NETWORK LAYER

Nel network layer viene gestito lo scambio dei dati. Vengono usati a livello di protocolli: IPv4 e IPv6. Gli indirizzi fisici, sono univoci alla scheda di rete, invece gli IP sono logici: quindi esso può cambiare. Questo può cambiare molto spesso, a volte succede che delle macchine anche se collegate alla stessa rete si possono collegare pure più mac.

Addressing end devices: sono indirizzi logici

Nella parte IP viene incapsulato il segmento e diventa un pacchetto. Il nat può cambiare, ed è quello che viene usato nell’IPv4.

CONNECTIONLESS:

I dati vengono inviati senza aver bisogno dell’uso della connessione. Esso si verifica nell’esempio semplice tra una telefonata e una lettera. Tipo nel telefono, serve instaurare una connessione, senno non posso trasmettere i dati.

Il dato viene inviato semplicemente nella lettera, basta inserirla nel box.

Nel livello 3 non c’è bisogno di avviare una connessione, L’IP è connectionless quindi non usa la connessione.

BEST EFFORT:

Non ci sono riconoscimenti, nell’IP i dati non vengono confermati e quindi non c’è la certezza che il dato sia arrivato a destinazione oppure no. Si chiama così siccome fa del suo meglio che i dati arrivino a destinazione, ma esso non è garantito. Questo servizio deve essere molto veloce quindi è comodo sia cosi, viene ridotto l’OVERHEAD, non aspettando dei riconoscimenti.

MEDIA INDEPENDENT:

Il frame è dipendente dal mezzo fisico, invece il pacchetto rimane sempre uguale quindi NON dipende dal mezzo fisico che attraversa.

Questo è UNRELIABLE quindi questi pacchetti non si occupa del riallineamento dei pacchetti, essi vengono rimessi in ordini dal livello di trasporto e non da quello IP.

Ogni rete ha la caratteristica della MTU (maximum transfer unit), questo significa che informazioni più grandi del MTU non possono essere inviate per intero, ma devono essere spezzate. Viene creato un minimo di latenza, cosa che nel IPv6 non esiste. Questo viene fatto per non monopolizzare la rete.

IPv4 PACKET HEADER CAMPI:

* Version: Contiene 4 bit per identificare che è ipv4
* La lunghezza della header è espressa in double word 🡪 5\*4 = 20 byte
* Lunghezza totale: Pay load 🡪 segmento incapsulato nel pacchetto (2 alla 16 - 1)
* Id: viene dato a ogni pacchetto inviato un numero progressivo identificativo (fondamentale per la ricostruzione della segmentazione dei pacchetti).
* Flag: DF ed MF esse sono legate al concetto del MTU, lunghezza massima trasferita (tipo Ethernet 🡪1500 bytes). DF : Don’t fragment 🡪 se messo a 1 non permette la frammentazione, nel caso fosse maggiore la quantità il dato viene scartato. Il more fragment è a 1 se c’è ne uno ancora dopo di lui, 0 se è l’ultimo pacchetto frammentato.
* Il fragment offset: ci dice qual è l’offset del primo pacchetto del segmento rispetto all’inizio del pacchetto originale (si basa sui byte)

Esempio: MTU da 1500 bytes, e la dimensione del pacchetto a 4000 bytes

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DF | MF | FRAGMENT OFFSET |
| FRAMMENTAZIONE DEL PACCHETTO | | | |
| 200 | 0 | 1 | 0 |
| 200 | 0 | 1 | 1500 |
| 200 | 0 | 0 | 3000 |

Il traffico parassita consuma le risorse della rete, questo succede per errori di instradamento o indirizzi. Per evitare questa situazione si usa il Time to Live: in questo tempo, modificato dal router, va decrementare il tempo di vita e se esso arriva a 0 allora viene scartato, mandando al mittente del pacchetto un messaggio con protocollo ICMP, che il pacchetto è stato scartato che il TTL è scaduto. Se si tiene lo standard viene lasciata la possibilità di attraversare solo 127 router.

Protocollo: campo che dice quale protocollo è incapsulato (TCP e UTP).

Controllo della parità solo sull’intestazione, anche perché il livello 2 che lo deve fare su tutto il pacchetto.

Source e il Destination: sono campi che contengono il mittente e il destinatario IP dei dispositivi.