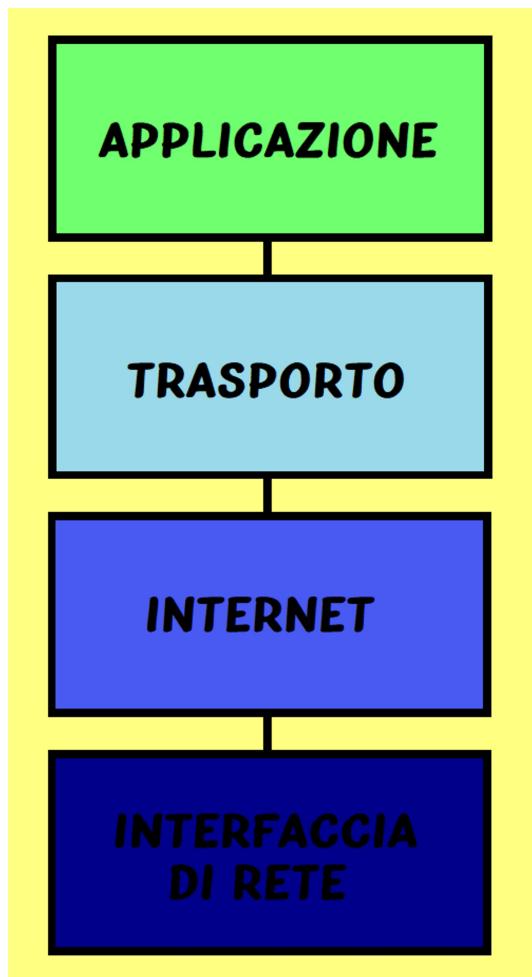


Modello TCP/IP

domenica 6 ottobre 2019 17:52



APPLICAZIONE

Programmi che accedono alla rete. Ogni programma interagisce con i livelli del modello TCP/IP per inviare o ricevere i dati tramite i messaggi o i flussi (stream).

M₂M -> Machine to Machine (novità)

Serve per la creazione di APP automatiche, che comunicano tra loro senza un intermediario umano in modo autonomo e indipendente.

Es: 20 o più robot che collaborano

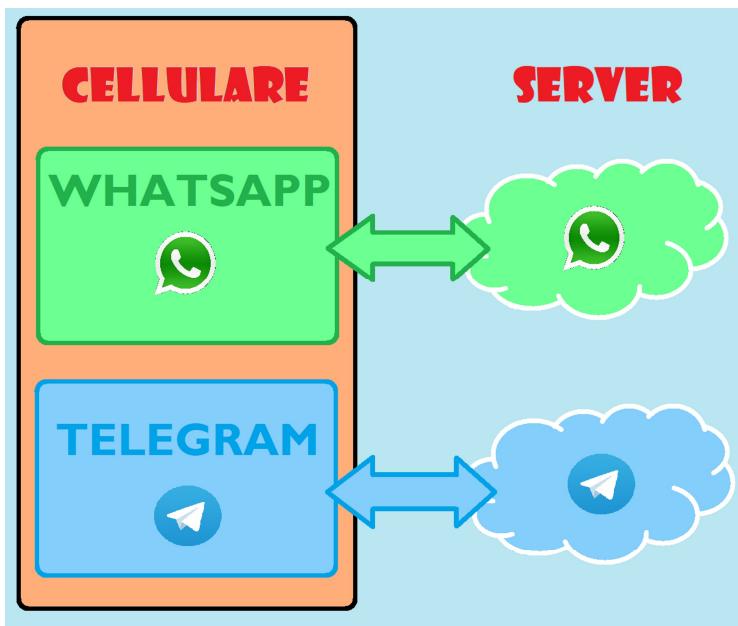
TRASPORTO

Comunicazione *end to end*, tra un programma e l'altro (processi)

Il livello trasporto permette la comunicazione tra il programma e i server o tra programmi.

I processi che può eseguire simultaneamente sono $2^{16} - 1 \cong 65000$ perché riceve messaggi o flussi contemporaneamente da tutti i processi e allora a ognuno di loro viene assegnato un codice

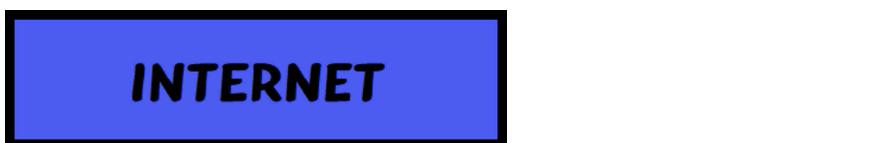
identificativo per riconoscerli.



È capace di regolare la velocità dei dati e di determinarne la loro tipologia, divide i messaggi in pacchetti da inviare al livello successivo.

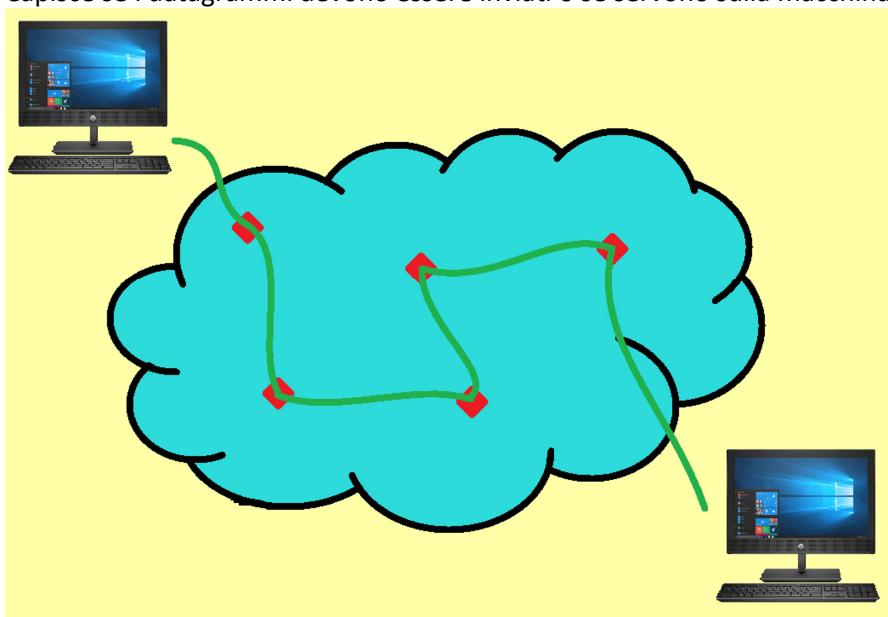
È affidabile -> ACKNOWLEDGE SYSTEM -> messaggio di conferma

Il protocollo **UDP** è meno affidabile del **TCP**, è utilizzato nello streaming perché è più veloce e anche se non arriva un frame durante lo streaming l'utente non se ne accorge.



Ha la funzione di realizzare la comunicazione tra computer diversi e controlla se i datagrammi sono validi.

Capisce se i datagrammi devono essere inviati o se servono sulla macchina locale.



Livello che è a cavallo tra il SO e l'hardware (scheda di rete), accetta (in entrata) o trasmette(in uscita) i datagrammi IP.

HOST-TO-NETWORK

lunedì 21 ottobre 2019 18:35

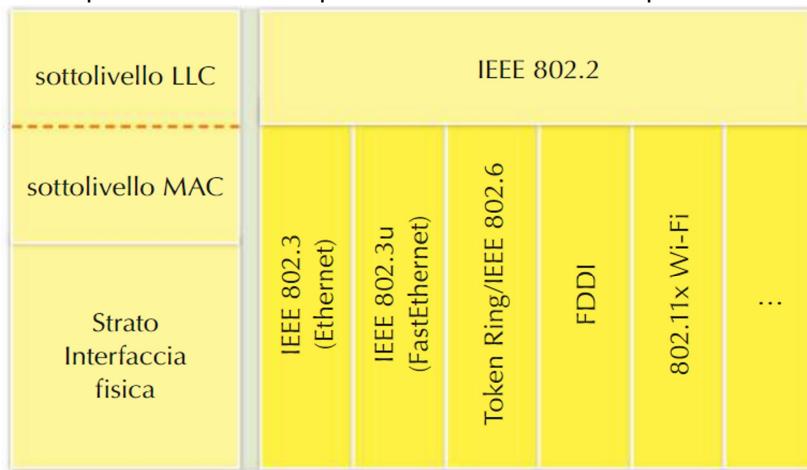


Il livello Host-to-network o interfaccia di rete è diviso in due sottolivelli:

LLC: Logical Link Control (connesso con il livello internet)

MAC: Medium Access Control (connesso con l'hardware)

Il livello LLC ha un solo protocollo mentre quello del Mac si adatta al tipo di mezzo di comunicazione.



LLC

lunedì 21 ottobre 2019 18:56

Logical Link Network

Il protocollo 802.2 è quello che definisce l'LLC ed è uguale per tutti.

Fornisce servizi senza connessione né affidabilità al livello superiore:

- **UNICAST:** Permette di spedire i frame a una destinazione
- **BROADCAST:** Permette di spedire i frame a più dispositivi
- **MULTICAST:** Permette di spedire i frame a tutti

Non ho però garanzia che ciò che mando arrivi né che arrivi nell'ordine giusto

MAC

lunedì 21 ottobre 2019 19:11

Medium Access Control

Questo livello può avere protocolli diversi in base al mezzo fisico utilizzato.

Si occupa di:

- **Generare Frame**
- **Controllare gli errori sui frame**
- **Accedere al mezzo fisico**

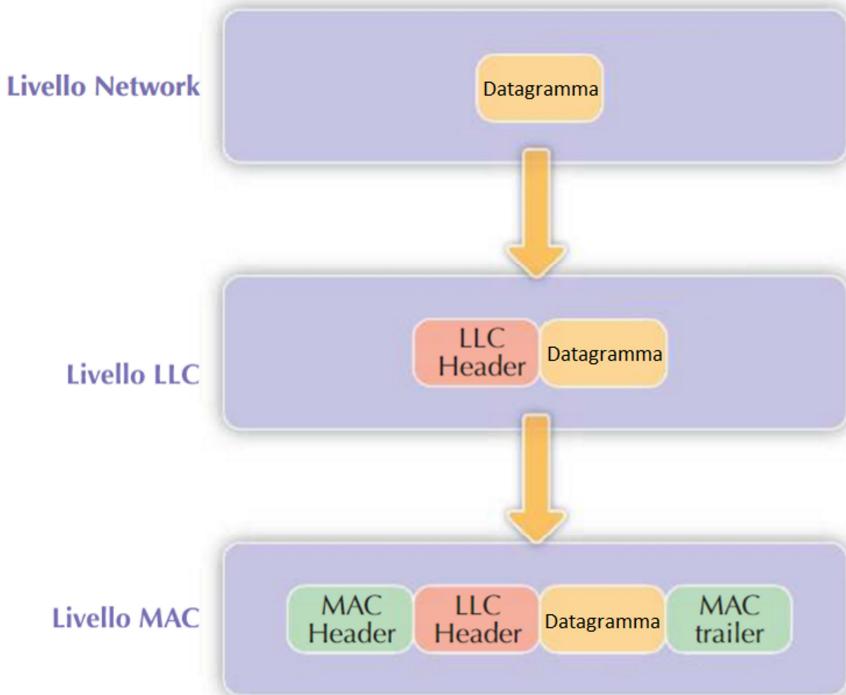
I messaggi partono da un dispositivo con un certo indirizzo MAC per arrivare a un dispositivo con un indirizzo MAC diverso, per farlo inviano il loro segnale tramite il mezzo fisico, nel caso più host comunicano attraverso lo stesso mezzo fisico è necessario evitare di mischiare le informazioni e per questo è necessario il protocollo specifico del mezzo

802.3	Ethernet
802.11	Wi-Fi
802.15	Bluetooth

Invio del messaggio

lunedì 21 ottobre 2019 19:21

Il messaggio arriva da un livello superiore e viene inviato dopo essere stato incapsulato.



Il livello Network trasmette un datagramma, nel livello LLC il datagramma viene incapsulato in un messaggio LLC che aggiunge un'introduzione al datagramma.

Successivamente il messaggio LLC viene incapsulato in un messaggio MAC nel livello MAC che aggiunge sia un'introduzione sia una coda.

Indirizzamento MAC

lunedì 21 ottobre 2019 19:22

INDIRIZZAMENTO FISICO

L'indirizzo MAC è salvato in una rom sulla scheda di rete ed è formato da 6 byte cioè da 6 coppie di caratteri esadecimali

1 byte.1 byte.1 byte.1 byte.1 byte.1 byte

XX.XX.XX.XX.XX.XX

Produttore della
scheda di rete

Codice identificativo
della scheda di rete

Non tutti gli indirizzi MAC sono utilizzati per degli HOST, 2 sono riservati: quello di broadcast (invia a tutti) e quello di multicast (invia a tutti di dispositivi con i primi 5 gruppi uguali al suo).

Indirizzo di Broadcast:

FF.FF.FF.FF.FF.FF

Indirizzo Multicast:

XX.XX.XX.XX.XX.X1

L'indirizzo MAC si può cambiare attraverso una procedura chiamata **MAC spoofing**.

Collisione

lunedì 28 ottobre 2019 15:41

Quando due segnali elettrici viaggiano utilizzando la stessa linea e si incontrano si sommano formando un segnale elettrico senza valore.

Dato che internet è una rete democratica non è gestita da elementi centrali (HUB, router, switch..) ma dai suoi utilizzatori (host).

Perciò le soluzioni alle congestioni sono:

- Il dispositivo centrale (HUB) potrebbe decidere di inviare i dati a un dispositivo alla volta ma nelle reti molto grandi sarebbe lentissimo
- Dato che internet è una rete democratica le congestioni vengono risolte dagli host

Protocolli IEEE 802.3: Ethernet

lunedì 28 ottobre 2019 15:54

- 802.3 10 Mbps
- 802.3u 100 Mbps
- 802.3z 1000 Mbps
- 802.3z 10000 Mbps

FRAME ETHERNET (802.3)

lunedì 21 ottobre 2019 19:42

Esce dalla scheda di rete del dispositivo emittente e arriva a quella del destinatario.

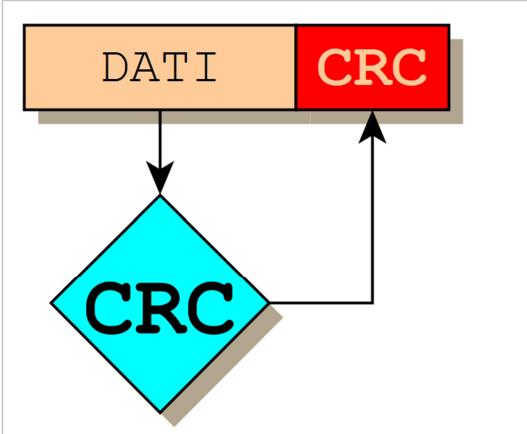
intestazione				coda	
Preambolo	Indirizzo destinazione	Indirizzo sorgente	Tipo	Dati	CRC
8 byte	6 byte	6 byte	2 byte	46-1500 byte	4 byte

- Preamble: identifica l'inizio di un frame
- Indirizzo destinazione: indirizzo del dispositivo che riceve il frame
- Indirizzo sorgente: indirizzo del dispositivo che invia il frame
- Tipo: tipo del frame ethernet
- Dati: dati provenienti dal livello network
- CRC: Controllo Ridondanza Ciclica

Controllo Ridondanza Ciclica

lunedì 21 ottobre 2019 20:28

Il CRC è un meccanismo che serve per capire se il messaggio è stato danneggiato.



Esso viene calcolato dal dispositivo di partenza e messo alla fine del frame, mi serve per capire la dimensione del dato.

Il dispositivo che riceve il frame separa i dati e il CRC, calcola il CRC sui dati e poi lo confronta con quello del frame, se sono uguali allora il messaggio è arrivato integro.

Dominio di Collisione

lunedì 28 ottobre 2019 15:47

Tutto dove può avvenire la collisione:

- HUB o WiFi: tutti i dispositivi connessi (tutti i PC)
- Switch: dispositivo che invia e dispositivo che riceve (2 PC)

Gestire le collisioni col protocollo IEEE 802.3

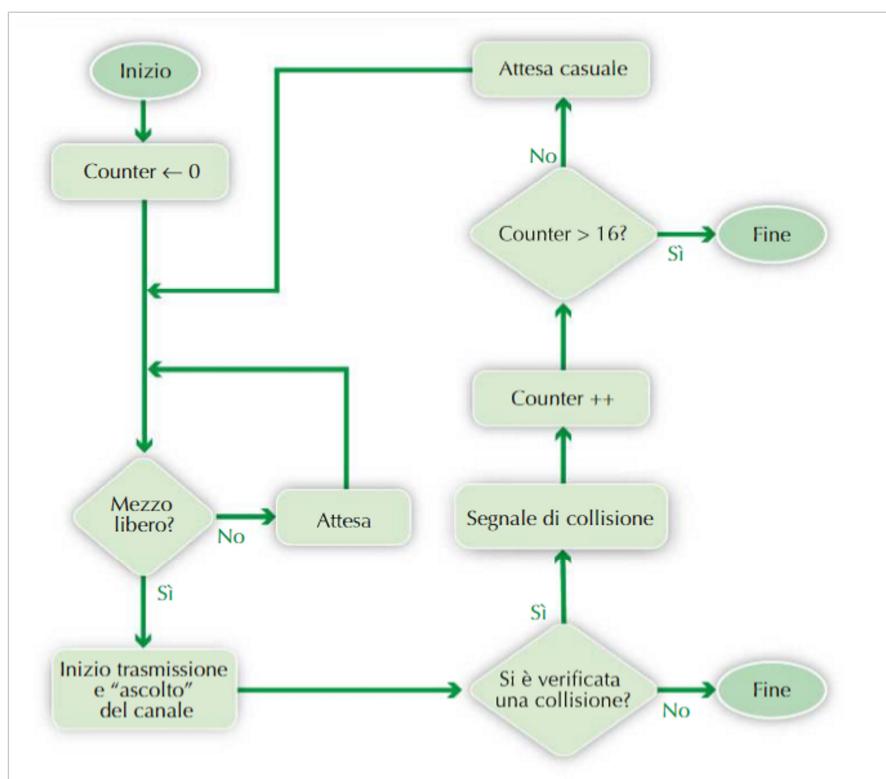
martedì 22 ottobre 2019 19:34

Nel protocollo Ethernet troviamo un algoritmo, l'algoritmo di CSMA/CD che mi permette di rilevare le collisioni del segnale.



Si basa sulle regole della buona educazione:

- "ascolto" prima di parlare, se parla già qualcun altro sto zitto
- Se qualcuno inizia a parlare con me io smetto di parlare



Inizializzo il contatore e poi controllo se il canale è libero, se lo è inizio a trasmettere e finisco l'invio a meno che si verifichi una collisione, in quel caso fermo l'invio del segnale e invio a tutti il segnale di collisione poi incremento il contatore e dopo un momento di attesa casuale riprovo.

Questo avviene per 16 volte (cosa molto rara) poi l'host smette di trasmettere perché il problema è della rete.

Il tempo casuale da attendere viene calcolato tramite l'**algoritmo di BACKOFF**

Il valore del tempo di attesa è un numero casuale tra **0** e $2^k - 1$.

K sarebbe il mio contatore. Quindi più K è grande più è probabile che l'intervallo sia grande questo per evitare di continuare a generare collisioni, quindi il dispositivo lascia trasmettere gli altri prima di trasmettere lui.

Questo è molto comodo per le app di messaggistica ma non per quelle di streaming perché dato che la trasmissione deve essere continua non può bloccarsi, per questo lo streaming utilizza il protocollo UDP e non il protocollo TCP.

Protocollo 802.11: Wi-Fi

lunedì 28 ottobre 2019 15:58



Wi-Fi è un simbolo registrato.



Host Wireless: sono dispositivi periferici che eseguono applicazioni.

Stazione base: è responsabile dell'invio e della ricezione dei messaggi tra gli host ad essa associati. Per host associato si intende un host tale che:

- si trova nell'area di copertura della stazione base
- utilizza la stazione base per trasmettere dati verso il resto della rete.

Access Point: è una stazione base nelle LAN 802.11.

Collegamenti wireless: l'host si connette alla stazione base attraverso un canale di comunicazione wireless.

SSID (Identificatore del Service Set): nome della rete Wi-Fi.

BEACON: messaggi per far identificare agli host la SSID della rete

È più soggettivo rispetto a errori rispetto alle reti cablate (Wired).

Problemi del protocollo 802.11

lunedì 28 ottobre 2019 16:18

❖ Attenuazione del segnale:

- A causa di ostacoli
- A causa della lontananza dall'access point:
 - $P = c * \frac{1}{d^2}$: potenza= costante (del router) per 1 fratto distanza al quadrato

❖ Interferenza da parte di altre sorgenti:

- sorgenti radio che trasmettono nella stessa banda di frequenza.

❖ Scrambler

- Dispositivi che mettono fuori uso una rete Wi-Fi

Tipi di protocollo 802.11

domenica 3 novembre 2019 15:07

Esistono due tipi di frequenze:

- 2.4 GHz
- 5 GHz

Sono frequenze molto alte perché devono trasportare una grande quantità di dati.

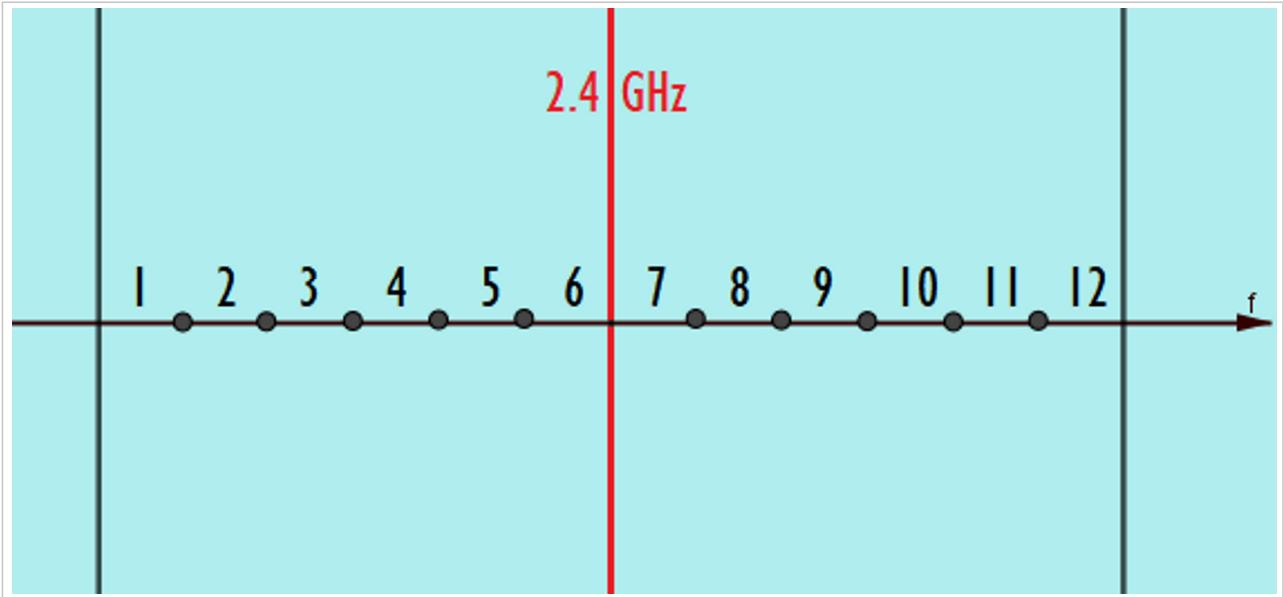
I vari protocolli esistenti per questo tipo di trasmissione sono:

Nome protocollo	Velocità	Distanza	Frequenza
• 802.11a	54 Mbps	50 m	5 GHz
• 802.11b	11 Mbps	100 m	2.4 GHz
• 802.11g	54 Mbps	100 m	2.4 GHz
• 802.11n	540 Mbps	250 m	2.4 GHz
• 802.11a/c	1.3 Gbps	250 m	5 GHz

Canali delle reti Wireless

domenica 3 novembre 2019 16:03

Non utilizziamo esattamente una frequenza ma un range di frequenze centrate in esso e dividendo questo abbiamo più canali.



Quindi anche se noi indichiamo una frequenza precisa intendiamo un range attorno ad essa.

FRAME Wi-Fi (802.11)

lunedì 21 ottobre 2019 19:42

Esce dalla scheda di rete del dispositivo emittente e arriva a quella del destinatario.
È molto simile al frame ethernet, l'unica differenza è che contiene dei campi in più.

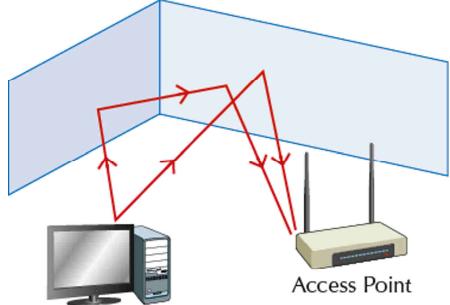
Frame Ethernet:

intestazione						coda
Preambolo	Indirizzo destinazione	Indirizzo sorgente	Tipo	Dati	CRC	
8 byte	6 byte	6 byte	2 byte	46-1500 byte	4 byte	

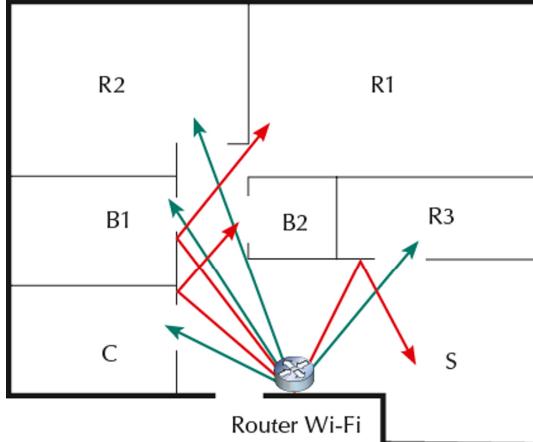
Collisioni del protocollo IEEE 802.11

domenica 3 novembre 2019 15:26

Il segnale arriva al router tramite più percorsi che fanno interferenza tra loro infatti per questo l'access point ha più antenne per distinguerli. **MULTIPATH**



Il pc invia il segnale in tutte le direzioni e il router deve riuscire a isolare un segnale per poter comprenderne il significato



Disposizione
ideale del router
in un
appartamento
per avere
un'ottima
copertura Wi-Fi

Gestire le collisioni col protocollo IEEE 802.11

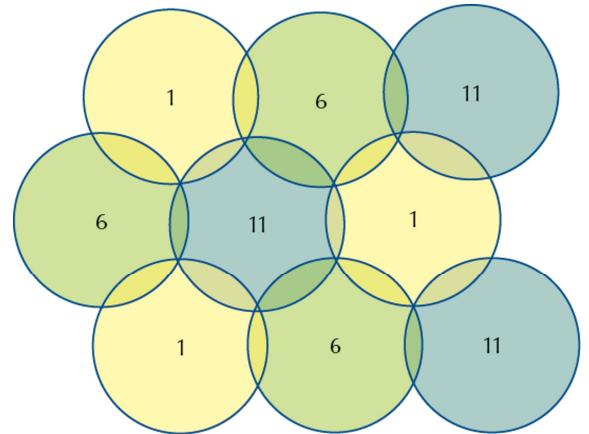
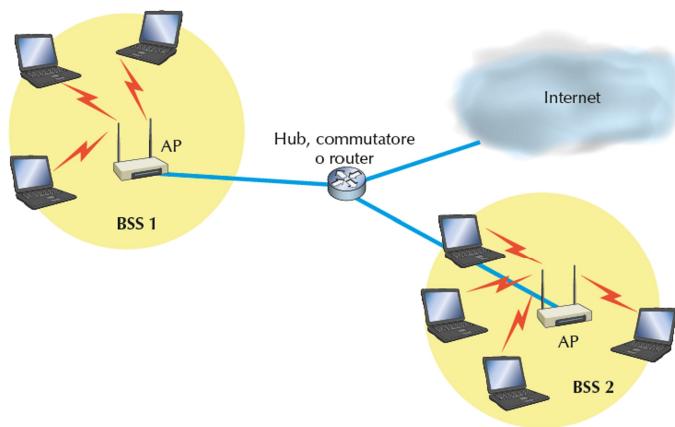
domenica 3 novembre 2019 15:34

Nel protocollo Wi-Fi troviamo un algoritmo, l'algoritmo di CSMA/CA che mi permette di evitare le collisioni del segnale. Questo perché rilevarle sarebbe troppo complicato.

CSMA/CA Carrier Sense Multiple Access / Collision Avoidance accesso multiplo a rilevazione della portante per evitare collisioni

In ogni rete ci sono più access point e ognuno ha la sua BSS (basic service set) cioè la sua copertura ma potrebbe capitare che i segnali si sovrappongono per evitare aree scoperte.

ESS: Somma di tutte le BSS della stessa rete.

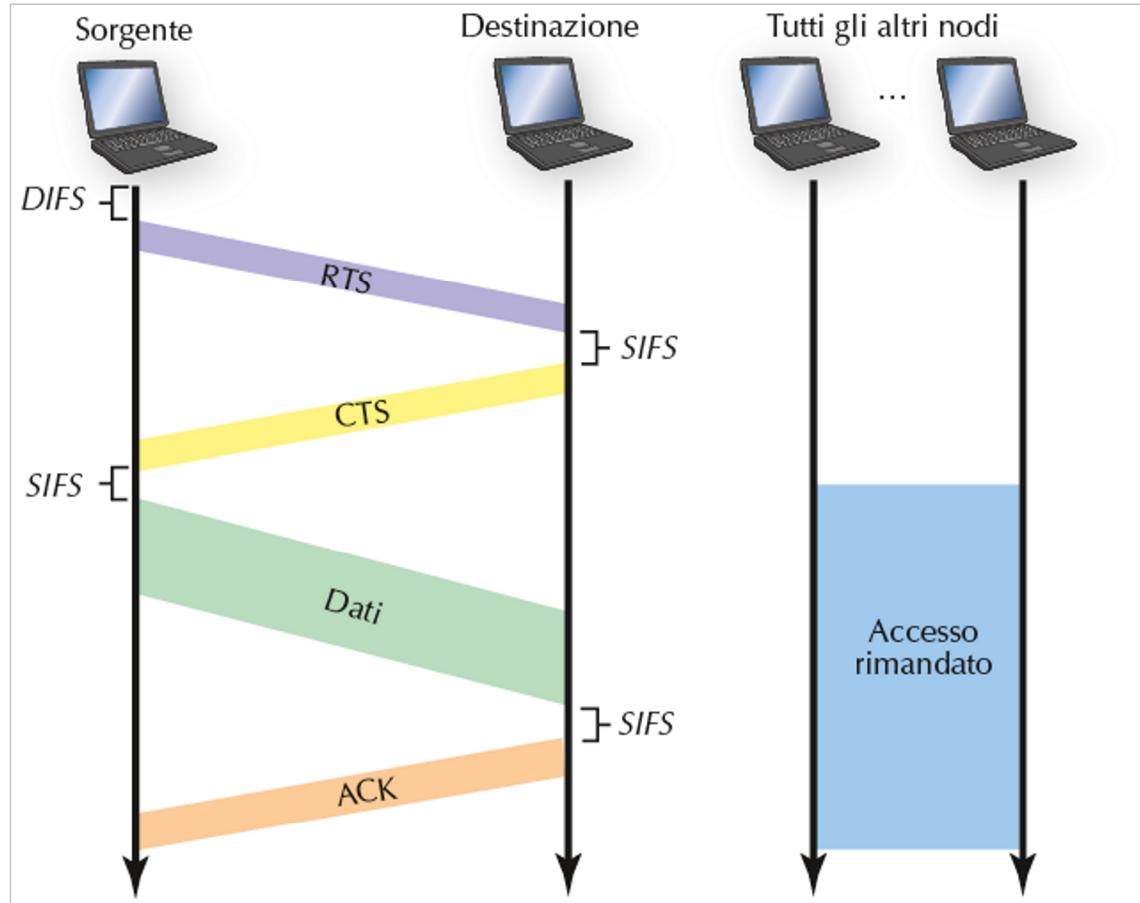


Quindi per evitare collisioni in questo caso si utilizza un altro canale.

Trasmissione di dati con il CSMA/CA

domenica 3 novembre 2019 16:29

Dato che non possono essere rilevate collisioni ma bisogna evitarle è necessario trasmettere il messaggio dall'inizio alla fine senza interferenze.



Prima di inviare i dati il dispositivo controlla se la rete è libera, se lo è invia una richiesta al router (destinazione) di poter trasmettere dati (RTS: richiesta di trasmissione dati) e l'access point risponde con un messaggio in broadcast con il quale comunica a tutti che quel dispositivo è l'unico autorizzato a trasmettere. Il pc allora invia i dati e se tutto è andato a buon fine il dispositivo di destinazione invia un messaggio in broadcast con il quale comunica che la trasmissione è stata completata senza errori (dati arrivati in ordine errato, mancanti o danneggiati).

Nel caso invece la rete non sia libera attende un tempo casuale prima di riprovare a inviare i dati come nell'algoritmo CSMA/CD.

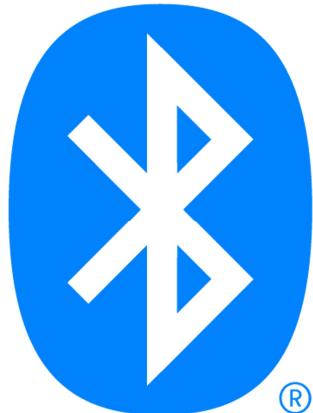
Protocollo IEEE 802.16: WiMAX

lunedì 11 novembre 2019 18:03

Questo protocollo è utilizzato soprattutto da qualche provider Internet e può arrivare fino a **50 Km** di distanza viaggiando su frequenze da **2 a 11 GHz**.

Protocollo 802.15: Bluetooth

lunedì 11 novembre 2019 18:06



Serve da formare reti a bassa potenza di tipo PAN (max 10 m), la bassa potenza serve a consumare poca batteria
Il Bluetooth consente di avere 1 dispositivo MASTER e al massimo 7 dispositivi SLAVE.

PICONET: unità di base

SCATTERNET: rete formata da più PICONET

AIRDROP: applicazione Apple per scambiare dati con il Bluetooth molto velocemente.

PPP e PPPoE

lunedì 11 novembre 2019 18:14

PPP: point to point protocol

Protocollo utilizzato per portare internet sui doppini del telefono

PPPoE: point to point protocol over Ethernet

Protocollo utilizzato per incapsulare un frame PPP in Ethernet

INTERNET

martedì 19 novembre 2019 18:06

Questo livello prende questo nome perché ha permesso la comunicazione tra molti dispositivi.

RFC 1958: regole della buona programmazione del livello internet

Mercoledì 19 novembre 2014 - 18:08 > [RFC: Request For Comments](#)

1) Deve Funzionare

Non posso pubblicarlo e subito dopo trovare un BUG

2) KISS: Keep It Simple

Cercala via più semplice

3) Scelte chiare

Unica idea, essenziale nei lavori di gruppo

4) Sfrutta la modularità

È più semplice, pratica e modificabile

5) Eterogeneità

Il codice deve essere eseguibile da tutti i dispositivi anche se differenti.

6) Evita parametri statici

Evitare di definire il valore della connessione ma creare un'algoritmo che trovi il valore migliore, la rete potrebbe essere troppo grande o troppo piccola per un valore prestabilito.

7) Meglio buono o perfetto?

Prima si sviluppa un buon programma funzionante e poi lo si perfeziona

8) Rigido o tollerante?

Chi invia i dati deve seguire molto rigidamente le regole mentre chi riceve deve essere tollerante perché deve aspettarsi delle eccezioni

9) Scalabilità

Il sistema deve riuscire a gestire un numero di host variabili

10) Costi e prestazioni

Se costa troppo o ha prestazioni poco elevate non viene utilizzato

IP internet protocol

martedì 3 dicembre 2019 17:41



Ne esistono 2 versioni:

- ▶ IP v.4: RFC 791
- ▶ IP v.6: RFC 4291

Attualmente si utilizzano entrambe ma principalmente la versione 4
I messaggi inviati da questo protocollo si chiamano datagrammi IP. Oltre ai messaggi implementa anche il viaggio che essi devono fare attraverso la rete ma non è affidabile.

VERSIONE 4

Ha pochi indirizzi IP ma grazie al NAT si riesce ad avere molti dispositivi in più.

VERSIONE 6

Ha tantissimi indirizzi IP ed è più semplice.

Utilizziamo principalmente la versione 4 rispetto alla 6 perché i router attuali non sono abilitati a supportare la versione 6.

IANA

martedì 3 dicembre 2019 19:06



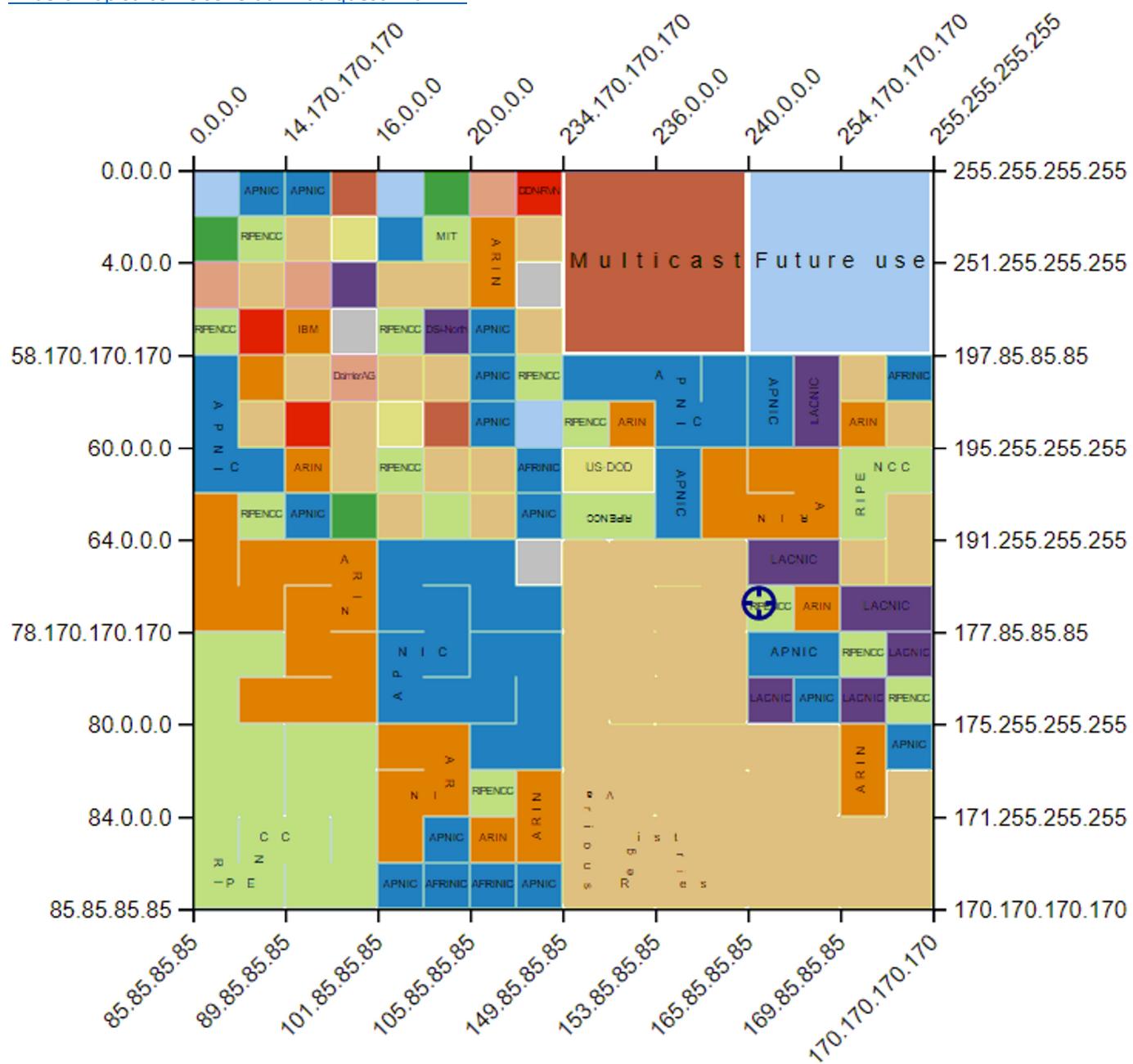
Internet Assigned Numbers Authority

Istituto mondiale che si occupa di assegnare gli indirizzi IP e le porte in internet.

Sul suo sito è possibile trovare tutti i domini registrati fino ad ora su internet con molte altre informazioni.

Fornisce inoltre la funzione Whois che permette di identificare un'indirizzo IP e ne fornisce molte informazioni.

[Hilbert map su come sono utilizzati questi indirizzi](#)



Datagrammi IP

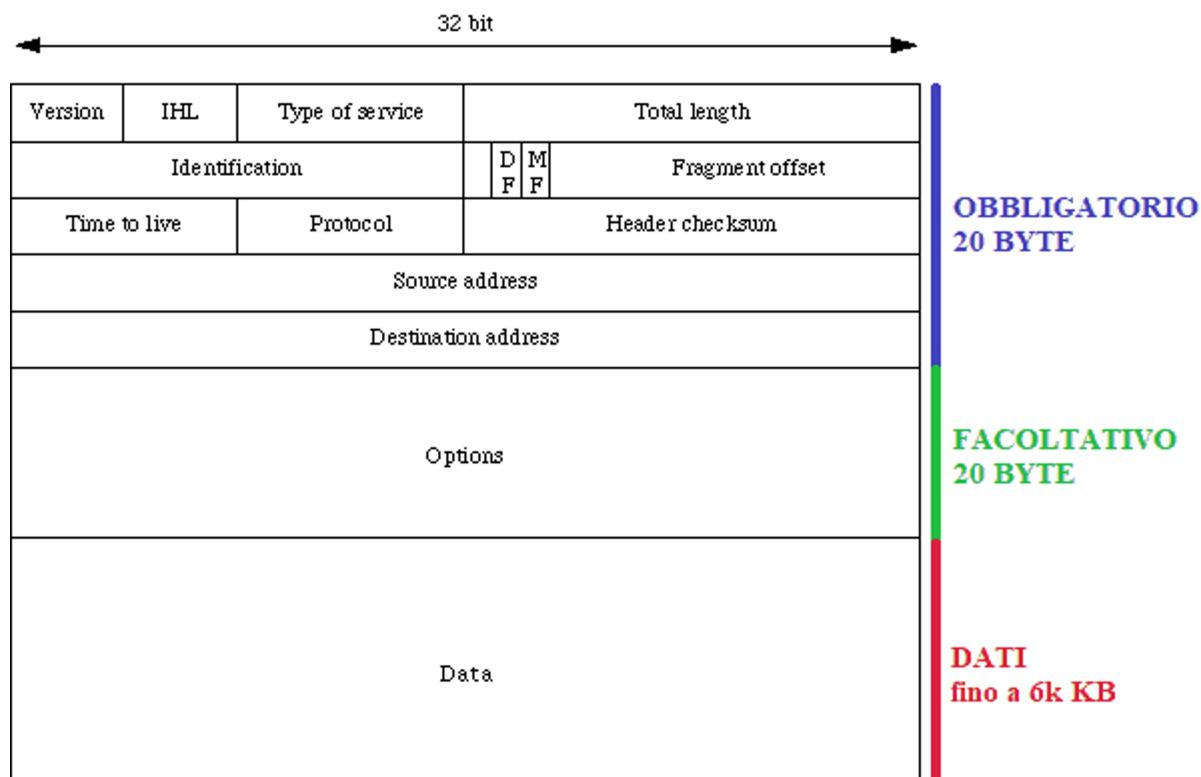
martedì 3 dicembre 2019 17:57

I datagrammi solo i pacchetti del livello trasporto spezzatati e occupano solitamente un massimo di 64 Kb. Infatti se è troppo grande per essere trasportato dal livello fisico viene frammentato e poi ricomposto.

I datagrammi sono come dei piccioni viaggiatori, una volta inviati devono trovare la loro destinazione a tutti i costi.

Datagramma IP v.4

martedì 3 dicembre 2019 18:03



È formato da 1 word per riga (1 word = 4 byte).



4 bit

Ogni host quando riceve un datagramma deve sapere se è un datagramma della versione 4 o della versione 6
0100 per la versione 4



4 byte

Indica l'indirizzo IP del dispositivo che invia il file



4 byte

Indica l'indirizzo IP del dispositivo che riceve il file



4 bit

Internet Header Length

Indica la lunghezza della parte di testa del datagramma (tutto tranne i dati)
Come unità di misura utilizza le word, vale un minimo di 5 ma può arrivare a valere 15



6 bit

Type of Service

Permette ai router di indirizzare i datagrammi per la strada giusta



TOS

6 bit

Type of Service

Permette al router di indirizzare i datagrammi per la strada giusta

Era pensato per indicare il tipo di servizio: streaming / download / navigazione, oggi serve per massimizzare la banda. È l'unico campo che ha cambiato significato.



TOTAL LENGTH

16 bit

Lunghezza totale del datagramma

Da 0 a 65535 (bit)



TTL

8 bit

Time to Live

Da 0 a 255, si decrementa di 1 ogni volta che subisce un hop (passaggio da un router)

Quando arriva a valere 0 il datagramma cessa di esistere.

Serve per evitare di intasare la rete quando il datagramma comincia a girare in Loop.

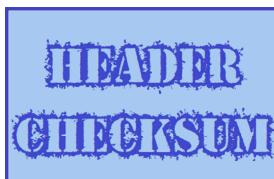


PROTOCOL

8 bit

Tipo di protocollo utilizzato

Soltanamente UDP (17) o TCP (6)



HEADER CHECKSUM

16 bit

Algoritmo che calcola se il datagramma è corretto

Viene ricalcolato a ogni Hop

Frammentazione del datagramma IP

martedì 7 gennaio 2020 09:52

Il datagramma deve essere spedito tramite frame e dato che questi hanno un MTV (Maximum Transmission Unit)

Identification	D F	M F	Fragment offset
----------------	--------	--------	-----------------

- **Identification: 16 bit**

Codice identificativo del datagramma

- **DF: don't Fragment: 1 bit**

Indica se il datagramma è frammentato

- **MF: More Fragment: 1 bit**

Indica se ci sono altri frammenti di quel datagramma

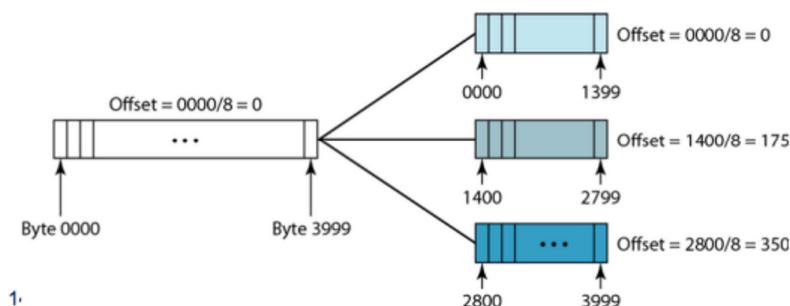
- **Fragment Offset: 8 bit**

Indica la posizione del frammento, serve per ordinarli

Esempio di frammentazione

Datagram di 4000 byte frammentato in 3 frammenti lunghi 1400byte

- Devo numerare da 0 a 3999
- Il primo da 0 a 1399 per cui l'offset è $0/8 = 0$. **MF = 1**
- Il secondo da 1400 a 2799: l'offset vale $1400/8 = 175$. **MF = 1**
- Il terzo 2800 a 3999: l'offset vale $2800/8 = 350$. **MF = 0**



Routing

martedì 11 febbraio 2020 08:17

Come i datagrammi IPv4 e IPv6 passano su internet

Indirizzi IP v.4

martedì 7 gennaio 2020 18:44

Esistono 2^{32} (4,294 miliardi) indirizzi IP

Esistono più classi per differenziare gli indirizzi:

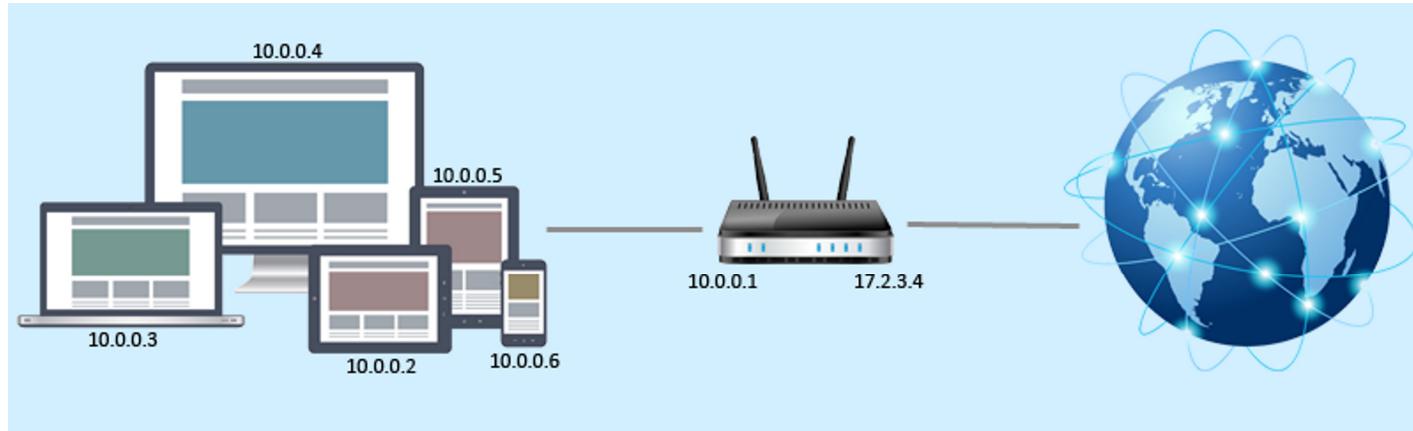
- **Classe A (0):** 128 networks con 16M indirizzi ciascuna
- **Classe B (10):** 16384 networks con 64K indirizzi ciascuna
- **Classe C (110):** 2M networks con 256 indirizzi ciascuna
- **Classe D (1110):** Indirizzi Multicast (268 M indirizzi)
- **Classe E (1111):** Riservata (di nuovo 268M indirizzi)

Indirizzi IP speciali

martedì 7 gennaio 2020 18:51

NAT: RFC 3022

martedì 7 gennaio 2020 18:53



È un meccanismo che permette di cambiare l'indirizzo IP nella rete locale (indirizzo privato ≠ indirizzo pubblico) e che permette di risparmiare indirizzi IP se utilizzato correttamente.

Tipologie:

- ◆ **NAT statico**
- ◆ **NAT dinamico**
- ◆ **Overloading NAT**

NAT STATICO

A ogni indirizzo IP nella sottorete ne corrisponde uno in internet

NAT DINAMICO

A ogni indirizzo IP nella sottorete viene provvisoriamente assegnato un indirizzo IP quando deve comunicare con l'esterno. Infatti il router possiede N indirizzi pubblici e li assegna in questo modo. Se al momento della connessione non ci sono indirizzi liberi allora il datagramma dovrà attendere

OVERLOADING NAT (NAT)

Da tanti indirizzi IP si passa a un solo indirizzo IP infatti i messaggi vengono trasmessi come indirizzo + porta (concetto del livello di trasporto) per sapere chi invia/riceve messaggi.

IP v.6

martedì 7 gennaio 2020 19:10



INDIRIZZI:

Sono formati da 8 gruppi di 4 cifre esadecimali separati dai ":"
fe80:0000:0000:0000:09ed:27b3:9283:4609

Se un gruppo inizia con lo 0 allora posso evitare di scriverlo, la stessa cosa vale per gruppi di tutti zeri che indico con :: (una sola volta in tutto l'indirizzo posso abbreviare più gruppi di tutti zeri come ::, tanto se si vuole ricavare l'indirizzo basta aggiungere gruppi di 0 in quel punto finché non si arriva a 8 gruppi)

fe80::9ed:27b3:9283:4609

Con questo metodo di indirizzamento ci sono abbastanza indirizzi IP per indirizzare tutto.

$2^{128} = 340,282,366,920,938,000,000,000,000,000,000,000,000,000,000$

utilizzati dai fornitori				utilizzati dall'utente	
3 bit	5 bit	16 bit	24 bit	32 bit	48 bit
CODICE DI UNICAST 010	GESTORI DI INTERNET 0000:internic:nord america 0000:ripnic:europa 0000:apnic:asia e pacifico	IDENTIFICATIVO DELL'INTERNET SERVICE PROVIDER	IDENTIFICATIVO DEL CLIENTE	UTILIZZATI PER CREARE SOTTORETI	USATI PER IDENTIFICARE UN SINGOLO NODO

Indirizzi riservati IP v.6

giovedì 30 gennaio 2020 15:16

This host	Tutti 0
Loopback	Tutti 0 tranne 1 al bit meno significativo
Compatibili con IP v.4	Tutti 0 tranne gli ultimi 32 bit
Mapped (usati per comunicare con host IP v.4)	Tutti 0, 16 bit a 1 e 32 utilizzati per l'indirizzo

Transizione da ip v.4 a ip v.6

giovedì 30 gennaio 2020 15:47

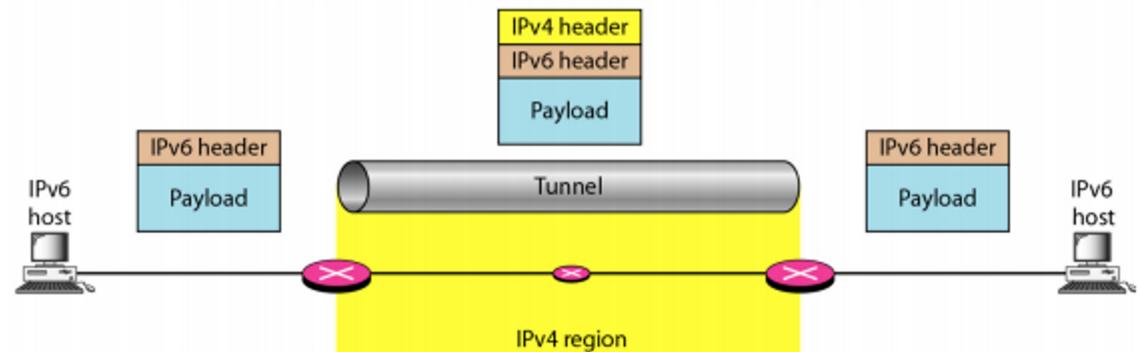


È iniziata ma è molto lenta.

All'inizio c'erano solo delle "isole" nella rete che utilizzavano ipv6 (anche ora) che un giorno si uniranno per rivoluzionare il mondo di internet.

Tutti gli host sono dual stack (ipv4 e ipv6) ma non lo sono i router/modem...

Queste isole ipv6 comunicano tra di loro tramite dei tunnel che gli permettono di attraversare zone ipv4 (TUNNELLING)



ARP: RFC 826

martedì 4 febbraio 2020 09:20

ADDRESS RESOLUTION PROTOCOL

ARP su basa su reti come ethernet sono in grado di eseguire il broadcast (servizi Host-to-Network).

Quando A vuole risalire all'indirizzo MAC dall'indirizzo IP di B I(B), trasmette un pacchetto speciale di broadcast che chiede all'host con l'indirizzo I(B) di rispondere con il proprio indirizzo fisico M(B).

Tutti gli host, tra cui B, ricevono la richiesta, ma solo B riconosce il suo indirizzo IP e invia la risposta contenente il suo indirizzo fisico. Quando A riceve la risposta, usa l'indirizzo fisico di B per comporre i frame ethernet contenenti i datagrammi diretti a B.

CACHE ARP

Può sembrare insensato che per inviare un pacchetto a B, A debba prima inviare un broadcast, quando invece potrebbe a questo punto inviare sempre i pacchetti in broadcast.

Il punto è che la trasmissione in broadcast è troppo costosa per la rete se utilizzata per ogni pacchetto. Per questo motivo i computer che usano ARP, tengono una cache contenente la tabella delle corrispondenze IP-MAC recentemente acquisite. Prima di inviare un datagramma a un destinatario, l'host cerca quel destinatario nella tabella.

Quindi la cache è molto utile e risparmia un sacco di messaggi broadcast.

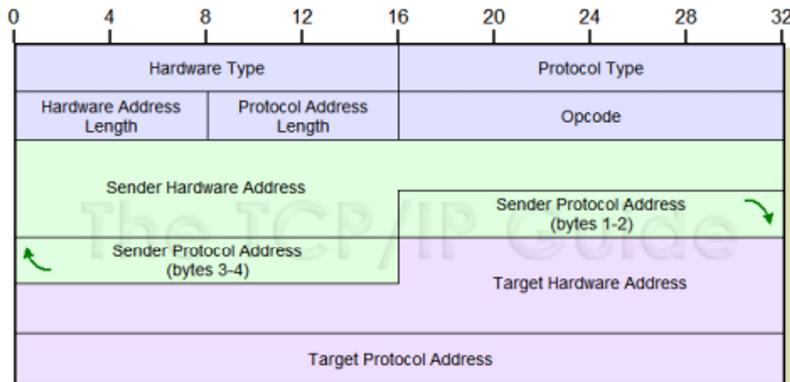
Per evitare di avere host non presenti sulla rete viene usato un timer (20 minuti) scaduto il quale la cache viene cancellata. Solo ora tramite nuovi messaggi broadcast ARP, l'host può scoprire se un host di destinazione è stato cancellato.

INVIO DELLE RICHIESTE e SALVATAGGIO DATI

- Quando A invia la richiesta ARP in broadcast a B include nella richiesta sia il suo IP che il suo indirizzo fisico, in modo che B possa già salvarli nella sua cache. Essendo che la richiesta è in broadcast, è ricevuta da tutte le macchine della rete, quindi ogni host si salva la traduzione dell'indirizzo IP di A in quello fisico.
- Quando A viene acceso, invia sempre una richiesta ARP senza destinatario a tutti gli host della rete.
- Quando A viene acceso invia una richiesta ARP anche per il proprio indirizzo IP, per verificare che non ci siano conflitti.

Datagramma ARP

martedì 4 febbraio 2020 09:32

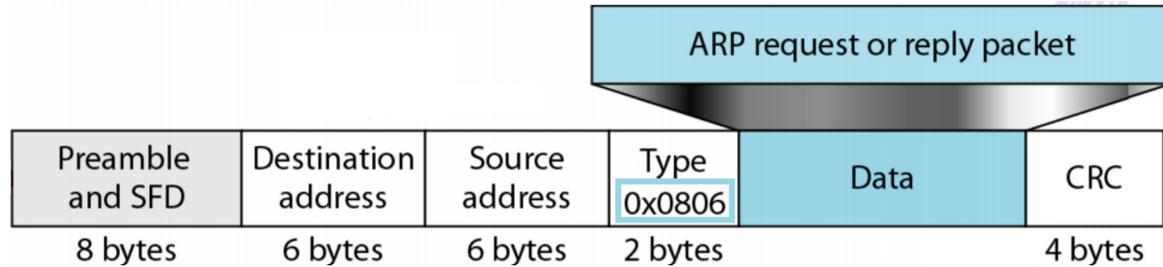


Hardware Type: 1 per ethernet...

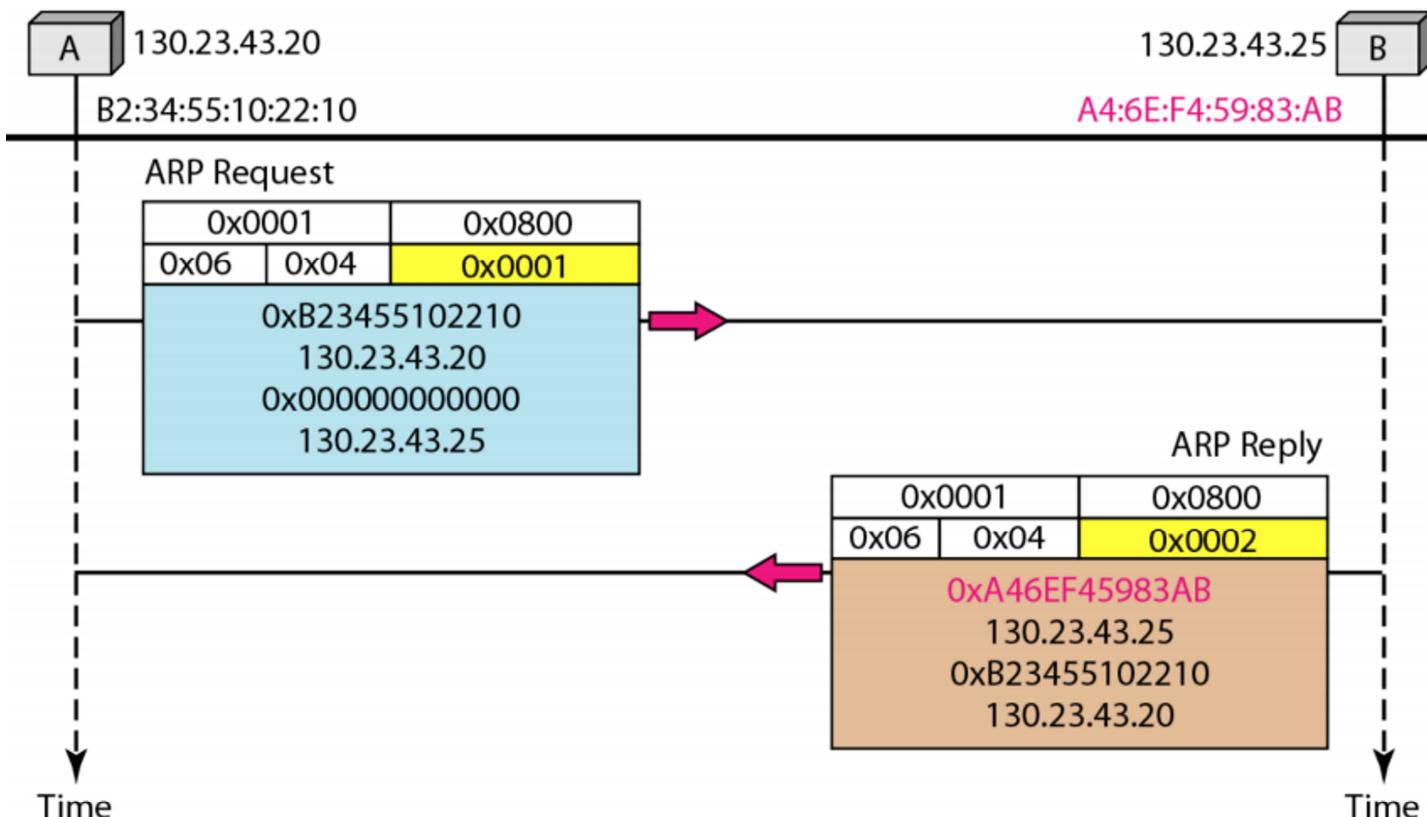
Protocol type: quali indirizzi di internet gestire IPv4: 0x8000

Opcode: codice operativo (1: richiesta ARP | 2: risposta ARP)

NEL FRAME ETHERNET



TRASMISSIONE

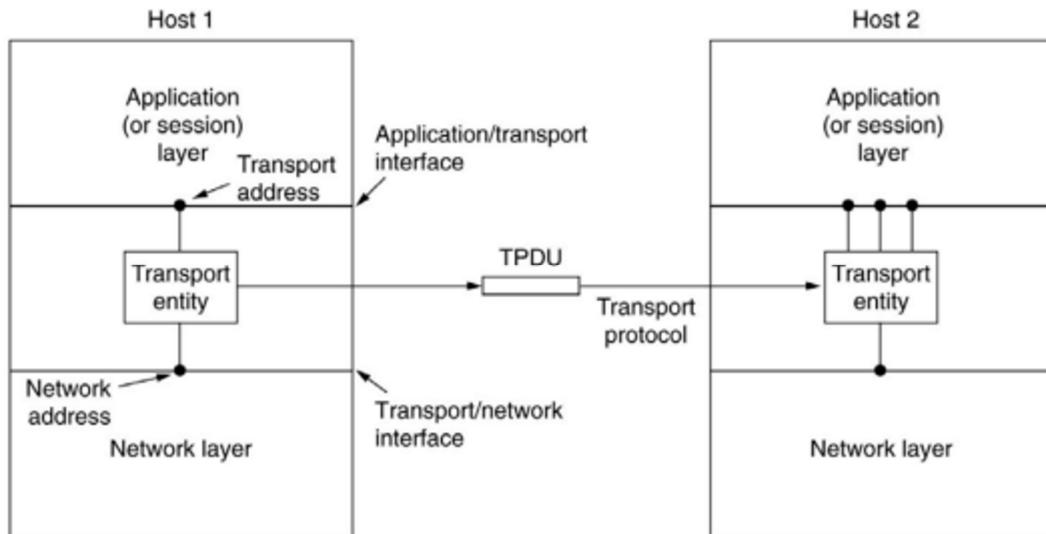


TRASPORTO

venerdì 24 aprile 2020 15:58

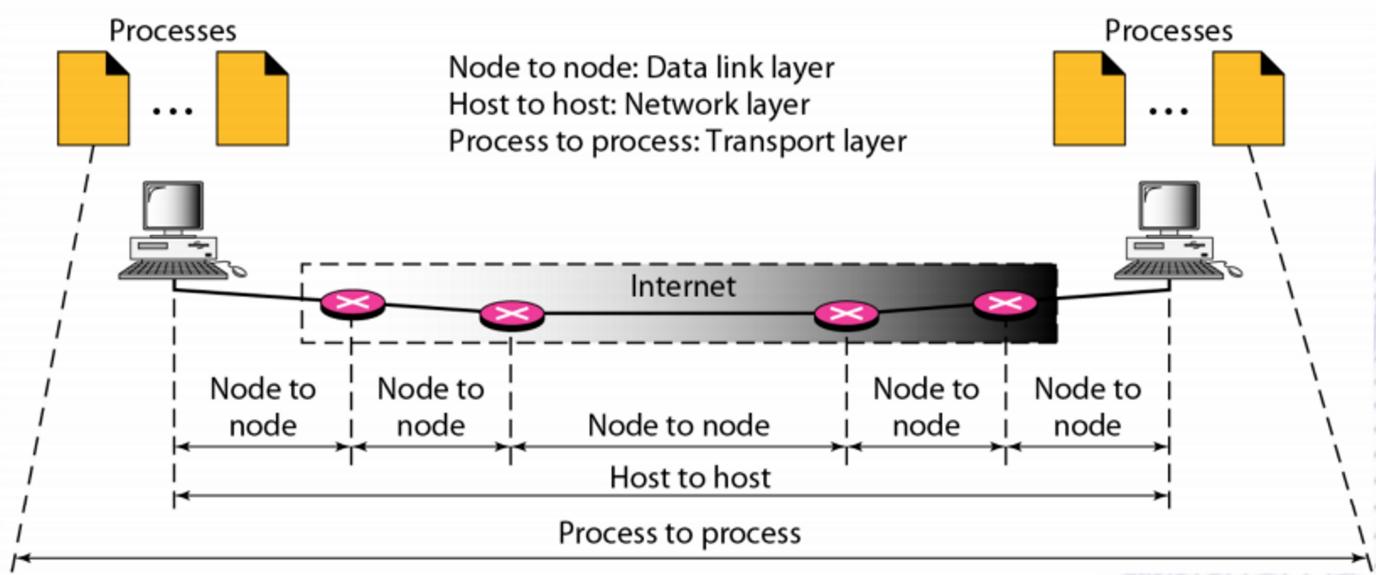
Deve garantire il trasporto di dati in modo efficiente e affidabile.

- Deve fornire un servizio di trasporto efficiente ed affidabile ai suoi clienti, normalmente processi del livello applicativo
- Si serve dei servizi forniti dal livello di network
- Solitamente è implementato nel kernel del sistema operativo o in processo separato dello spazio user in una libreria del sistema operativo.



Cosa fa?

venerdì 24 aprile 2020 16:27



Questo livello realizza la connessione tra processo e processo

Primitive o Socket Berkeley

venerdì 24 aprile 2020 16:29

SAP: Service access point (ogni protocollo comunica con il livello sottostante tramite di esso)
Quelli tra il livello applicazione e il livello trasporto vengono detti Primitive o Socket Berkeley
Quindi questi punti di accesso permettono di sfruttare lo stack tcp/ip e quindi permettono l'accesso alla rete.

Per programmare basta sapere quali sono le primitive e come sfruttarle.

Procedure primitive: (Bastano per creare qualsiasi applicazione)

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

Esempio:

Prendiamo un server e un client.

- Il server chiama una LISTEN, procedura di libreria che fa una system call e blocca il server fino a quando un client non si fa vivo
- Il client esegue una CONNECT, eseguita bloccando il chiamante e mandando un pacchetto al server. Dentro il payload di questo pacchetto c'è il messaggio di trasport layer per l'entità di trasporto del server.

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

Primitive	UDP	TCP	Server	Client	Locante
Socket	✓	✓	✓	✓	✗
Bind	✓	✓	✓	✗	✗
Listen	✗	✓	✓	✗	✗
Accept	✗	✓	✓	✗	✓
Connect	✗	✓	✗	✓	✗
Send	✓	✓	✓	✓	✗
Receive	✓	✓	✓	✓	✓
Close	✓	✓	✓	✓	✓

Socket

martedì 5 maggio 2020 12:19

SOCKET. Crea un end point e alloca spazio nel server

- I parametri indicano il formato di indirizzamento da usare, il tipo di servizio desiderato (es. reliable data stream) e il protocollo
- Una chiamata eseguita con successo restituisce un file descriptor da usare nelle call successive
- In questo senso si comporta come una OPEN unix su di un file

Su linux è un file perché tutto in quel sistema operativo è un file. Tipica di tutti i sistemi operativi tranne Windows.

Bind

martedì 5 maggio 2020 12:22

- Un socket appena creato non ha un indirizzo di rete. Questo viene assegnato dalla BIND
- Solo a questo punto si può fare la connessione
- Il SOCKET non si crea direttamente l'indirizzo perché alcune applicazioni possono volersi scegliere l'indirizzo, mentre per altre è irrilevante o inutile.

Listen

martedì 5 maggio 2020 12:22

- La LISTEN alloca dello spazio per accodare chiamate entranti, nel caso diversi client vogliano connettersi allo stesso istante
- Nei Socket Berkeley la LISTEN non è bloccante!

Accept

martedì 5 maggio 2020 12:23

- Per bloccarsi in ascolto il server chiama una ACCEPT
- Quando arriva una TPDU il server crea un nuovo socket con le stesse proprietà di quello originale e ritorna un file descriptor per esso
- Il server può creare (con una fork) un nuovo processo o un nuovo thread per gestire la connessione sul nuovo socket e tornare ad aspettare la prossima connessione

Tipi di app

venerdì 24 aprile 2020 16:37

Standalone: processo che non usa la rete

Client

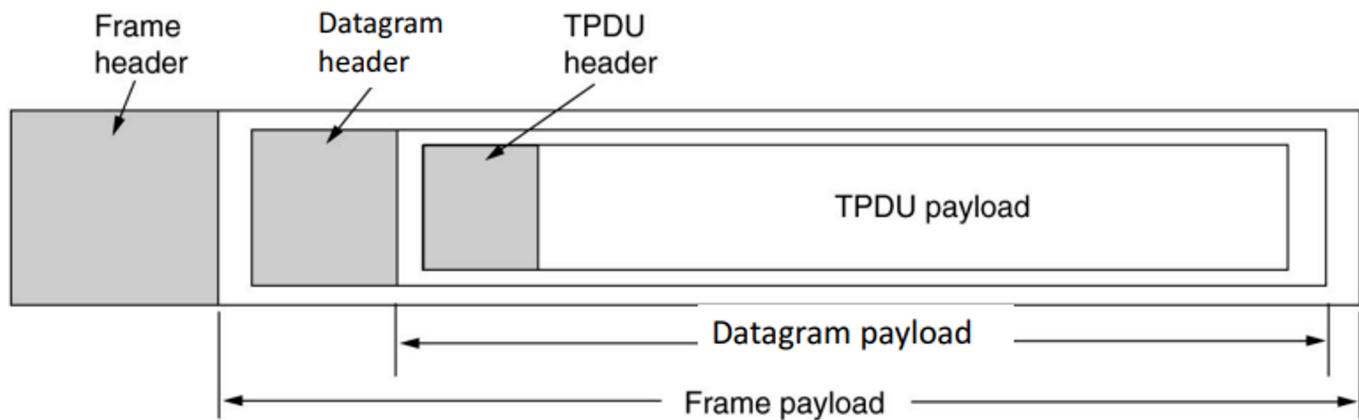
Server: Processi che forniscono un servizio

Actor: Processo Sia Client - Sia Server

Messaggi del livello trasporto

venerdì 24 aprile 2020 16:48

Chiamiamo TPDU, Transport Protocol Data Unit il pacchetto di livello Transport:



Protocolli internet

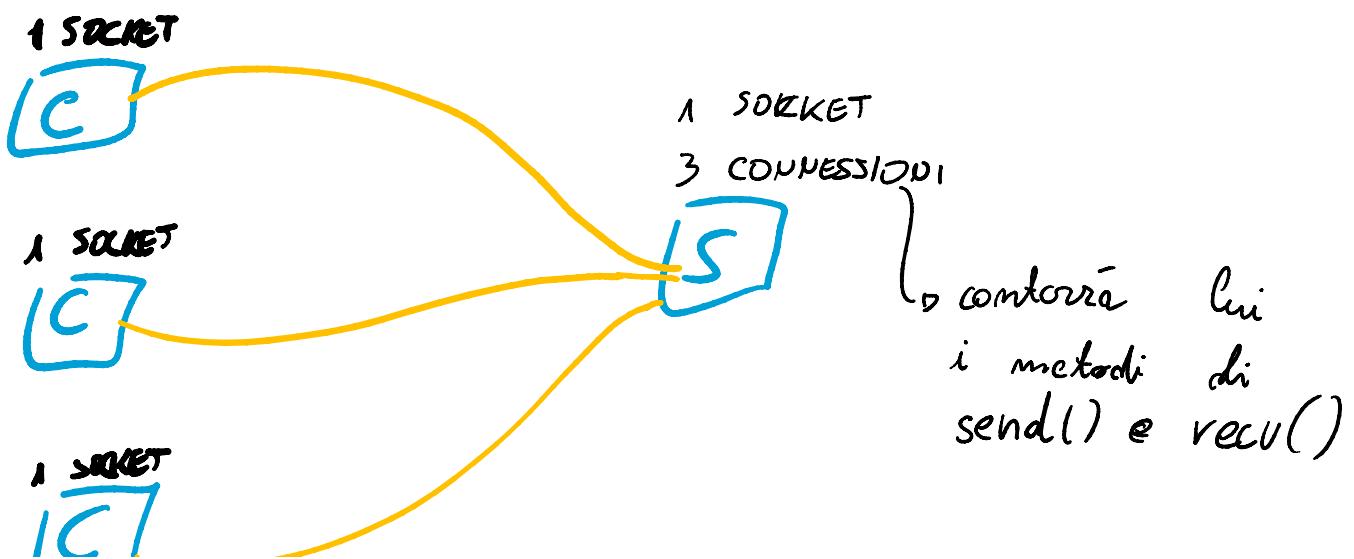
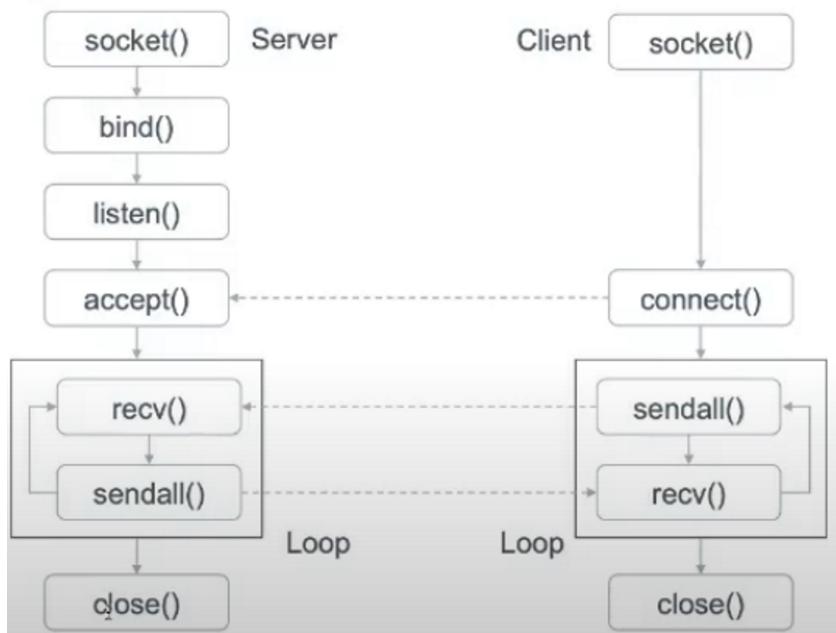
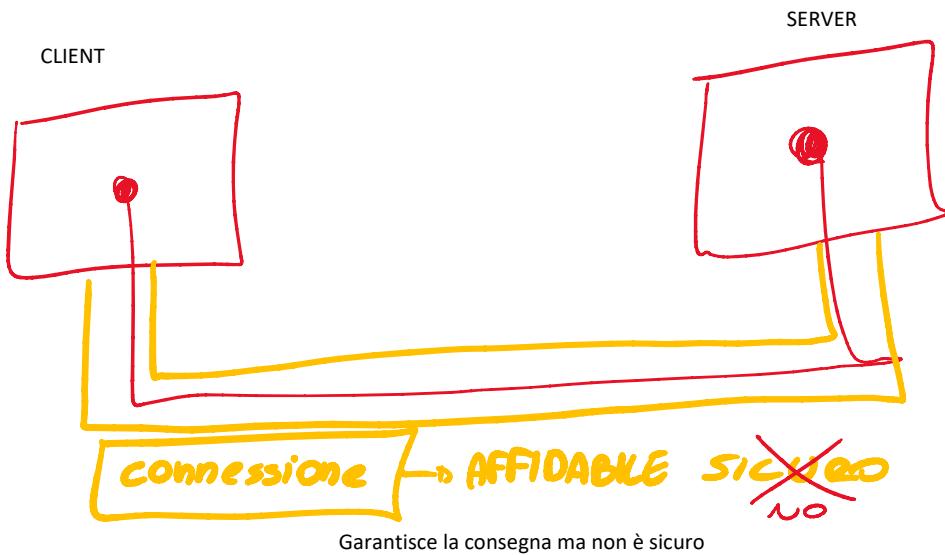
sabato 9 maggio 2020 11:37

Internet ha due protocolli di trasporto principali:

- uno connectionless: UDP (User Datagram Protocol)
- uno connection oriented: TCP (Transmission Control Protocol o anche Transfer Control Protocol)

TCP

martedì 5 maggio 2020 12:26





Tsap

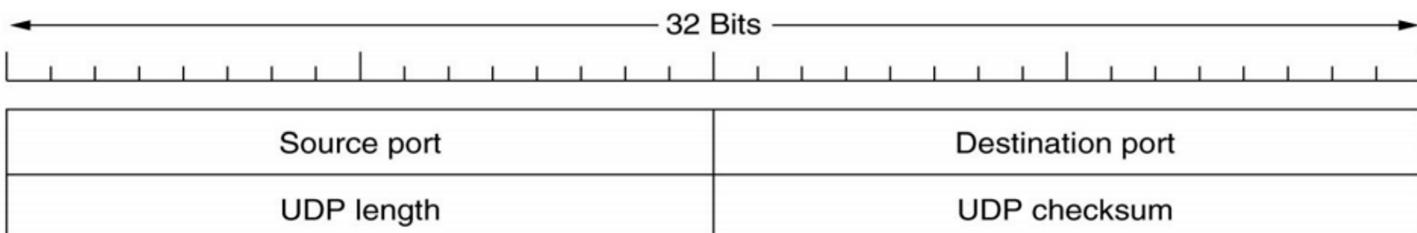
sabato 9 maggio 2020 11:30

Come trovo la porta? Come faccio a sapere che devo usare la TSAP 1522 ?

- Il server “time of day” è da anni sulla TSAP1522 e quindi tuo lo sanno (come tuo sanno che il web è sulla TCP:80). Sono i cosiddetti well known services (1 - 1023)
- Ma se voglio parlare con un processo che esiste solo per poco tempo? Posso usare un process server che mi fa da proxy: quando arriva la CONNECT con l’indirizzo della TSAP se non c’è un server in attesa viene connesso al process server. Questo fa partire un nuovo processo con il server richiesto, dopo di che si rimette in ascolto per nuove richieste • –Se il server non può essere creato ogni volta ci potrebbe essere un name server (directory server) a cui i server si registrano fornendo il nome del servizio che offrono e il loro TSAP. Il client contatta il name server che è ad una TSAP ben nota e chiede di un certo servizio. Il server risponde con la TSAP

UDP e RFC 768

sabato 9 maggio 2020 11:37



La Source port serve quando devo mandare indietro un reply:

- Copiando il campo Source port del segmento entrante nel campo
- Destination port indica la porta di destinazione
- Il campo UDP length comprende header e dati
- UDP checksum è opzionale e messo a zero se non calcolato – Non conviene disabilitarlo a meno che la qualità dei dati non interessi

RTP

sabato 9 maggio 2020 12:01

Real-time Transport Protocol:

- RFC 1889, nato per unificare i vari protocolli di streaming di contenuti real time multimediali (internet radio, telefonia internet, videconferenza, video on demand, music on demand)
- Normalmente RTP sta nello spazio utente e gira sopra UDP
- Le applicazioni multimediali consistono di diversi stream audio, video o testo, che accedono ad una libreria nello spazio utente.
- La libreria multiplexa gli stream e li codifica in pacchetti RTP e li mette in un socket.
- All'altro lato del socket, stavolta nel kernel del sistema operativo, vengono generati pacchetti UDP