitare di confondere una trama con un flag, la sorgente aggiunge uno 0 se incontra 5 bit di 1 consecutivi all'interno della trama.

Ad esempio, per delimitare i frame in questa sequenza di bit
011011110101
scriviamo
011111110 0110101 **011111110** 1110101 **011111110**

Si descriva la fase di instaurazione della connessione del protocollo TCP, indicando i messaggi scambiati e i campi dell'header coinvolti durante tale fase

Il TCP è un protocollo orientato alla connessione, cioè prima di iniziare a trasferire i dati instaura una connessione bidirezionale tra 2 host. La procedura utilizzata per instaurare una connessione TCP tra 2 host è chiamata three-way-handshake. I 2 host si scambiano 3 messaggi:

1. il client invia un segmento SYN al server. Il segmento SYN è una header TCP in cui il flag SYN è posto a 1 e il campo sequence number contiene l'initial sequence number del client, che è casuale
2. il server invia un segmento SYN-ACK al client. Il segmento SYN-ACK è un header TCP in cui i flag SYN e ACK sono posti a 1, il campo sequence number contiene l'initial sequence number del server, che è casuale, e il campo acknowledgment number è uguale al sequence number del client + 1
3. il client invia un segmento ACK al server. Il segmento ACK è un header TCP in cui il flag ACK è posto a uno, il campo sequence number è uguale al sequence number del client + 1 e il campo acknowledgment number è uguale al sequence number del server + 1

Una volta che la connessione è stata instaurata, il client può iniziare a inviare i segmenti del messaggio dell'applicazione.

L'header IP contiene un campo chiamato "IDENTIFICATION": si spieghi cosa contiene e come viene utilizzato

Il campo identification è un numero di 16 bit (di solito sequenziale) assegnato al datagramma che viene utilizzato per ricomporre un datagramma nel caso in cui venga frammentato. Il campo identification identifica i frammenti che fanno parte del datagramma originale: tutti i frammenti hanno lo stesso valore del datagramma originale.

In riferimento al livello Data-Link nelle reti wireless si spieghi il problema del terminale nascosto e di quello esposto. Si discuta una possibile soluzione a tali problemi

Il problema del terminale nascosto è una situazione che si verifica quando 2 stazioni che non hanno visibilità diretta tra loro provano ad accedere al canale di comunicazione nello stesso istante.

1. la stazione A ascolta il canale, lo percepisce libero e trasmette
2. la stazione B ascolta il canale, non rileva la trasmissione di A perché è fuori range, e invia una trama
3. nell'access point si verifica una collisione e le stazioni A e B non la percepiscono e quindi non ritrasmettono le trame

Il problema del terminale esposto è una situazione che si verifica quando una stazione non trasmette perché percepisce il canale occupato nonostante la trasmissione in corso stia avvenendo tra altre 2 stazioni, di cui una si trova nelle vicinanze.

Per risolvere questi problemi si utilizzano le trame RTS/CTS.

1. la stazione A, dopo aver percepito il canale libero per un intervallo DIFS, invia una trama RTS (request to send), contenente la lunghezza della trama da trasmettere, all'access point
2. l'access point include questa informazione nella trama CTS (clear to send) e la invia alla stazione A e alla stazione B
3. da quel momento in poi la stazione B si astiene dal trasmettere per il tempo indicato nel campo duration presente nella trama CTS. Durante questo periodo vengono spenti i circuiti legati alla trasmissione e alla ricezione.

Si descriva come TCP calcola l'RTT e il Retrasmission Timeout (RTO)

L'RTT (round trip time) è l'intervallo di tempo tra l'invio di un segmento e la ricezione del riscontro di quel segmento. Dato che l'RTT cambia nel

tempo, consideriamo il valore medio dell'RTT, chiamato SRTT (smoothed RTT). Calcoliamo SRTT nel seguente modo:

$$\text{SRTT}_{\text{attuale}} = (\alpha \cdot \text{SRTT}_{\text{precedente}}) + ((1 - \alpha) \cdot \text{RTT}_{\text{istantaneo}})$$

dove

- $\text{RTT}_{\text{istantaneo}}$ è la misura di RTT sull'ultimo segmento
- $\text{SRTT}_{\text{precedente}}$ è la stima precedente del valore medio di RTT
- $\text{SRTT}_{\text{attuale}}$ è la stima attuale del valore medio di RTT
- α è il coefficiente di peso che ha un valore compreso tra 0 e 1

L'RTO (retrasmission time out) è il tempo entro il quale la sorgente si aspetta di ricevere il riscontro (ack); se il riscontro non arriva, la sorgente procede alla trasmissione. Il calcolo dell'RTO si basa sulla misura del RTT e viene calcolato dinamicamente di volta in volta durante la fase di instaurazione della connessione e durante la trasmissione dei dati. Calcoliamo l'RTO nel seguente modo:

$$RTO = \beta \cdot \text{SRTT}$$

dove β è il delay variance factor e tipicamente vale 2. Di conseguenza, la sorgente attende fino a 2 volte l'RTT medio prima di considerare il segmento perso e ritrasmetterlo. In caso di ritrasmissione, l'RTO per quel segmento viene ricalcolato in base ad un processo di exponential backoff: se è scaduto l'RTO, probabilmente c'è congestione, quindi è meglio aumentare l'RTO per quel segmento calcolando $\text{RTOretransmission} = 2 \cdot \text{RTO}$.

Le implementazioni attuali del TCP utilizzano algoritmi più evoluti per il calcolo di RTT e RTO ma il principio dell'adattamento rispetto le condizioni della rete rimane lo stesso.

L'header TCP contiene il campo "Sequence Number": si pieghi a cosa serve e come viene utilizzato

Il campo sequence number (32 bit) specifica il numero di sequenza (sequence number) del primo byte del payload (campo dati). A livello data link, la tecnologia permette di trasmettere pacchetti di dimensione massima parti a MTU (maximum transmission unit). Il protocollo TCP legge il valore MTU e frammenta il messaggio che arriva dall'applicazione in segmenti di dimensione massima pari a MTU meno l'overhead dei vari protocolli. Il TCP utilizza il campo sequence number per poter ricostruire l'ordine dei segmenti ricevuti rispetto al messaggio originale.

L'initial sequence number (ISN) viene inserito come parametro nel primo segmento di SYN inviato dalla stazione che vuole aprire la connessione. L'ISN viene usato per ordinare i dati ricevuti secondo una sequenza di byte numerati in modo progressivo a partire dal valore dell'ISN.

Si spieghi brevemente la funzionalità di frammentazione dei pacchetti IP, incluse le motivazioni e gli apparati che effettuano frammentazione/deframmentazione

Se la dimensione di un datagramma che vogliamo inviare è maggiore della MTU della rete di destinazione o delle reti intermedie che deve attraversare per arrivare alla destinazione, il router divide il datagramma in datagrammi più piccoli, chiamati frammenti, e li invia in modo indipendente.

Il router usa il valore del MTU e della dimensione dell'header per calcolare al dimensione massima dei dati che possono essere inviati in ogni frammento e il numero di frammenti necessari. Il router crea i frammenti usando i campi dell'header originale per creare l'header del frammento, copia la porzione di dati dal datagramma originale al frammento e trasmette il risultato.

Il protocollo IP usa 3 campi dell'header IP per riassemblare i frammenti: il campo identification, il campo fragment offset e il flag more fragment.

- il campo identification identifica i frammenti che fanno parte del datagramma originale
- Il campo fragment offset specifica l'offset di un frammento relativamente all'inizio del datagramma IP originale.
- il flag more fragment, in combinazione con il campo fragment offset, specifica si il frammento è il primo, l'ultimo o è intermedio.

Il riassemblaggio dei frammenti per ottenere il datagramma originale viene fatto a destinazione. Quando la destinazione riceve il primo frammento fa partire un timer: se la destinazione riceve tutti i frammenti prima dello scadere del timer riassembla i frammenti, altrimenti scarta tutti i frammenti.

Si descriva la modalità di framing dei livello Data-Link chiamata "Bit Stuffing" aiutandosi con un esempio numerico

il metodo del bit stuffing consiste nell'inserire all'inizio e alla fine del frame uno speciale pattern di bit 011111110, chiamato byte di flag. Per evitare di confondere una trama con un flag, la sorgente aggiunge uno 0 se incontra 5 bit di 1 consecutivi all'interno della trama. Ad esempio, per delimitare i frames in questa sequenza di bit
011011110101
scriviamo
011111110 0110101 **011111110** 1110101 **011111110**

Si spieghi il concetto di porta del Livello Trasporto

Una porta [...]

Si spieghi brevemente perché la Congestion Window (CWND) non è un parametro fisso ma varia continuamente nel tempo

La CWND è una finestra di trasmissione [...]

Si spieghi la differenza tra commutazione di circuito e commutazione di pacchetto

Nelle reti a commutazione di circuito, quando 2 host vogliono scambiarsi dati, viene stabilita una connessione dedicata ed esclusiva. Le risorse di rete lungo il collegamento sono riservate per l'intera durata della sessione e non vengono condivise con altri collegamenti. Le risorse non utilizzate rimangono inattive. La commutazione di circuito è ideale se gli utenti sono pochi e la quantità di dati da trasmettere è costante.

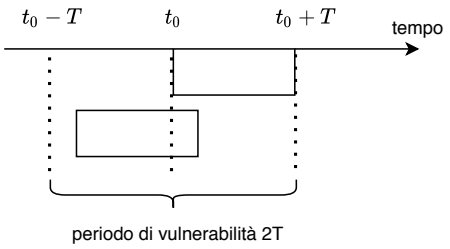
Nelle reti a commutazione di pacchetto, i dati scambiati tra 2 host sono suddivisi in pacchetti che vengono inviati individualmente e in sequenza, e condividono le risorse di rete a seconda della necessità. Se la richiesta di risorse eccede la quantità di risorse disponibili si crea congestione. La maggior parte dei router utilizza la trasmissione store and forward che prevede che il router invii il pacchetto sul collegamento in uscita solo quando l'ha ricevuto completamente. La commutazione di pacchetto è più semplice della commutazione di circuito ma richiede protocolli per il trasferimento affidabile dei dati e per il controllo della congestione. La commutazione è ideale se gli utenti della rete sono molti e la quantità di dati da trasmettere non è costante.

Come viene aggiornato il valore medio dell'RTT (SRTT) durante una connessione?

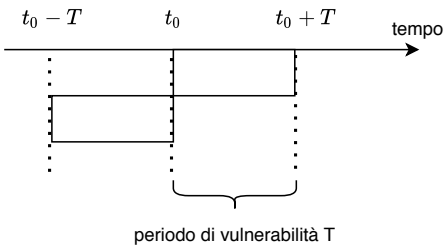
L'RTT (round trip time) [...]

Definizione di periodo di vulnerabilità e qual è il periodo di vulnerabilità per il protocollo ALOHA (con disegno)

Il periodo di vulnerabilità [...].
Se T è il tempo di trama, il periodo di vulnerabilità del protocollo ALOHA puro è 2T



Il periodo di vulnerabilità del protocollo slotted ALOHA è T.



Cosa succede quando un host si connette ad una rete e ha bisogno di ricevere un indirizzo IP

Il DHCP (dynamic host configuration protocol) è un protocollo che permette l'assegnamento automatico dell'indirizzo IP agli host ogni volta che si connettono ad una rete.

1. quando un host si connette ad una rete, invia il messaggio DHCP DISCOVER in broadcast per ottenere un indirizzo IP
2. i server DHCP inviano un messaggio DHCP OFFER che contiene un indirizzo IP e altri parametri di configurazione
3. l'ost sceglie uno di questi indirizzi IP e invia un messaggio DHCP REQUEST in broadcast indicando quale server ha scelto
4. il server selezionato conferma l'assegnazione dell'indirizzo inviando un messaggio DHCP ACK all'host

Il server DHCP rilascia un indirizzo IP per un periodo di tempo limitato chiamato lease: quando il periodo di lease scade, l'host invia una nuova richiesta DHCP per chiedere al server un estensione del periodo di lease. Se il server non approva la richiesta d'estensione, l'host deve richiedere un nuovo indirizzo IP.

Perché il congestion windows non è fissa ma cambia nel tempo?

La congestion windows è una finestra di trasmissione che varia dinamicamente dimensione per adattarsi alle situazioni di sovraccarico e reagire alla congestione. Esistono diversi algoritmi che regolano la dimensione della finestra, ad esempio lo slow start e il congestion avoidance. Con lo slow start l'evoluzione della CWND ha un andamento esponenziale mentre con il congestion avoidance l'evoluzione della CWND ha un andamento lineare.

In riferimento al livello di trasporto, l'header TCP contiene un campo denominato "Acknowledge number": si spieghi come viene utilizzato tale campo, anche attraverso un esempio di scambio tra 2 host

Il campo "Acknowledge number" è lungo 32 bit e indica il numero di sequenza (sequence number) del byte successivo del segmento TCP che l'host mittente si aspetta di ricevere. Questo campo ha significato solo se il flag ACK è posto a 1.

Supponiamo che l'host A abbia ricevuto tutti i byte numerati da 0 a 535 e che stia per mandare un segmento all'host B. L'host A è in attesa del byte 536 e dei successivi byte. Di conseguenza, l'host A scrive 536 nel campo ackowledge number del segmento che spedisce all'host B.

Si descriva brevemente un possibile schema di router, evidenziando le funzionalità delle diverse parti.

Il router esegue gli algoritmi e i protocolli di routing, e trasferisce i datagrammi dalla porta di input alla porta di output. Le porte di input ricevono il datagramma dalla rete e determinano a quale porta di output inviare il datagramma utilizzando le tabelle di inoltro. La struttura di commutazione inoltra il datagramma alla porta di output che li trasmette sulla rete. Le porte di output:

- svolgono funzioni di buffering, quando la velocità di arrivo dei datagrammi è superiore alla velocità di trasmissione
- svolgono funzione di scheduling per determinare l'ordine di trasmissione

Si descriva il problema del terminale nascosto "hidden terminal problem" nelle reti wireless LAN e la soluzione adottata nello standard 802.11

Il problema del terminale nascosto [...]