Metodi di controllo dell’accesso:

* MAC 🡪 controllo di accesso al mezzo fisico, quando esso è comune ho n nodi, per far sì che essi accedano al mezzo fisico senza collisioni cioè se hanno la stessa frequenza collidono. Per gestire questo problema bisogna gestire i seguenti concetti:
  + Accesso basato sulla competizione: essi sono metodi probabilistici, CSMA/CD e CSMA/CA, il primo è a rilevazione della portante con rivelazione della collisione. Si fa avvenire la collisione e poi la si controlla
  + Si previene la collisione 🡪 CSMA/CA

CSMA/CD:

* Cavo comune in cui tutti possono trasmettere, quando un nodo vuole trasmettere va a testare rilevando la portante e controlla quindi se qualcuno sta trasmettendo, se nessuno trasmissione inizia a trasmettere. Se un altro nodo contemporaneamente fa la stessa cosa, il segnale si propaga e va a collidere. Questo segnale colliso è derivato dalla somma delle ampiezze, e le schede di rete capiscono che quando si superano le ampiezze massime. La prima di esse che riceve il segnale capisce che è un segnale colliso e quindi manda un segnale di “jamming” a tutte le schede di rete. Le due schede di rete che hanno generato la collisione smettono di trasmettere e vanno a generare un intervallo di tempo casuale di attesa, Algoritmo back off esponenziale binario è il nome dell’algoritmo per il tempo casuale. Il nodo per il quale è scaduto il tempo, testa il mezzo fisico e se non c’è portante ritrasmette il dato.

Algoritmo back off esponenziale binario si chiama così siccome il range nel quale esso viene generato, è casuale però man mano che ci sono collisioni consecutive lui va ad aumentare il range in maniera esponenziale. Inizia con 0-1, poi 0-3, poi 0-15 ecc Però non si va avanti all’infinito, si va avanti fino a 16 volte, se non va a buon fine bisogna resettare la scheda di rete o sostituirla.

CSMA/CA:

* Si ci basa sull’ultima trasmissione avvenuta, quindi ogni nodo che si collega alla rete, basandosi sull’ultima connessione avvenuta, attende un intervallo di tempo e diverso a tutti i nodi che si sono collegati 🡪 al fine di evitare la collisione. L’access point manda un dato per gestire la sincronizzazione dei nodi. Il concetto è che si basa su una prevenzione della collisione.

Accesso controllato invece, si parla di accesso deterministico 🡪 in un instante di tempo si sa chi sta trasmettendo. Per esempio nella rete Token Ring, il mezzo fisico comune (cioè l’anello) la connessione utilizza una unità dati che viene usato come token (esso può essere libero e occupato), e quindi se libero ogni nodo deve ricevere il token per far partire la propria connessione. Questo token fa il giro di tutto l’anello e viene letto dall’effettivo destinatario e ritorna al mittente il quale lo libera e poi lo passa al nodo successivo. Facendo così si evitano le collisioni.

La variante Token bus, utilizza una tecnologia bus, dalla quale viene ricavata una tipologia logica ad anello. Anche se bus vengono mandati i dati a livello logico al nodo successivo. Qui il token viene trattenuto dal nodo, e non aggancia il dato come per quello prima. L’unico vincolo è il limite di tempo sul passaggio dei dati, che se non vengono mandati in tempo allora si passa il token al nodo successivo a livello logico.

Frame: Data link

Nel protocollo Ethernet, utilizzato nella rete cablata, il frame start si chiama preambolo. Secondo la codifica Manchester, non esiste un clock di rete che scandisce il tempo quindi si utilizza queste transizioni. 0🡪 fronte di salita, 1 🡪 fronte di discesa. Per sincronizzare bene le due schede di rete si utilizza il preambolo di 8byte (1-0 alternati) i quali utilizzando una codifica Manchester, viene trasmessa un’onda quadra. I primi 62 bit sono 1-0 alternati e gli ultimi bit sono 11, qui l’onda quadra raddoppia la sua frequenza. Questo viene fatto per far capire alla scheda di rete che sono sincronizzati senno significa che non lo sono.

In seguito c’è la parte di indirizzamento, dove c’è prima il destinatario e poi il mittente, ovviamente indirizzi MAC, sono messi in questo ordine siccome quando la scheda di rete riceve il dato deve capire se è indirizzata a lei oppure no, quindi è la prima informazione che gli interessa. Come un po’ la lettera. Il mittente non serve perché in caso il secondo livello fa il controllo dell’errore ma non lo recupera.

Il controllo identifica la tipologia di invio dati, come broadcast.

Il tipo serve

Il data contiene i dati incapsulati, cioè in questo caso lo stato precedente del frame cioè il pacchetto.

Il trailer, nell’ethernet il campo del Error Detection utilizza l’algoritmo CRC a 32bit. Esso funziona al seguente modo: ogni bit diventa il coefficiente di grado n, dove n è il peso del bit, quindi si va creare un polinomio. Questo polinomio viene diviso in un polinomio generatore simmetrico che è noto a tutte le schede di rete. Questi calcoli sono fatti in HW, questo è fatto perché così è più veloce rispetto all’SO. Esso è di grado 32. Il polinomio associato e quello generatore si vanno a dividere, e il polinomio risultato va buttato via ma quello resto viene tenuto e può avere massimo grado 31. I coefficienti di esso sono effettivamente i bit che vengono impostati nel campo del Error Detection, il destinatario riceve il frame ed esso lo associa un polinomio il quale viene diviso di nuovo dal polinomio generatore che è uguale per tutte le schede di rete. Se il resto è uguale a 0 il dato è corretto senno esso è sbagliato, e che quindi nella trasmissione c’è un problema al bit. Nel caso ci fosse un problema il destinatario del dato, lui va a scartare il dato, il livello 4 poi si occupa della ritrasmissione del dato. Tramite poi un meccanismo di time-out esso viene ritrasmesso oppure no. Non è detto che un errore deve essere obbligatoriamente recuperato, basta pensare ad uno streaming, dove recuperare un dato nuoce alla trasmissione. UTP (non ritrasmette) e TCP (trasmette)

Il CRC è molto difficile che ci siano errori che si compensano, quindi è un controllo dell’errore sicuro 🡪 al 99.9%.

Livello 2 di indirizzamento:

* Gli indirizzi MAC, sono indirizzi che servono che il frame arrivi correttamente a destinazione. I vari mac cambiano ma gli indirizzi logici non cambiano. Questo viene fatto per mantenere l’effettiva destinazione del pacchetto.

ETHERNET:

C’è una dimensione minima del frame che è 64byte, io posso anche trasmettere meno di 64 byte e per raggiungere la dimensione minima bisogna usare i bit di padding poi tramite la length vengono poi scartati.

La lunghezza massima è 1500byte. Sui metodi di controllo di accesso al messo, quelli del modulo precedente, ricordo possono essere probabilistici e deterministici. Quest’ultimo funziona bene quando c’è il traffico elevato invece quelli probabilistico nel caso in un cui c’è un traffico basso, siccome nel traffico elevato possono avvenire più collisioni. Anche se ormai ricordo che con gli switch la questione delle collisioni è ormai inesistente.

Perché c’è una dimensione minima? 🡪 questo viene fatto siccome costringe il mittente e trasmettere per un certo tempo, al fine che il segnale di jamming possa essere ricevuto in modo che si riceva quindi ancora le schede di rete stanno ancora trasmettendo.

INDIRIZZO MAC:

Sono 6 byte quindi 48 bit, quindi con combinazione 2 alla 48-1.

C’è una parte che è di OUI, dove ogni azienda ha 3 byte univoci. Invece gli altri sono tutti numeri progressivi, così da rendere sicuramente univoca la scheda. Ogni azienda può produrne massimo 16milioni di schede. In caso un’azienda finisca un questo numero si richiede un altro numero siccome 16milioni di aziende disponibili. Ogni macchina che si collega ad una rete locale e identificabile in maniera univoca.

Cosa succede quando una scheda di rete riceve un frame? 🡪 Se il controllo dell’errore da esito corretto il pacchetto viene de capsulato e passato al livello 3. In caso viene scartato.

BROADCAST: Tutte le macchine ricevono il messaggio qui troviamo sia un IP di Broadcast che un Mac di broadcast.