Corso Sistemi e reti

Figura 1 Corso di riferimento: https://www.udemy.com/course/networking-101-corso-di-reti-da-zero

Indice:

Cap. 1 – Introduzione

Nodo: un generico host, un dispositivo connesso alla rete

Link: collegamento fra due nodi effettuabile in vari modi, cablato, wireless, ecc.

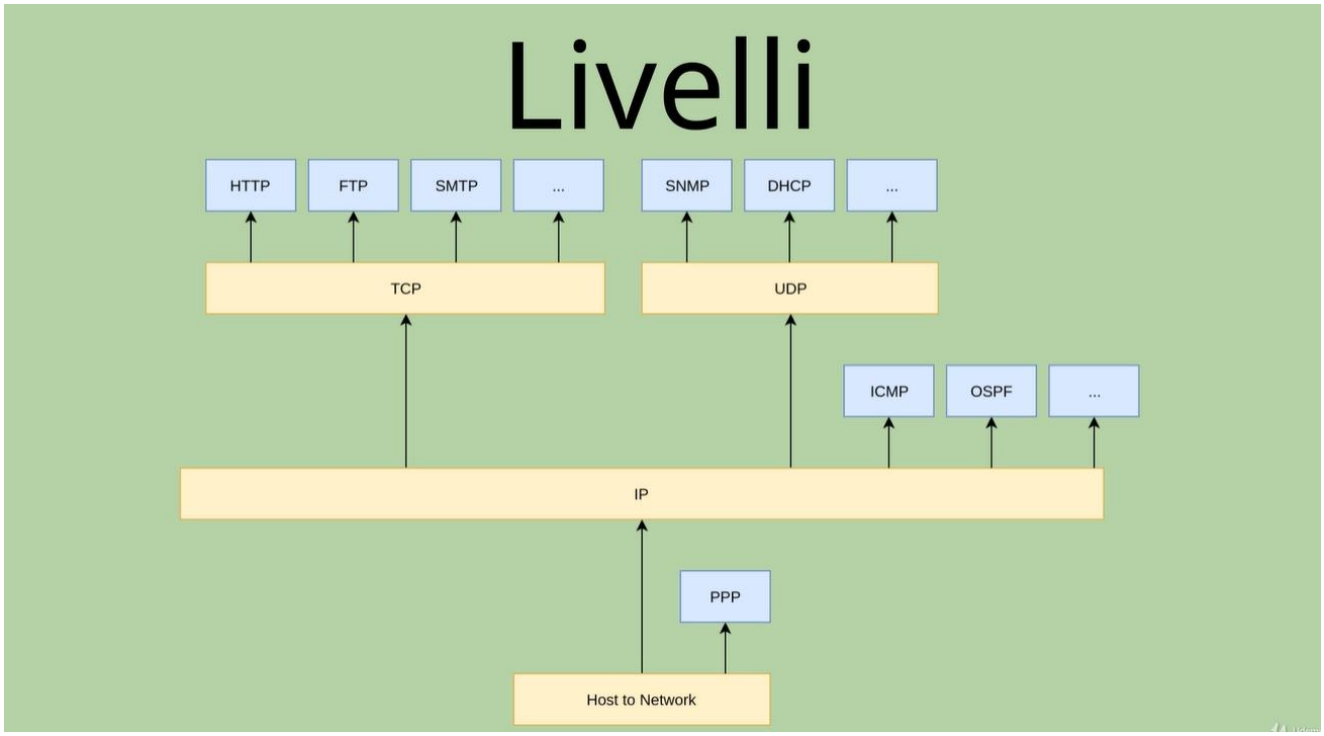
Rete: Insieme di più nodi connessi da link

Tipologia di reti:

- **WAN** (Wide Area Network): Rete di grande estensione, livello regionale, statale o addirittura continentale.
  Estensione: > 1Km
- **LAN** (Local Area Network): Rete locale di breve estensione, può arrivare a livello di un edificio, campus o meno.
  Estensione: **10m < x < 1km**, può avvenire grazie cavi ethernet o/e ponti wifi.
- **PAN** (Personal Area Network): es. Connettività Bluetooth tra uno smartwatch e un telefono.
  Estensione: 1m < x < 10m.

Protocolli: Set di regole che permettono di avere una omogeneità comunicativa tra due/più dispositivi differenti tra loro.

Livelli: sistema di astrazione progressivo che permette di gestire da lato macchina fino a livello più astratto applicativo, la comunicazione tra due dispositivi.



Cap. 2 – Modello ISO-OSI e TCP/IP

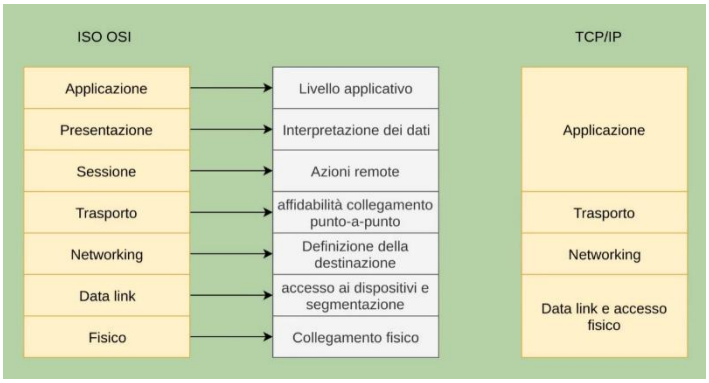
Esistono più protocolli implementati su più livelli.

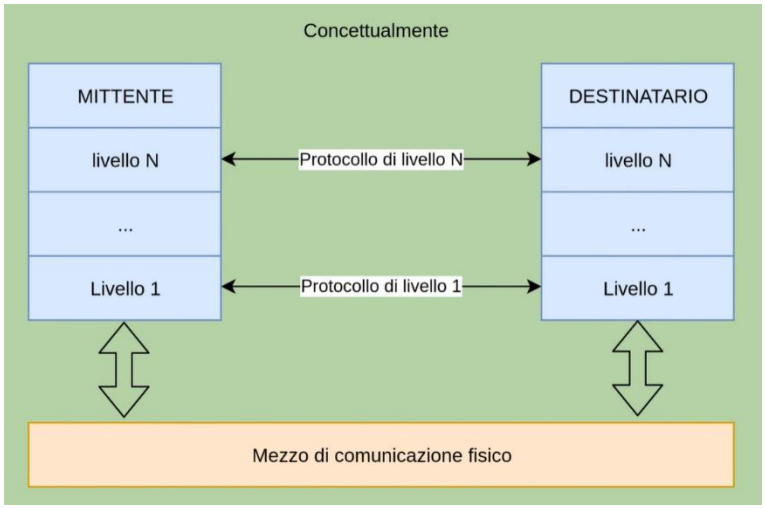
Un modello importante, ma mai praticamente attuato, fu l'**ISO-OSI**, esso è strutturato su **7 livelli**:

Tale modello, avendo una ferrea connessione tra i vari elementi della connessione (dall'applicazione vera e propria, al punto ultimo di connessione, quello fisico) e per motivazione di altro carattere, non venne mai usato.

Il modello tutt'ora in uso, non perfetto, ma funzionale, è il **TCP/IP** (Transmission Control Protocol/ Internet Protocol).

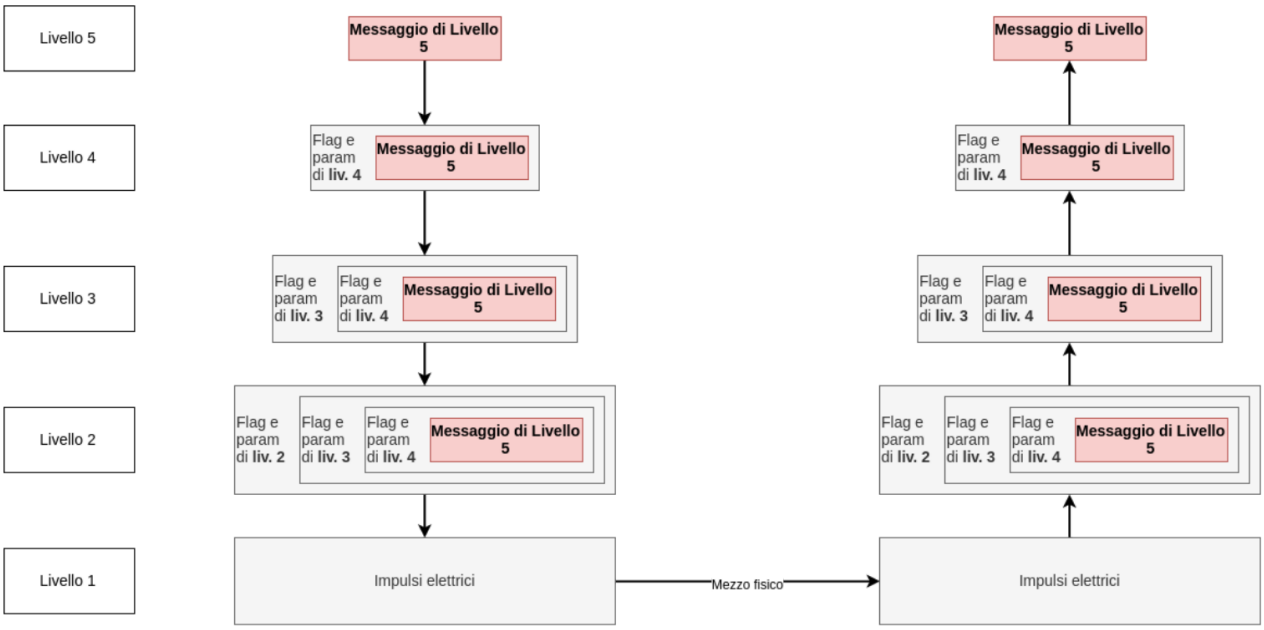
Questo va ad accorpare la parte di Applicazione, Presentazione e Sessione in un unico blocco funzionale, e gestisce in un unico modulo i livelli Data link e Fisico, dando vita a soli **4 livelli** totali.





Il sistema di collegamento tra due client aggiunge, da livello a livello, una serie di layer del dato tali da permette la prosecuzione del passaggio di esso da un livello al successivo che poi, arrivati al destinatario verranno man mano rimossi, così da dare, in fase finale, l'informazione pulita.

Questo viene chiamato **incapsulamento**.



Cap. 5 - Liv. 1 - Mezzi trasmissivi e standard

Le metodologie di connessione alla rete principali sono **via radio** o per **mezzo cablato**.

Wifi: marchio registrato della wifi alliance, che si occupa di certificare che tutti gli utilizzatori rispettino lo standard del gruppo IEEE 802.11.

Il **gruppo IEEE 802.11** si divide in 3 categorie:

Standard 802.11				
Nome	Anche detto	Anno	Frequenza	Velocità teorica
802.11		1997	2.4 GHz	2 Mbps
802.11a		1997	5 GHz	54 Mbps
802.11b		1999	2.4 GHz	11 Mbps
802.11g		2003	2.4 GHz	54 Mbps
802.11n	Wi-Fi 4	2009	2.4GHz & 5GHz	600 Mbps
802.11ac	Wi-Fi 5	2013	5GHz	3.46 Gbps
802.11ax	Wi-Fi 6	2019	2.4GHz & 5GHz	9.6 Gbps

- wifi a
- wifi b
- wifi ac

ecc…

Ognuno di questi è il miglioramento del precedente ed è legato strettamente all'hardware.

Cablato: usa uno standard denominato **IEEE 802.3**, chiamato anche standard **ethernet**.

Queste sono alcune delle famiglie di cablaggi con standard ethernet che vengono usate tutt'ora per attività di varia tipologia.

Standard 802.3

Codice	Standard	Importanti Limitazioni	Velocità
100Base-TX (Fast Ethernet)	802.3		100 Mbps
1000Base-X (Gigabit Ethernet)	Famiglia di implementazioni	(Voci seguenti)	1000 Mbps
1000Base-SX (Fibra ottica multimodale)	802.3z	distanza massima tra 275 m e 550 m	
1000Base-LX (Fibra ottica monomodale)		distanza massima 5 km	
1000Base-T (cavi di rame UTP cat. 5)	802.3ab	distanza massima 100 m	
1000Base-TX (cavi di rame UTP cat. 6)	802.3ab	distanza massima 100 m	

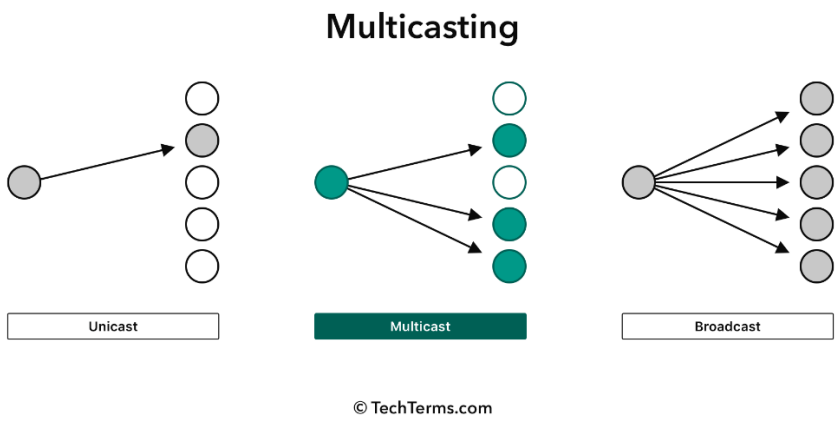
Alcuni dei mezzi fisici utilizzati:

- **Doppino telefonico**: coppia di cavi per cablare una connessione
- **Cavo di rete**: coppia di doppini, che possono essere schermati tra di loro (STP) o non schermati (UTP)
- **Cavo coassiale**: prima versione di ethernet, usato ancora per le tresmissioni televisive
- **Fibra ottica**: ultima versione, performante ma difficile da gestire

Cap. 6 - Liv. 1 - Modalità di trasmissione e modalità di collegamento

Tipologie di trasmissione (metodo):

- **Unicast**: comunicazione tra un mittente e un destinatario (es. un messaggio ad un altro utente)
- **Multicast**: comunicazione tra un mittente e più destinatari (es. un messaggio ad **altri** utenti **prescelti**)
- **Broadcast**: comunicazione tra un mittente e tutti destinatari (es. un messaggio a **tutti** gli utenti)

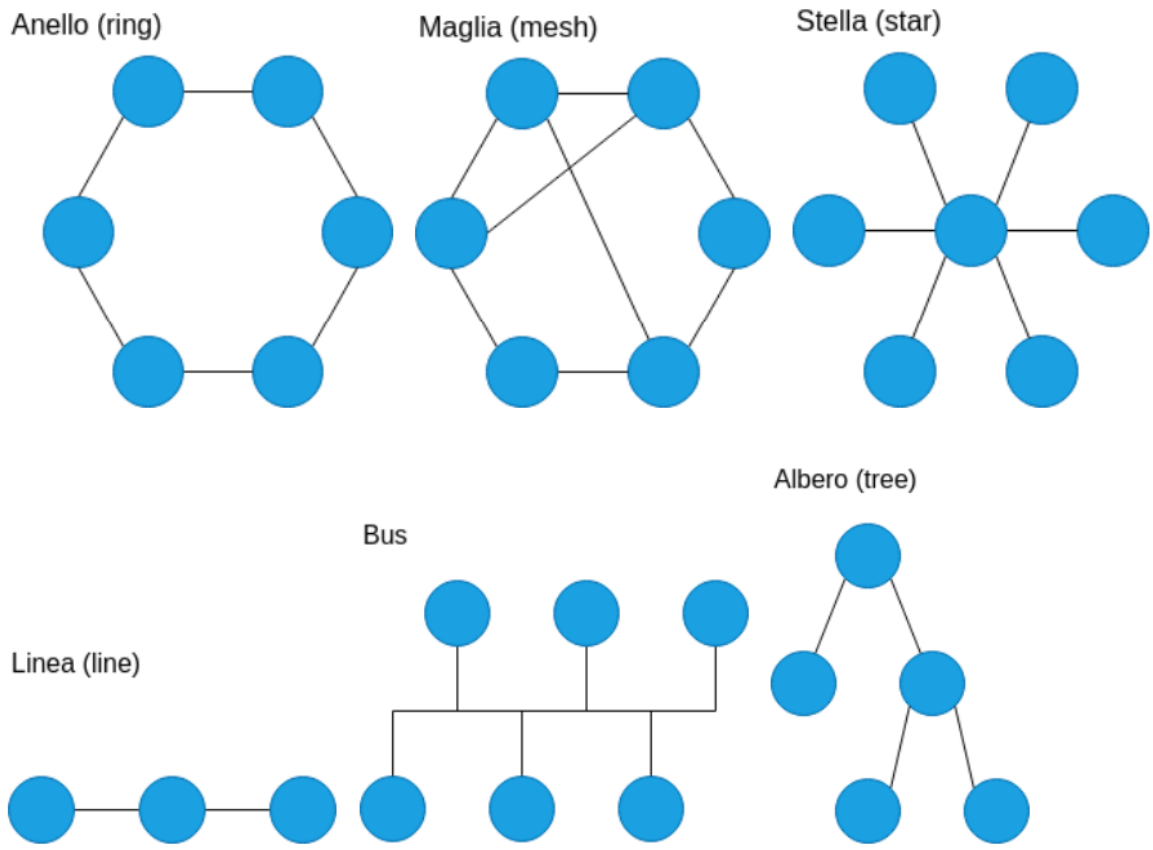


Tipologie di collegamento (supporto fisico):

- **Broadcast**: nodi tutti collegati tra loro (deve essere gestito da algoritmi che deve gestire i segnali, perché può essere distruttivo)
- **PTP** (Punto-punto): un nodo è collegato al successivo (non distruttivo)

Cap. 7 - Liv. 1 - Topologie di rete

- **Anello**: ogni host è collegato al successivo, in un anello
- **Mash** (modello a meglio): come quello sopra, ma con degli archi (link) aggiuntivi tra i vari host
- **Linea**: collegamento in una catena tra host
- **Bus**: sistema di connessione completo, ma presenta collisioni
- **Albero**: in stile gerarchico
- **Stella**: host nodo (uno switch) che veicola da mittente a destinatario il messaggio (più usata e diffusa, anche se complessa)

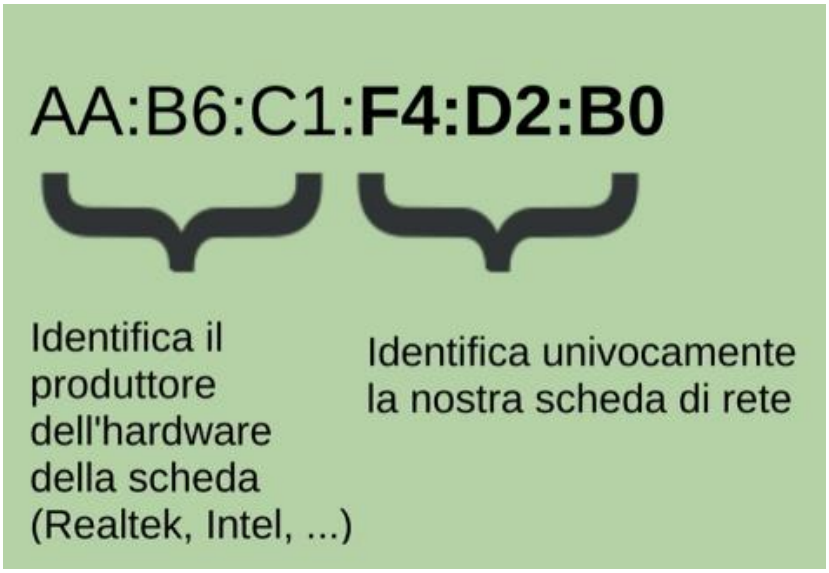


Cap. 10 - Liv. 2 - Cos'è un MAC Address

Il livello 2 affronta le problematiche di interconnessione tra più host, trasmissione dati tra host direttamente connessi e connessione di un host a internet.

Ogni host che si connette ad internet tramite una **scheda di rete**, la **NIC** (Network Interface Card), ogni scheda di rete ha un indirizzo univoco, questo è il MAC Address.

MAC Address (Media Access Control): codice di 48 bit espresso come 6 blocchi **esadecimali** da un byte.



I blocchi sono composti da coppie di lettere/numeri separati da ":".

Essendo cifre esadecimali vanno da **0** a **F** (**0 1 2 3 4 5 6 7 8 9 A B C D E F**).

Le **prime 3 coppie** identificano il **produttore della scheda** di rete (realtek, intel, ecc…), le **altre 3 coppie** identificano univocamente la scheda di rete del **dispositivo**.

Un dispositivo può non avere un IP, ma non può non avere un MAC Address.

A questo livello i messaggi scambiati tra gli host prendono il nome di **Frame Ethernet**

Nota: l'indirizzo **FF:FF:FF:FF:FF:FF** viene usato come **indirizzo broadcast** ed è l'indirizzo limite utilizzabile. Se io mando un frame ethernet a questo indirizzo, tutti gli host lo riceveranno.

E' possibile modificare a livello software il MAC Address in via temporanea.

Cap. 11 - Liv. 2 - Apparati di rete di livello 2: Hub, Bridge, Switch

Apparati di rete:

- **Hub**: è uno sdoppiatore di porte che non ha una logica interna, ma sdoppia solo i frame ethernet che vi transitano dentro.

In caso di reti con più di 2 host, senza una logica di smistamento si presenteranno delle collisioni se la connettività è fatta unicamente con degli hub. In questo caso si dice che il **Dominio di Broadcast** è l'intera rete e che il **Dominio di Collisione** è l'intera rete.

Dominio di Broadcast = Dominio di Collisione

Dominio di Broadcast: Intera rete (perché un messaggio inviato da un host ad un altro arriva comunque a tutti gli altri host)

Dominio di Collisione: Intera rete (perché se c'è una collisione nel mezzo trasmissivo, essendo un unico per tutti quanti gli host tutta la rete è soggetta alla collisioni).

- **Switch**: stesso funzionamento di un hub, ma ha un **sistema di smistamento interno** che evita le collisioni. In questo caso, il pacchetto inviato da un host ad un altro sarà veicolato direttamente al solo host destinatario, a meno che il frame ethernet non sia inviato in broadcast.

Es. **A invia a C**, il messaggio partirà da A e arriverò solo a C. Mentre se l'invio verrà fatto in broadcast, il messaggio arriverà a tutti gli altri host.

In questo caso il **Dominio di Broadcast** è l'**intera rete** mentre il **Dominio di Collisione** è **host to host**.

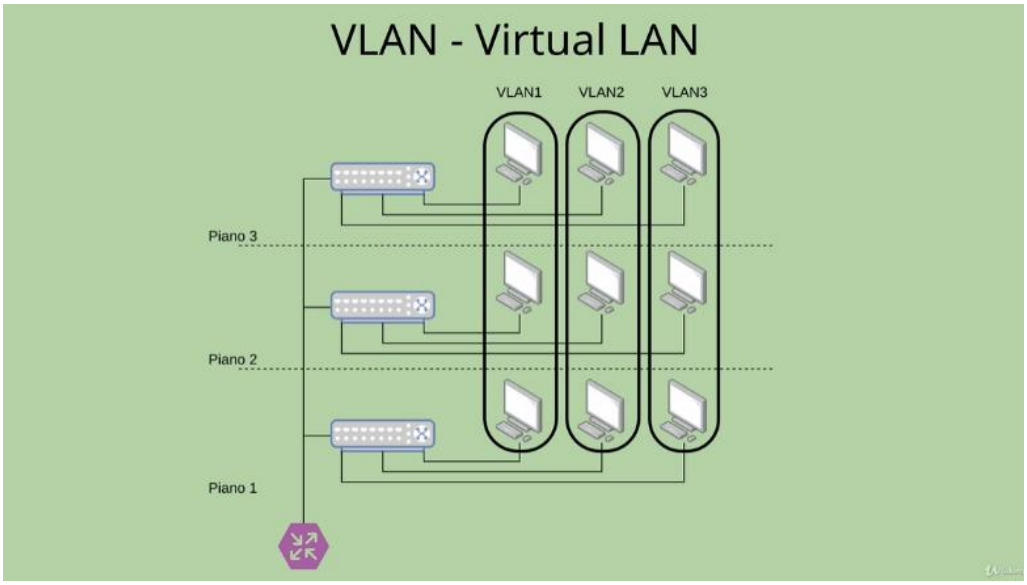
Dominio di Broadcast = Intera Rete | Dominio di Collisione = Host to Host

- **Bridge**: è un dispositivo che può connettere sulla stessa rete logica **2 dispositivi sue reti fisiche diverse** in maniera trasparente.

Es. 2 pc sono collegati ad un modem, uno in modo cablato e un altro in wifi. Questi 2 pc possono comunicare grazie al fatto che il modem funga da switch, per la rete cablata e da bridge verso la rete wifi.

Cap. 12 - Liv. 2 – Cosa è una VLAN

La rete logica deve rispettare la rete fisica?



No, e questo è permesso dalla **Virtual LAN**, che permette di raggruppare gli host in sottoreti differenti.

La **VLAN** viene amministrata dall'amministratore di sistema su gli switch.

Quando configuriamo una VLAN su degli switch, ci sono 2 modi con i quali è possibile configurarla:

- **VLAN Trunk:** Richiede **configurazione lato host**, le regole verranno settate in base IP, MAC, Protollo, ecc…
- **VLAN Access Link: Non** richiede **configurazione lato host**, ma viene effettuato un attacco fisico direttamente lato switch. Naturalmente , collegando il pc ad un'altra porta dello switch, si collegherà ad un'altra porta e quindi ad un'altra VLAN.

Nota: La VLAN è un metodo di collegamento tra host e di setup di una rete, ma non definisce un sistema sicuro e isolato di rete. Un utente malevolo può saltare da una VLAN ad un'altra compiendo atti impropri.

Cap. 13 - Liv. 2 – Accesso residenziale

Per Accesso residenziale si intende il **modo** con il quale la **connettività arriva all'host**.

Il sistema è di tipo **point-to-point** e ha come estremi provider (**ISP**: **Internet Service Provider**) internet e **utente**.

Le **metodologie** di **connettività** più comune sono state:

- **Dial-Up:** Modem a 56K su rete telefonica. **Banda a 56K**.
- **ISDN:** Questa sostituisce la rete telefonica analogica commutata con una linea digitale commutata. **Banda A 128k**.
- **xDSL:** Una famiglia di tecnologie che usa il doppino in rame sia per i dati digitali che per il segnale telefonico analogico, anche se questi 2 segnali viaggiano su 2 bande totalmente diverse. Appartengono ad essa:
  ADSL (Asymmetric Digital Subscriber Line): La più comune, asimmetrica indica che la banda dedicata al download e all'upload è sbilanciata
  HDSL (High Bitrate Subscriber Line): Tipica connessione simmetrica usata in ambito aziendale.
  VHDSL (Very-High Bitrate Subscriber Line): Come sopra, ma ad alto bitrate, bisogna essere a meno di 300m dalla cabina, a causa di problemi di intereferenza.
  Fibra ottica: La più recente e performante.

Il protocollo per stabilire la connettività è il **Protocollo PPP (Point to Point Protocol)**, è un protocollo semplice poiché si stabilisce una connessione punto a punto, ovvero tra il solo host e il provider.

Il **protocollo PPP** è costituito da tali **fasi**:

1) Stabilimento della connessione
2) Autenticazione (facoltativa)
3) Configurazione del protocollo di rete da usare (es. IP)
4) Terminazione della connessione

Esempio e struttura di un **Frame PPP**:

- **Flag**: delimitatore di fine frame
- **Address**: indirizzo del destinatario (essendo solo uno il destinatario, non viene considerato)
- **Control**: impostato ma mai usato
- **Protocol**: protocollo di livello superiore a cui il frame viene passato (Es. IP)
- **Data**: chiamato anche info che è il messaggio di livello superiore
- **Check**: controllo di correttezza (tipo un hash md5, ma più semplice)
- **Flag**: delimitatore di inizio frame

Cap. 16 - Liv. 3 – Scopo del livello IP e Datagram

Ogni host presente sulla rete deve essere identificato da un **indirizzo IP** (Internet Protocol), è assegnato alla scheda di rete, ma non è legato lato harware ad essa. Esso è **modificabile lato software**.

1. **Struttura:**

è un codice composto da **4 gruppi di numeri**.

Ogni blocco è rappresentabile ad 8 bit, per questo ogni blocco va da 0 a 255 **(2^8 = 256)**.

In totale un **IP** è a **32 bit**, ponendo un limitato numero di indirizzi IP, pari a **2^32**.

Per ovviare a questo problema si sta lavorando ad un nuovo standard, l'**IPv6**, successo di IPv4, che lavora con **128 bit**, aumentando di molto il numero di IP disponibili.

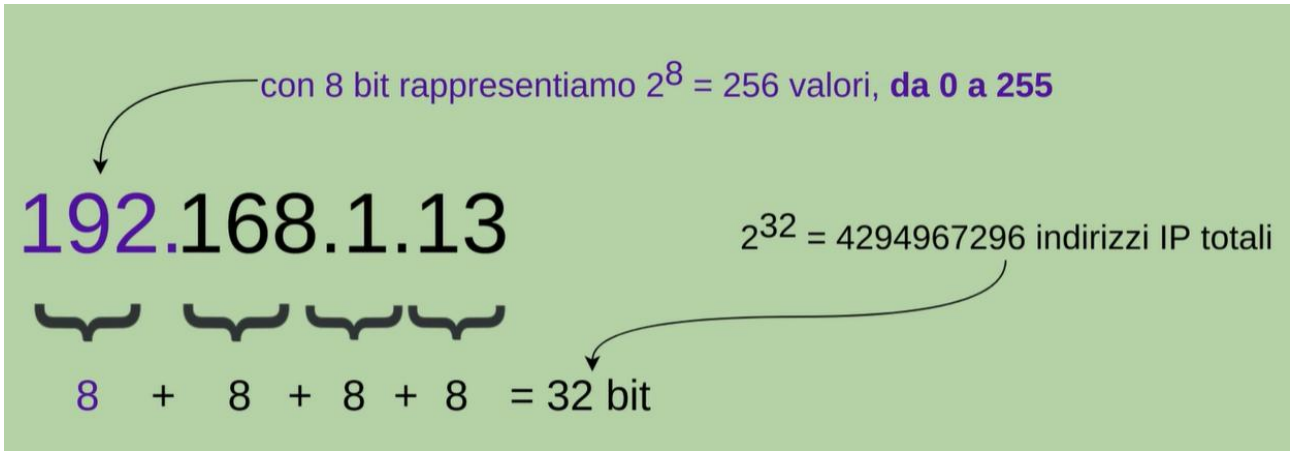
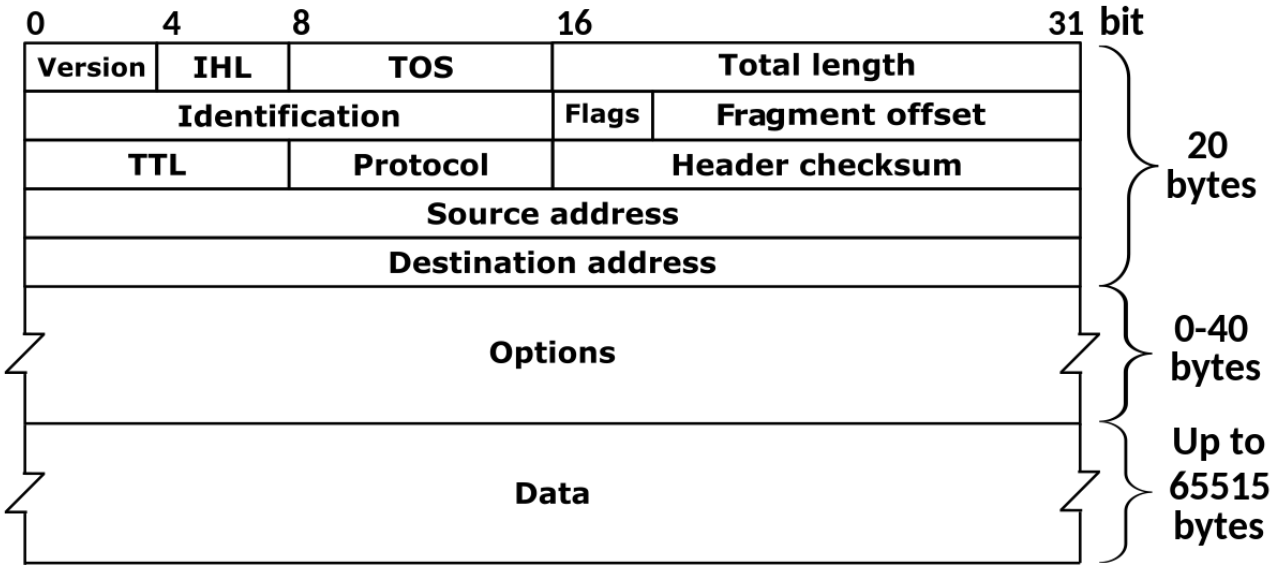


Figura 2 In IPv6 è possibile abbreviare i blocchi composti da più 0 in spazi vuoti Es.: fe80:0000:51e1: … fe80::51e1: …

A questo livello il frame di passaggio del dato prende il nome di **Datagram IP**, con tale **struttura**:



Ogni campo ha una funzione, esempio:

- **Vers**: indica la versione del protocollo, può contenere un **4** o un **6**
- **Len**: lunghezza delle header
- **Total length**: lunghezza totale del datagram
- **Identification**: identificativo del datagram
- **TTL**: tempo di **expiration** del datagram, decresce ad ogni passaggio di un router. A 0 il datagram non verrà più fatto passare e morirà, eviterà un possibile ciclo infinito.
- **Protocol**: quale protocollo applicativo può usare i dati trasportati da questo frame
- **Header Checksum**: controllo di **integrità** dei dati dell'header
- **Source address** e **Destination address**: indirizzo di **sorgente** e **destinazione** attraverso cui passa il datagram
- **Data**: i dati veri e propri, con incapsulamento

2. Bandwith: La metrica di **prestazione** per il trasferimento dati è detta **Bandwith** (larghezza di banda), indica la quantità di dati trasmessi in intervallo di tempo.

Es. 1Kbps → 1 kilo**bit** per secondo

3. Routing: Scelta del **percorso** di un **pacchetto** per andare da un **host A** ad un **host B**.

Il protocollo IP si occupa di una consegna non affidabile, non è garantita e senza controllo della connessione, per evitare latenze e che sono ad appannaggio a livelli successivi.

Tabella riassuntiva delle classi di indirizzamento

		Utilizzo bit (N: Network; H: Host)	Maschera di sottorete	Reti disponibili	Host disponibili per rete	Range decimale primo byte	Range binario primo byte	Note	Indirizzi totali
Classe	A	0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH	255.0.0.0 /8	126 (2^7-2) (1° ottetto)	16.777.214 (2^{24}-2)	0-127 = 128 indirizzi	00000001 - 01111111	Loopback address	2.147.483.646 (2^{31}-2)
	B	10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH	255.255.0.0 /16	16.382 (2^{14}-2) (1° e 2° ottetto)	65.534 (2^{16}-2)	128-191 = 64 indirizzi	10000000 - 10111111		1.073.741.822 (2^{30}-2)
	C	110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH	255.255.255.0 /24	2.097.150 (2^{21}-2) (1°, 2° e 3° ottetto)	254 (2^8-2)	192-223 = 32 indirizzi	11000000 - 11011111		536.870.910 (2^{29}-2)
	D	1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX		non definito	non definito	224-239 = 16 indirizzi	11100000 - 11101111	Indirizzo multicast	non definito
	E	1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX		non definito	non definito	240-255 = 16 indirizzi	11110000 - 11111111	Per usi futuri ed esperimenti	non definito

Cap. 17 - Liv. 3 – Il Protocollo ARP

Protocollo ARP: Address Resolution Protocol

Ogni host su internet deve essere univocamente definito da un IP.

Ma questo passaggio non avviene in modo diretto, considerata la struttura della rete, ponendo degli host intermediari chiamati **next hop**, che passeranno il datagram all'host finale.

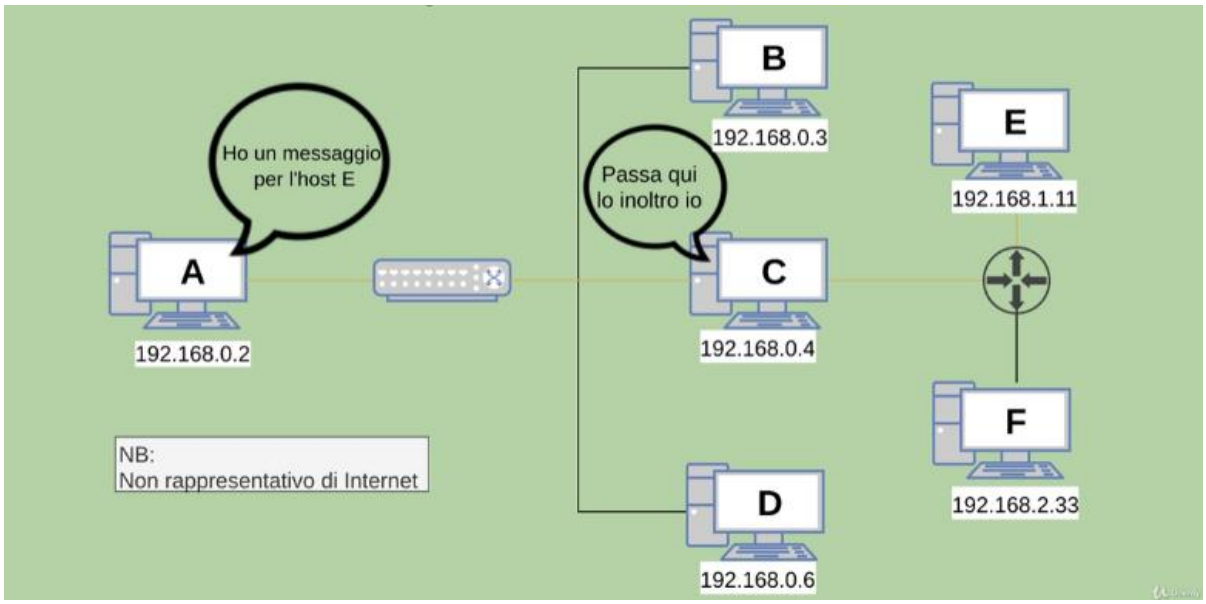


Figura 3 Se l'host A deve inviare un messaggio all'host E, dovrà prima passare per C, unico suo punto di connessione nella rete. Questo problema viene gestito con il Routing.

Problema: Se 2 host comunicano tramite indirizzi MAC, come faranno 2 host a comunicare tra loro tramite gli indirizzi IP? Dovrebbe conoscere il MAC address associato a quell'indirizzo IP.

Soluzione: Qui entra in gioco il protocollo ARP.

A invierà il messaggio in **broadcast** (FF:FF:FF:FF:FF:FF) a tutti, gli risponderà unicamente C, che ha l'indirizzo IP cercato da A.

A questo punto A memorizzerà l'associazione tra indirizzo IP e Indirizzo MAC associato e dovrà fare la stessa cosa con tutti gli host con i quali vorrà comunicare.

L'elenco di tali associazioni è conservato nella **ARP Cache** (o ARP Table), visualizzabile nel prompt dei comandi usando il comando **arp -a**.

```
C:\Users\giacomo.borsellino>arp -a

Interfaccia: 192.168.5.152 --- 0x6
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.5.1           6c-3b-6b-fe-85-3a     dinamico
  192.168.5.8           00-15-5d-05-e0-00     dinamico
  192.168.5.9           00-15-5d-05-e0-01     dinamico
  192.168.5.101         00-15-5d-05-e0-02     dinamico
  192.168.5.118         00-15-5d-05-e0-04     dinamico
  192.168.5.151         6c-ad-f8-9d-1d-a2     dinamico
  192.168.5.164         e0-70-ea-d3-6c-93     dinamico
  192.168.5.176         00-15-5d-05-e0-03     dinamico
  192.168.5.255         ff-ff-ff-ff-ff-ff     statico
  224.0.0.22            01-00-5e-00-00-16     statico
  224.0.0.251           01-00-5e-00-00-fb     statico
  224.0.0.252           01-00-5e-00-00-fc     statico
  239.255.255.250       01-00-5e-7f-ff-fa     statico
  255.255.255.255       ff-ff-ff-ff-ff-ff     statico
```

Questa contiene tutte le associazioni fatte in quel momento.

Un attacco hacker mirato a questo protocollo è lo **spoofing**.

Naturalmente non è statica, ma cambia con il cambiare degli indirizzi IP e delle relative associazioni.

Cap. 18 - Liv. 3 – Indirizzi IP e classi

L'indirizzo IP è un codice unico e compatto che contiene 2 informazioni:

1) **Nome della rete (Net ID)**
2) **Singolo Host (Host ID)**

192.168.1.13

Nota: Ma questa suddivisione non è una regola fissa

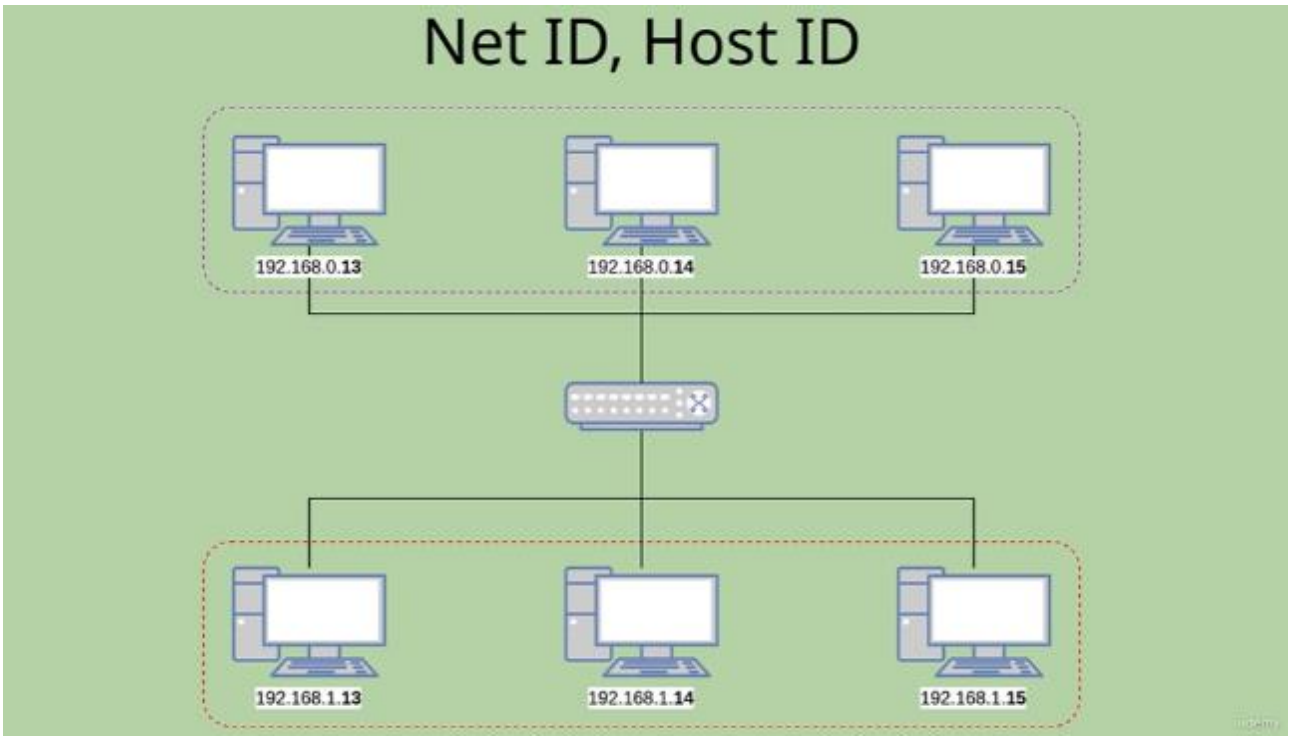
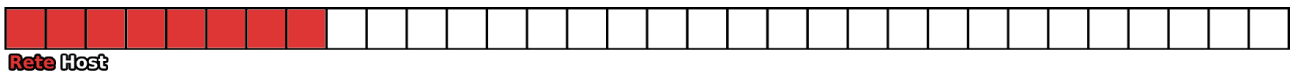


Figura 4 Ogni computer può comunicare con un computer appartenete ad una stessa rete, non appartenente ad una rete diversa.

È possibile **ripartire** queste **parti** differentemente, seguendo un sistema a **classi**:

- **Classe A**: 192.**168.1.13**/8
  Primi **8 bit** indicano la rete e i restanti l'host. **Netmask** = **8**



- **Classe B**: 192.168.**1.13**/16
  Primi **16 bit** indicano la rete e i restanti l'host. **Netmask** = **16**

- **Classe C**: 192.168.1.**13**/24 (tipica casalinga con max 254 dispositivi)
  Primi **24 bit** indicano la rete e i restanti l'host. **Netmask** = **24**

Sommando gli **ottetti** usati per indicare la **rete** otterremo la **Netmask** (o **Subnet Mask**).

Esiste una notazione alternativa per descrivere la netmask, fatta **esplicitando i bit**:

192.168.1.13/24 → 192.168.1.13/**255.255.255.0**

192.168.1.13/16 → 192.168.1.13/**255.255.255.0.0**

192.168.1.13/8 → 192.168.1.13/**255.255.255.0.0.0**

Solitamente i **modem casalinghi** arrivano configurati con un prefisso di rete a **24 bit**, quindi una rete di classe c.

Questo permetterà di avere fino a 256 indirizzi, anche se quelli realmente disponibili sono **254**, visto che lo **0** e il **255** sono riservati (0 al nome della rete senza specificare l'host e 255 per il **broadcast**).

Se per caso volessimo usare più host potremmo usare una rete di classe b, dove la netmask è 16 (255.255), quindi avremmo

Totali: 192.168.0.0 → 192.168.255.255

Utilizzabili: 192.168.0.1 → 192.168.255.254

Quindi avremmo **65634** (2^16 - 2) host disponibili.

L'IP è assegnato alla **scheda di rete** dell'host.

Se abbiamo più schede di rete, avremo più IP possibili.

L'IP può essere assegnato **dinamicamente** o **staticamente** lato software.

- **IP Dinamico**: Nel primo caso verrà assegnato dal **server DHCP** (spesso già installato nei nostri modem, router, ecc…) a cui è collegato l'host.
- **IP Statico**: Nel secondo caso verrà **configurato** sull'host.

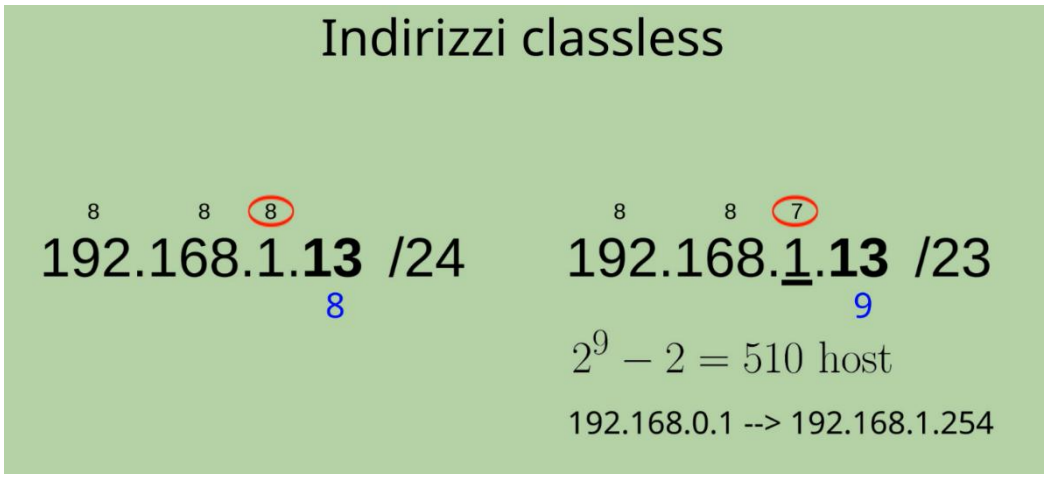
Indirizzi IP Speciali:

- **127.0.0.1**: indica **localhost**
- **0.0.0.0**: indica tutti gli indirizzi IP dell'host e **non è valido**
- **192.168.1.255**: Indirizzo di **broadcast** della rete 192.168.1.0
- **255.255.255.255**: Indirizzo di **broadcast** della rete in cui siamo (utilizzabile se non sappiamo il nostro prefisso di rete, che in questo caso è 192.168.1)
- **Classe D e Classe E**: IP usati rispettivamente per il multicast (da 224.0.0.0 a 239.255.255.255) e per esperimenti futuri (da 240.0.0.0 a 255.255.255.254)

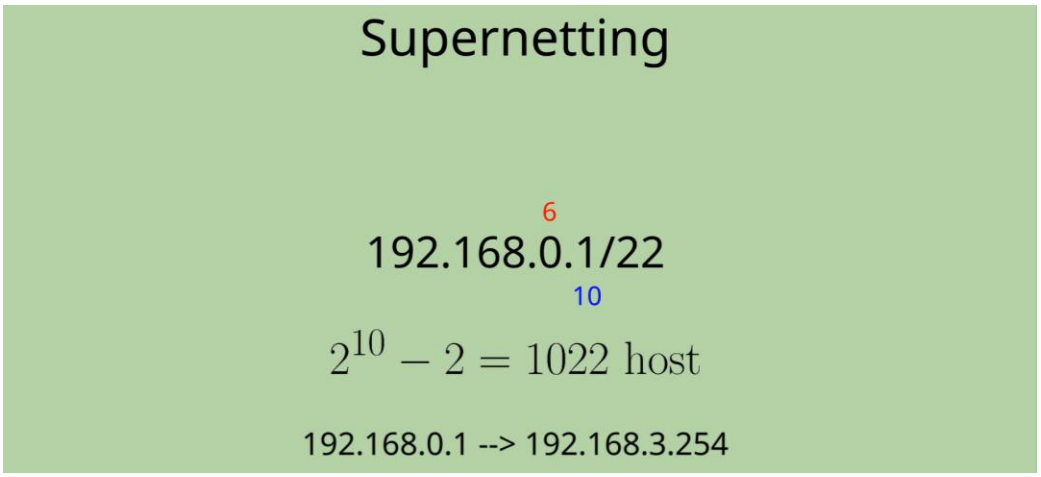
Cap. 20 - Liv. 3 – CIDR, Subnetting e Supernetting

Essendo le classi molto rigide e ponendo dei range di numero di host abbastanza ampi, si è deciso di poter definire delle **infraclassi** tali da poter, variando la disponibilità di bit per gli host, scegliere un numero di host predefinito e **intermedio**:

Es.: **Netmask** a **23 bit**



Es.: **Netmask** a **22 bit**

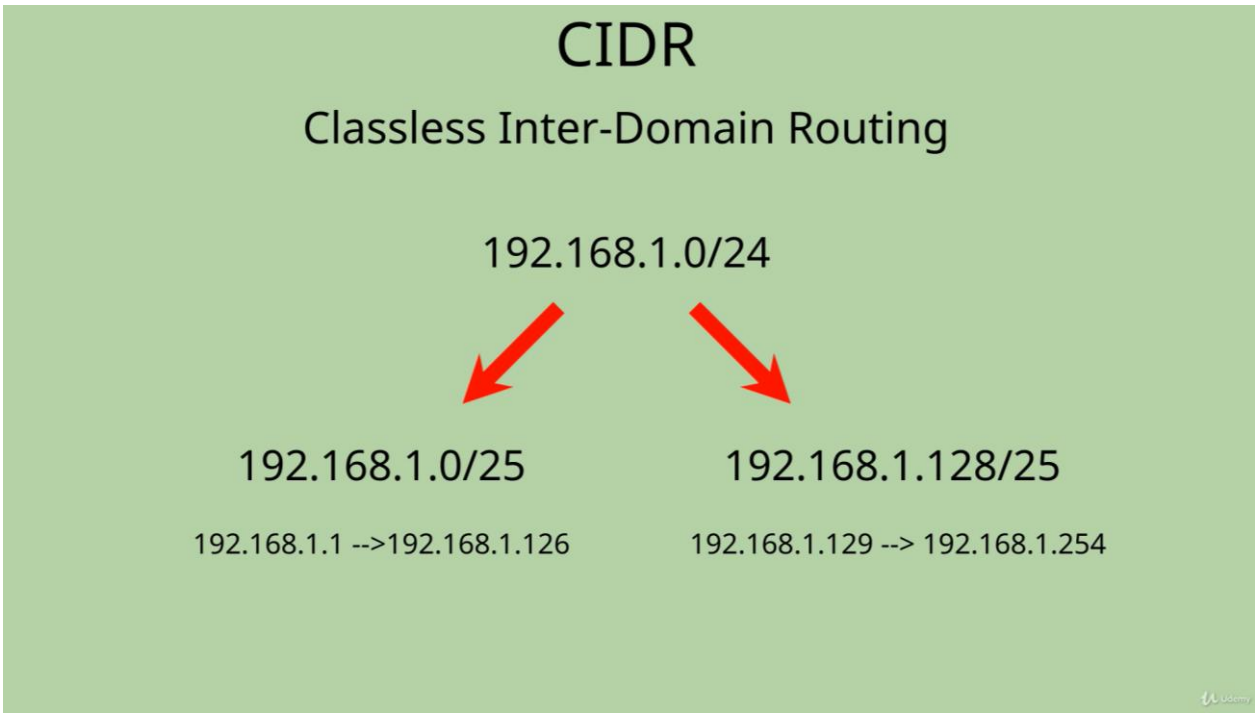


Questa pratica è il **Supernetting**.

È possibile calcolare il numero usando uno strumento chiamato **ipcalc** (installabile su cmd o altrove online).

Il processo inverso è il **Subnetting**.

Ad esempio, nel caso sotto abbiamo scisso una rete a 24 bit in 2 da 25, da 126 host ciascuna



La notazione a **slash** utilizzata è denominata **CIDR** (**Classless Inter-Domain Routing**).

Cap. 22 - Liv. 3 – NAT (Network Address Translation)

Problema: indirizzi troppi pochi

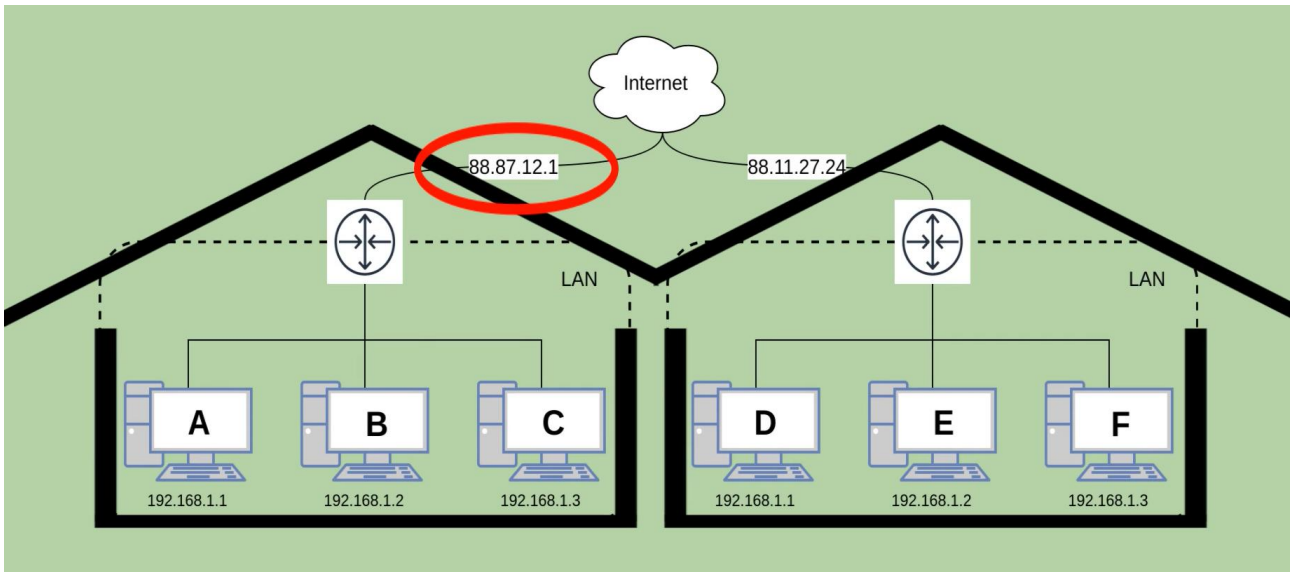
Soluzione: **IANA** ha permesso lo stanziamento di un range di ip locali ad uso domestico che non richiedono autorizzazione.

Questi indirizzi sono “non-rootable”, ovvero vengono scartati da tutti i router su internet.

Indirizzi **Non-Rootable** possono essere di classe A, B o C

Classe A:	[10.0.0.0 - 10.255.255.255]	(10.0.0.0**/8**)	- 1 rete
Classe B:	[172.16.0.0 - 172.31.255.255]	(172.16.0.0**/12**)	- 16 reti
Classe C:	[192.168.0.0 - 192.168.255.255]	(192.168.0.0**/16**)	- 256 reti

Indirizzi Ip per definire devices ad uso interno e che poi verrano identificati esternamente da un unico indirizzo, quello del router.



Questo evita il consumo di IP ed essendo un tipo di rete “semi-privata” evita che gli host siano **direttamente** esposti alla rete.

Flusso:

Un device invia un messaggio ad un sito.

→

L’host invia un datagram verso il router, il datagram ha come ip quello dell’host, poi questo ip viene cambiato in quello del router e, con il next-hop, invia il datagram al sito.

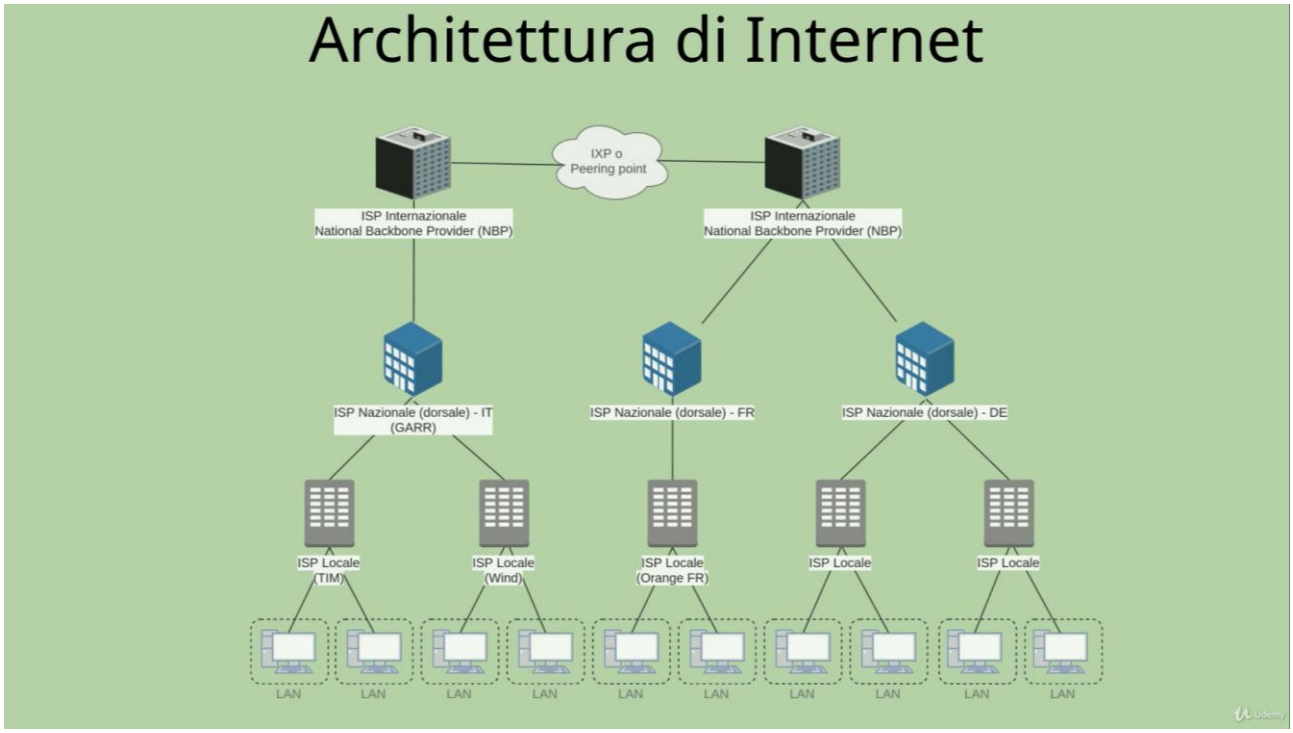
Questo processo di traduzione dell’ip locale a quello del router per l’invio verso l’esterno è il **NAT**

←

Il sito risponde comunicando al router, che ha immagazzinato l’ip del device e gli restituisce la risposta.

Questo processo di traduzione dell’ip del router a quello del device locale per la risposta verso l’interno è il **Source Natting**.

Cap. 23 - Liv. 3 – L'infrastruttura di Internet



LAN (pc)

|

+--- ISP Locale (es. TIM)

|

+--- ISP Nazionale (GARR)

|

+--- ISP Internazionale (NBP)

|

+--- **IXP** ** o **Peering Point** *

Internet è un **Autonomous System (AS)**, ovvero un insieme di sistemi che usano medesimi protocolli, questi sistemi sono isolati da altri, creando dei sottosistemi. Questi non possono gestire più del 5% del flusso di rete.

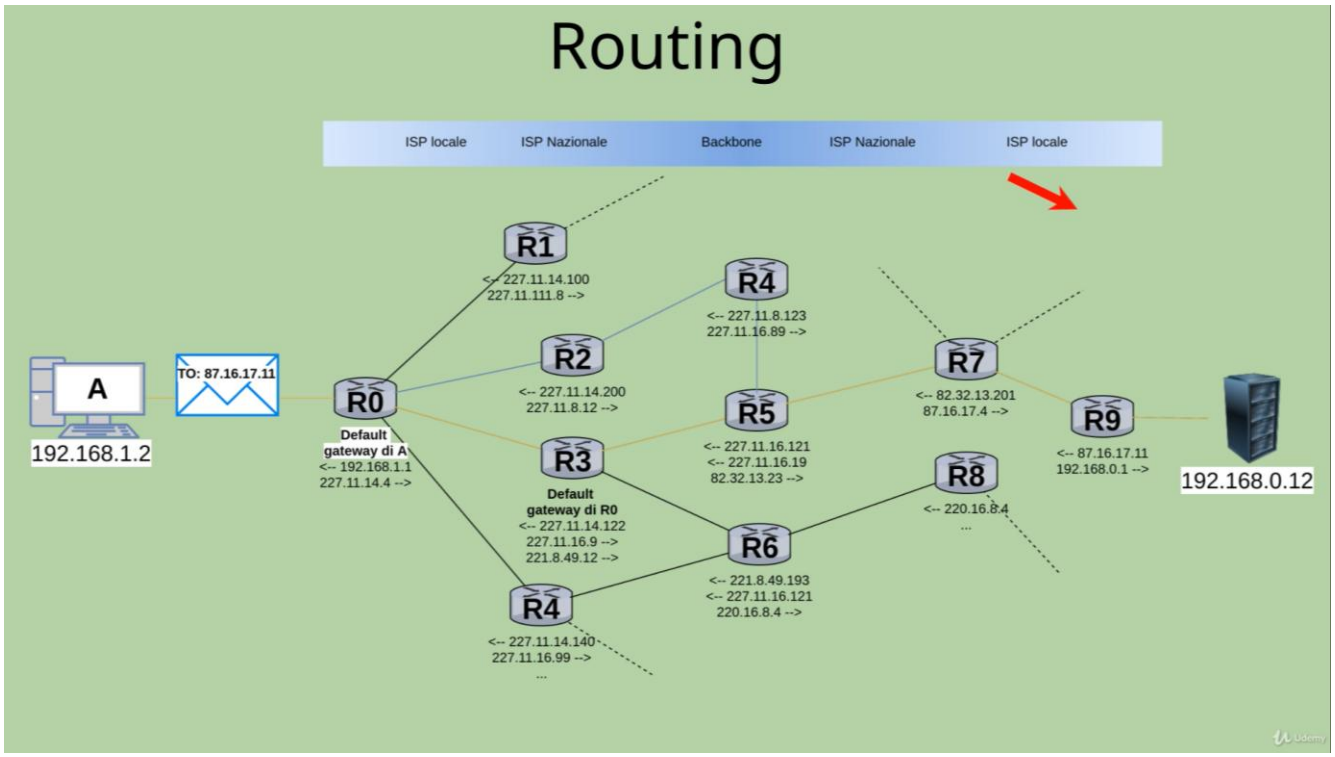
- **Peering Point** *: in questo caso gli AS possono dividere equamente o in modo sproporzionato le spese di gestione del sistema.
- **IXP** **: Internet Exchange Point, consorzi indipendenti senza scopo di lucro spesso supportati da finanziamenti pubblici, es. **superNAP** di Las Vegas

Cap. 24 - Liv. 3 – Router e Routing

Il router interconnette 2 reti separate.

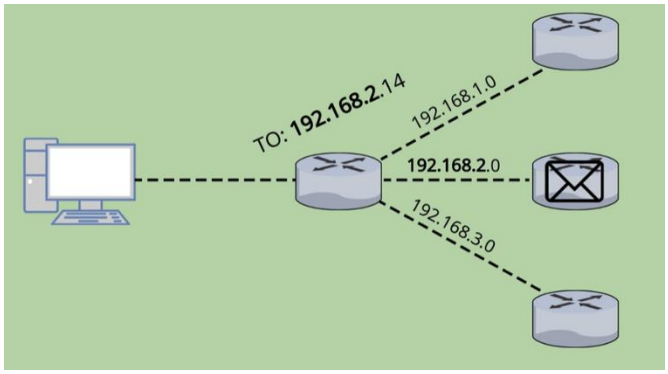
Lo scopo del riuting è decidere il percorso che il pacchetto deve fare per raggiungere un altro host.

Visto che il mio pc non sa con chi interfacciarsi, questo si interfaccerà con il **default gateway**, ovvero il router di default (lo scatolotto del provider, es, TIM). Se questo non saprò dove indirizzarlo, lo manderà ad altri router, e così via, fino a che non ce ne sarà uno che lo saprà, controllando la lista dei suoi routing



Flusso:

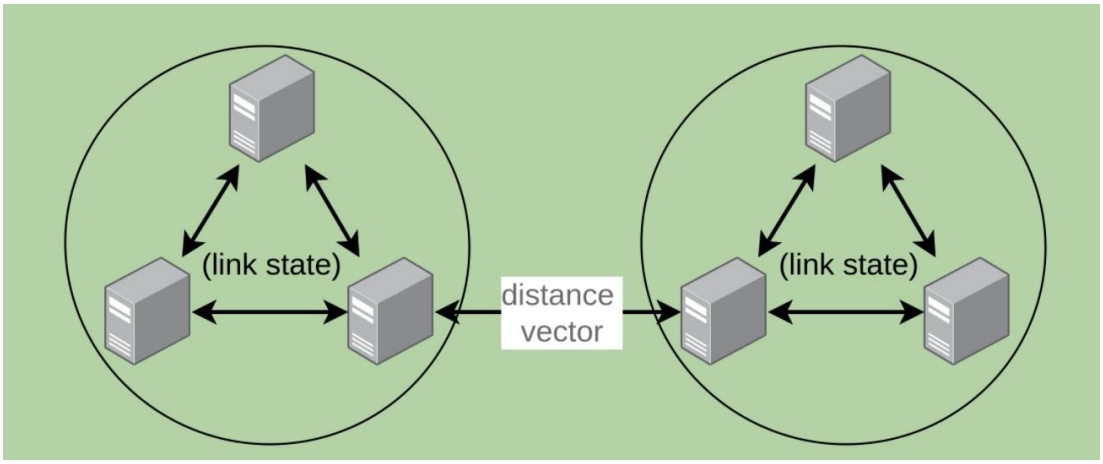
1. PC invia **messaggio**
2. Router estrae dall'header del **datagram** l'ip del **destinatario**, prendendo il **prefisso di rete**
3. Il router (dafault gateway) ha una lista e invia all'altro router che ha prefisso di rete desiderato
4. È possibile che ci siano più vie possibili



5. Visto che è possibile che si formi un loop di invio tra i vari routers, il datagram dispone di un parametro **TTL**, che sarebbe il tempo di **expiration** del datagram stesso, così, ad un certo numero di passaggi, il **datagram** scadrà e non verrà più inviato.
6. Il calcolo del percorso da seguire è definito dagli **algoritmi di routing**

Algoritmi di Routing

- **Globale**: Tutti i nodi conoscono lo stato dell'intera rete (es. Link State Protocol)
- **Locale**: un nodo comunica solo con i nodi vicini a sé (es. Distance Vector Protocol)



I Globali sono usati negli Autonomous System, i locali per le interconnessioni tra i 2.

Es. su windows è possibile vedere la tabella di routing con il **comando**:

route PRINT

```
Prompt dei comandi
C:\Users\[redacted]>route print
===========================================================================
Elenco interfacce
  9...6c 02 e0 94 9e dd ......Realtek PCIe GbE Family Controller
  6...b0 22 7a c3 39 a5 ......Realtek USB GbE Family Controller
 14...00 ff 73 82 40 07 ......TAP-Windows Adapter V9
 21...40 1c 83 eb 14 9b ......Intel(R) Wi-Fi 6 AX201 160MHz
 22...40 1c 83 eb 14 9c ......Microsoft Wi-Fi Direct Virtual Adapter
 18...42 1c 83 eb 14 9b ......Microsoft Wi-Fi Direct Virtual Adapter #2
 13...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete            Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0      192.168.5.1    192.168.5.155     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.5.0    255.255.255.0         On-link     192.168.5.155    281
    192.168.5.155  255.255.255.255         On-link     192.168.5.155    281
    192.168.5.255  255.255.255.255         On-link     192.168.5.155    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.5.155    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.5.155    281
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  1    331 ::1/128                  On-link
  6    281 fe80::/64                On-link
  6    281 fe80::896f:6a56:41e7:1dae/128
                                    On-link
  1    331 ff00::/8                 On-link
  6    281 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna

C:\Users\[redacted]>
```

Cap. 25 - Liv. 3 – Protocollo ICMP

ICMP: Internet Control Message Protocol

È un protocollo usato per il controllo della diagnostica di base delle reti.

Ha una serie di **codici descrittivi**:

- **0** Destination network unrechable
- **1** Destination host unrechable
- **2** Destination protocol unrechable
- **3** Destination port unreachable

ecc…

Di base il protocollo ICMP **serve** a

- Controllare flussi dei datagram
- Determinare cicli o cammini troppo lunghi
- Misurare la latenza tra un mittente e un destinatario

Alcuni strumenti che usano questo protocollo sono

- **Ping**

commando: es. `ping google.com`

Questo invia pacchetti in (**echo request**) e riceve delle risposte (**echo reply**)

Nota: i tempi di risposta comprendono sia andata che ritorno del pacchetto (**RTT – Round Trip Time**)

- **Trace Route**

Commando: es. `tracert google.com`

Questo traccia il percorso di routing di un pacchetto

```
Traccia instradamento verso google.com [142.251.143.174]
su un massimo di 30 punti di passaggio:

  1     1 ms    <1 ms    <1 ms  192.168.5.1
  2    18 ms    20 ms    19 ms  100.64.0.61
  3    19 ms    18 ms    19 ms  213.233.30.150
  4    19 ms    19 ms    19 ms  100.64.0.138
  5    18 ms    20 ms    20 ms  195.250.254.161
  6    22 ms    22 ms    19 ms  213.233.30.149
  7    20 ms    29 ms    20 ms  194-183-16-217.uni.it [194.183.16.217]
  8    27 ms    27 ms    26 ms  google.rom.namex.it [193.201.28.86]
  9    30 ms    31 ms    31 ms  192.178.104.99
 10    29 ms    31 ms    30 ms  192.178.104.104
 11    34 ms    33 ms    33 ms  142.251.243.55
 12    36 ms    37 ms    36 ms  142.251.238.205
 13    34 ms    35 ms    31 ms  142.251.241.27
 14    32 ms    33 ms    32 ms  trn06s03-in-f14.1e100.net [142.251.143.174]

Traccia completata.
```

Nota: alcuni router possono declinare echo reply perché hanno disabilitato il protocollo ICMP

Esempio di **datagram ICMP incapsulato**

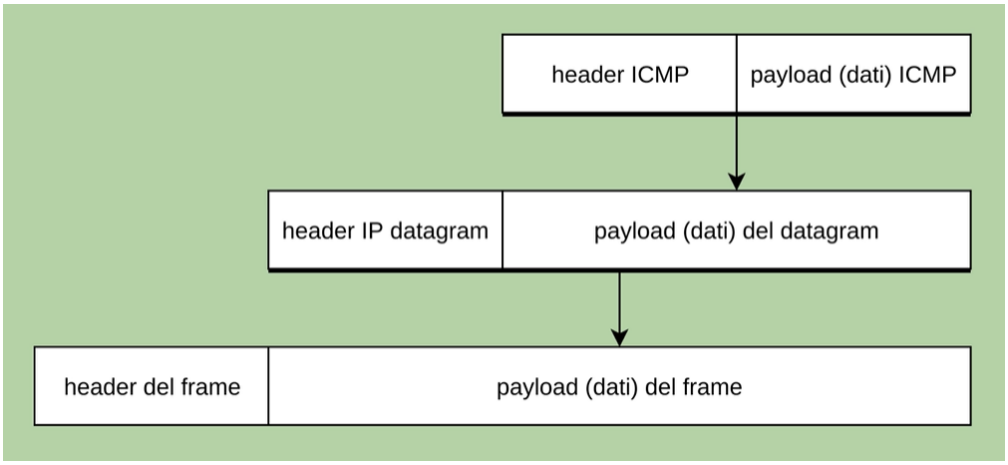


Figura 5 header icmp incapsulato in un datagram ip incapsulato, a sua volta, in un frame ethernet

Cap. 26 - Liv. 3 – Gestione degli indirizzi IP

Un po' di storia

1986 In USA venne creata **IANA**, da Jon Postel

IANA aveva la giurisdizione sugli indirizzi IP, questi venivano distribuiti da **InterNIC.**

A **livello locale** un provider aveva un tange di indirizzi, dati da InterNIC.

1998 In USA IANA e InterNIC vengono subordinate e controllate da ICANN, un ente internazionale, che fa gestire a IANA l'allocazione degli indirizzi IP, insieme ai Regional Internet Registry (RIR), gli organi continentali di gestione degli indirizzi IP.