Domande Reti di Telecomunicazione (appelli vecchi):

1. Differenze tra protocollo TCP e UDP
2. Struttura di una trama del protocollo HSLC, tipologie di trama e le loro funzioni evidenziando le maggiori differenze
3. Problematica della Silly Window
4. Procedure di First Retransmit e Fast Recovery del TCP (con esempi per ogni procedura)
5. L’importanza dei modelli protocollari quali TCP/IP e il modello ISO/OSI evidenziandone le differenze e le rispettive funzionalità
6. Il funzionamento delle tecnologie LAN di propria conoscenza attraverso la trattazione delle differenti topologie di reti, di alcune tecniche adotatte al livello fisico, protocolli di livello datalink e protocolli di accesso al mezzo.

Appelli recenti:

1. Tecniche di accesso al mezzo come CSMA, CSMA-CD e Aloha, con Vantaggi e Svantaggi
2. Descrivere le differenze dei protocolli Link State e Distance Vector, con gli algoritmi associati, evidenziandone vantaggi e svantaggi
3. Differenze tra i protocolli ARQ Stop and Wait, Go Back N e Selective Repeat
4. Problematica della Silly Window
5. Il controllo di flusso nel protocollo TCP
6. Come il protocollo TCP effettua il controllo di congestione, evidenziando con esempi, le differenze tra i meccanismi Slow Start e Congestion Avoidance
7. Descrizione del protocollo IPv4 evidenziando le funzionalità di rete supportate
8. Il modello ISO/OSI indicando livelli protocollari conosciuti e funzionalità associate ai livelli
9. Cosa cambia tra protocolli di accesso al mezzo centralizzati e protocolli di accesso al mezzo distribuiti
10. Vantaggi e svantaggi delle due tipologie MAC
11. TCP: come effettua il controllo di flusso, di errore e di congestione

[ Appelli vecchi ]

1. Differenze tra protocollo TCP e UDP

Cosa sono?

Sono due dei protocolli di rete più utilizzati per stabilire la modalità in cui debba avvenire la comunicazione tra il dispositivo dell’utente e il server remoto. Questi dividono i dati in pacchetti più piccoli per poi inviarli al destinatario identificato tramite indirizzo IP.

DIFFERENZE

Se il protocollo TCP è affidabile ma più lento, il protocollo UDP è più veloce, ma meno affidabile. Ciò significa che si prestano ad essere utilizzati per scopi diversi.

Ad esempio, uno dei vantaggi del protocollo TCP è la possibilità di interrompere e riprendere l'invio di file. Nel caso si utilizzasse il protocollo UDP per la stessa operazione, bisognerebbe invece ricominciare il processo interrotto da capo.

In caso di perdita del pacchetto, inoltre, il protocollo TCP si accorge subito della perdita, mentre il protocollo UDP ne realizza la scomparsa solo durante il controllo finale, agendo solo al termine. Il protocollo TCP invece, predispone tutto al fine di rinviare il pacchetto prima di procedere con l’invio dei successivi.

Usare il protocollo UDP ha però i suoi vantaggi: essendo più veloce, può essere utilizzato in tutti quei casi in cui la latenza deve essere ridotta al minimo e l'integrità dei file non è un problema.

1. Struttura di una trama del protocollo HDLC, tipologie di trama e le loro funzioni evidenziando le maggiori differenze

La trama è composta da tre parti principali: un header (dimensione di un otteto composto da flag, address e control, un campo information a lunghezza variabile e un trailer (composto da fcs e flag).

1. Problematica della Silly Window

La silly window syndrome (sindrome da finestra sciocca, abbreviata con SWS) è un problema legato alla cattiva implementazione del controllo di flusso a livello TCP. Un processo di scrittura molto lento da parte del mittente nel buffer di trasmissione (o di lettura da parte del ricevente) porta infatti all'invio di segmenti di dati molto piccoli, aumentando così il rapporto tra header e dati con un conseguente uso inefficiente del canale. La causa può essere ricondotta tanto al mittente quanto, nel secondo caso, al ricevente.

1. Procedure di First Retransmit e Fast Recovery del TCP (con esempi per ogni procedura)
2. L’importanza dei modelli protocollari quali TCP/IP e il modello ISO/OSI evidenziandone le differenze e le rispettive funzionalità

Sono uno dei fondamenti di Internet: senza i protocolli TCP/IP, l’azione quotidiana del navigare in rete non sarebbe concepibile. Tramite i protocolli (il termine comprende più raccolte di regole contemporaneamente), i pacchetti di dati vengono trasferiti nella Local Area Network (LAN) o Wide Area Network (WAN), quindi anche nel World Wide Web, ossia in Internet.

TCP (Transmission Control Protocol) / IP (Internet Protocol) è stato sviluppato dall’agenzia di progetto del Dipartimento della Difesa (DoD) . A differenza del modello OSI, è costituito da quattro livelli ciascuno con i propri protocolli. I protocolli Internet sono l’insieme di regole definite per la comunicazione sulla rete.

TCP/IP è considerato il modello di protocollo standard per il networking. TCP gestisce la trasmissione dei dati e IP gestisce gli indirizzi. La suite di protocolli TCP/IP ha una serie di protocolli che include TCP, UDP, ARP, DNS, HTTP, ICMP, ecc. È un modello robusto e flessibile. Il modello TCP/IP viene utilizzato principalmente per l’interconnessione di computer su Internet.

Il modello ISO/OSI è uno standard stabilito nel 1984 dall'International Organization for Standardization (ISO), il principale ente di standardizzazione internazionale. Tale modello stabilisce per l'architettura logica di rete, ovvero per le funzioni di comunicazione delle telecomunicazioni o di sistemi informatici, una struttura a strati composta da una pila di protocolli di comunicazione di rete suddivisa in 7 livelli, i quali insieme eseguono tutte le funzionalità della rete, seguendo un modello logico-gerarchico. A livello implementativo lo standard de facto affermatosi per architetture di rete a livelli è invece il TCP/IP.

Il modello OSI (Open System Interconnection) è stato introdotto da ISO (International Standard Organization) . Non è un protocollo ma un modello che si basa sul concetto di stratificazione. Ha un insieme verticale di livelli, ciascuno con funzioni diverse. Segue un approccio dal basso verso l’alto per trasferire i dati. È robusto e flessibile, ma non tangibile.

Ci sono alcune somiglianze e differenze tra di loro. Una delle principali differenze è che OSI è un modello concettuale che non viene praticamente utilizzato per la comunicazione, mentre TCP/IP viene utilizzato per stabilire una connessione e comunicare attraverso la rete. Il modello OSI pone principalmente l’accento sui servizi, interfacce e protocolli; fare una chiara distinzione tra questi concetti. Al contrario, il modello TCP non è in grado di descrivere distintamente questi concetti. Inoltre, il TCP/IP abilita solo la modalità di comunicazione senza connessione nel livello di rete ma entrambe le modalità (senza connessione e orientata alla connessione) nel livello di trasporto.

* TCP/IP è un modello client-server, cioè quando il client richiede un servizio, viene fornito dal server. Considerando che, OSI è un modello concettuale.
* TCP/IP è un protocollo standard utilizzato per ogni rete inclusa Internet, mentre OSI non è un protocollo ma un modello di riferimento utilizzato per comprendere e progettare l’architettura del sistema.
* TCP/IP è un modello a quattro livelli, mentre OSI ha sette livelli.
* TCP/IP segue l’approccio orizzontale. D’altra parte, il modello OSI supporta l’approccio verticale.
* TCP/IP è tangibile, mentre OSI non lo è.
* TCP/IP segue un approccio dall’alto verso il basso, mentre il modello OSI segue un approccio dal basso verso l’alto.

1. Il funzionamento delle tecnologie LAN di propria conoscenza attraverso la trattazione delle differenti topologie di reti, di alcune tecniche adottate al livello fisico, protocolli di livello datalink e protocolli di accesso al mezzo.

[ appelli recenti ]

1. Tecniche di accesso al mezzo come CSMA, CSMA-CD e Aloha, con Vantaggi e Svantaggi

Nelle telecomunicazioni CSMA indica una tecnica di trasmissione dati che si basa sull'accesso multiplo tramite rilevamento della portante. È un protocollo MAC (Media Access Control), quindi posto al secondo livello del modello ISO/OSI, nelle reti a bus per condividere tra più host la capacità della rete evitando che due dispositivi trasmettano contemporaneamente generando una collisione.

PRO: il CSMA rappresenta il protocollo più facilmente implementabile che consente l'accesso multiplo ad un canale di comunicazione condiviso tra più utenti ed allo stesso tempo anche molto efficiente/flessibile in funzione del numero di terminali cioè in termini di scalabilità della rete.

CONTRO: il trasmettitore, nel CSMA puro, non è in grado di rilevare i conflitti.

In telecomunicazioni CSMA/CD (acronimo inglese di Carrier Sense Multiple Access with Collision Detection, ovvero accesso multiplo tramite rilevamento della portante con rilevamento delle collisioni) è un protocollo di accesso multiplo, evoluzione del protocollo di livello MAC CSMA, nato per la risoluzione dei conflitti di trasmissione, ovvero collisioni, dovuti al CSMA puro, presenti in un certo dominio di collisione su reti locali cablate di tipo broadcast. In pratica, il protocollo CSMA/CD consente ad un computer di utilizzare la rete Ethernet soltanto se nessun altro elaboratore la sta già utilizzando.

PRO: integra la rilevazione degli errori mancante nel CSMA puro.

CONTRO: per evitare conflitti, aumentano i tempi di attesa.

In telecomunicazioni ALOHA è un protocollo di rete atto a garantire le funzionalità di accesso multiplo al mezzo di trasmissione dati condiviso tra più utenti. Il protocollo ALOHA viene utilizzato per connessioni di tipo broadcast, dove quindi il mezzo di trasmissione è condiviso da più di due punti di connessione (ovvero postazioni capaci di trasmettere e ricevere informazioni). Tale protocollo è di tipo multicast ed è utilizzato a livello MAC (Media Access Control, controllo di accesso al mezzo).

Questo protocollo deve garantire la correttezza e l'efficienza delle trasmissioni che, avvenendo appunto su reti condivise da molte postazioni, vanno incontro a numerose collisioni. Esistono principalmente tre tipi di ALOHA, quello cosiddetto "puro", quello "a slot" e quello "a trame e a slot".

PRO: prestazioni indipendenti dalla distanza delle stazioni.

CONTRO: poco efficiente, solitamente si preferiscono i CSMA.

1. Descrivere le differenze dei protocolli Link State e Distance Vector, con gli algoritmi associati, evidenziandone vantaggi e svantaggi
2. Differenze tra i protocolli ARQ Stop and Wait, Go Back N e Selective Repeat

* Stop and Wait - Il mittente invia il pacchetto e attende l'ACK (riconoscimento) del pacchetto. Una volta che l'ACK raggiunge il mittente, trasmette il pacchetto successivo in fila. Se l'ACK non viene ricevuto, ritrasmette di nuovo il pacchetto precedente.
* Torna indietro N - Il mittente invia N pacchetti che sono uguali alla dimensione della finestra. Una volta che l'intera finestra è stata inviata, il mittente attende quindi un ACK cumulativo per inviare più pacchetti. Sul lato ricevente, riceve solo i pacchetti in ordine e scarta i pacchetti fuori ordine. Come in caso di perdita di pacchetti, l'intera finestra verrebbe ritrasmessa.
* Ripetizione selettiva - Il mittente invia il pacchetto di dimensione finestra N e il destinatario riconosce tutti i pacchetti indipendentemente dal fatto che siano stati ricevuti in ordine o meno. In questo caso, il destinatario mantiene un buffer per contenere i pacchetti fuori ordine e li ordina. Il mittente ritrasmette selettivamente il pacchetto perso e sposta la finestra in avanti.

1. Problematica della Silly Window
2. Il controllo di flusso nel protocollo TCP
3. Come il protocollo TCP effettua il controllo di congestione, evidenziando con esempi, le differenze tra i meccanismi Slow Start e Congestion Avoidance
4. Descrizione del protocollo IPv4 evidenziando le funzionalità di rete supportate
5. Il modello ISO/OSI indicando livelli protocollari conosciuti e funzionalità associate ai livelli
6. Cosa cambia tra protocolli di accesso al mezzo centralizzati e protocolli di accesso al mezzo distribuiti
7. Vantaggi e svantaggi delle due tipologie MAC
8. TCP: come effettua il controllo di flusso, di errore e di congestione