Reti

Stefano Cattonar

Settembre 2019

1 Domande

L'header del protocollo IP contiene un campo chiamato "Time to live" (TTL): si spieghi come viene utilizzato tale campo eperché è stato introdotto

Il campo "TTL" viene utilizzato per determinare quando un pacchetto deve essere scartato. Ad ogni accesso ad un apparato di rete questo campo viene decrementato e se raggiunge lo zero il pacchetto viene scartato. Questo campo diviene utile specialmente quando ci sono dei problemi sulla rete, come per esempio una sezione irraggiungibile causa guasti per evitare la congestione della rete con pacchetti che non possono arrivare a destinazione e che continuano a venire "rimbalzati" fra i vari apparati.

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

Per chiuder la connessione in uscita una stazione deve inviare un segmento di FIN all'altra, che risponderà con un ACK per confermare l'avvenuta ricezione del FIN. A questo punto la prima stazione risponderà con un altro ACK e chiuderà la connessione. Questa pratica si chiama "half close" perché chiude la connessione solo dalla stazione che ha inviato il FIN, ma l'invio di dati nel senso opposto può continuare(gli ACK non vengono considerati traffico generato). Per chiudere completamente la connessione il procedimento va fatto anche partendo dall'altra stazione.

Si descriva l'algoritmo CSMA nella sua variante Collision Detection (CSMA-CD), indicando il motivo che ha portato all'introduzione di tale variante.

L'algoritmo CSMA-CD è stato introdotto per le reti wireless in cui la condivisione del mezzo fisico è obbligatoria.Questa variante in caso di rilevamento di una collisione fa immediatamente terminare la connessione e quindi permette

di risparmiare tempo. L'algoritmo CSMA ja 3 varianti: persistent: 1)Ascolto il canale 2a)E' libero quindi trasmetto 2b)E' occupato, aspetto finchè non si libera quindi trasmetto Se c'è collisione aspetto un periodo casuale quindi ricomincio dal punto 1

non-persistent: 1)Ascolto il canale 2a)E' libero quindi trasmetto 2b)E' occupato, attendo un tempo casuale(strettamente maggiore del tempo di trasmissione di una trama) Se c'è collisione aspetto un periodo casuale quindi ricomincio dal punto 1

p-persistent: 1)Ascolto il canale 2)Se è libero decido di trasmettere con una probabilità p 3a)Se ho deciso di non trasmettere aspetto un intervallo di tempo poi si torna al punto 1 3b)Se ho trasmesso e c'è collisione aspetto un periodo causuale e torno al punto 1

Per consentire il risparmio di energia nelle Wireless LAN (WLAN), le stazioni utilizzano il cosiddetto "Network Allocation Vector" (NAV): si spieghi che cos'è il NAV e come viene utilizzato.

Il NAV è una tipologia di ascolto virtuale del canale di trasmissione nello standard 802.11 Si basa sul fatto che nella maggior parte delle trame che rispettano lo standard 802.11 ci sia la lunghezza delle stesse. I nodi che percepiscono le trame impostano il NAV = alla lunghezza delle trame. Se il NAV è ¿0 allora il canale è da considerarsi occupato.

In riferimento al livello di trasporto, si spieghi che cosa sono le "porte note" (Well Known Ports) e il motivo per cui sono state introdotte.

Le porte note sono le porte che vanno dalla porta 0 alla porta 1023 compresa e sono state introdotte per avere porte esclusive per protocolli conosciuti e utilizzati spesso come l'HTTP(porta 80)

In riferimento al livello di rete, si spieghi, anche attraverso un esempio, che cos'è il Network Address Translation (NAT), specificando per quale motivo tale funzionalità è stata introdotta

IL nat è stato introdotto perché la richiesta di indirizzi IP è cresciuta in modo esponenziale, e quindi sfruttando la struttura a multi reti di Internet si è potuto ovviare temporaneamente al problema, inventando gli indirizzi privati. Una sottorete ha un solo indirizzo privato e sarà compito del NAT dell'apparato di rete esterno Il nat mantiene in memoria un mapping tra l'indirizzo privato della sorgene e l'indirizzo pubblico della destinazione in questo modo Il nat in uscita sostituisce l'indirizzo privato con il proprio pubblico e in entrata leggendo

la tabella e l'indirizzo pubblico esterno può capire a che host all'interno della propria rete inviare i dati

Protocollo ARP: perché è stato introdotto?

Il protocollo ARP è stato introdotto perché se la comunicazione deve avvenire tra due host in reti diverse c'era bisogno di un modo per far arrivere ai router i dati senza cambiare l'indirizzo IP di destinazione, altrimenti l'informazione andrebbe persa. La soluzione è usare gli indirizzi MAC che vengono risolti dal protocollo ARP. ARP viene utilizzato specialemente in caso di connessioni ethernet e wireless(802.11) ma non è legato a una singola tecnologia e non è limitato a tradurre indirizzi MAC e IP, quindi la lunghezza del datagramma non è fissa.

ICMP

L'Internet Control message protocol è un protocollo complementare al protocollo IP che serve a definire eventuali errori o per ottenere informazioni. Per esempio il comando ping usa il protocollo ICMP. Per inviare un datagramma ICMP un router mette un header IP e mette nel payload il messaggio ICMP

1.1 Parlami del'IPv6 e dell'extension header

L'IPv6 ha uno spazio di indirizzamento di 128bit contro i 32 dell'ipv4. La lunghezza dell'header ipv6 è flessibile grazie all'introduzione dell'"extension header". In un header ci possono essere da 0 a N extension header. Ogni estension header fa riferimento a una funzionalità diversa. Sono stati implementati diversi exstension header, ma in futuro se ne potranno implementare altri. Sia l'header di base che l'estension header ha campo in cui definisce il contenuto dell'header successivo. L'exstension header può avere dimensioni variabili, quindi ogni header ha un campo con la propria dimensione.

Indirizzi IPv6 speciali

L'IPv6 implementa 3 indirizzi speciali:

- Unicast: Corrisponde a un singolo host e i dati vengono instradati sul cammino minimo verso quell'host.
- Multicast: Corrisponde a un gruppo di host che può cambiare nel tempo. I dati vengono spediti a tutti i membri del gruppo.
- Anycast: Corrisponde a un gruppo di host che condividono un prefisso. I dati vengono spediti a un singolo membro del gruppo.