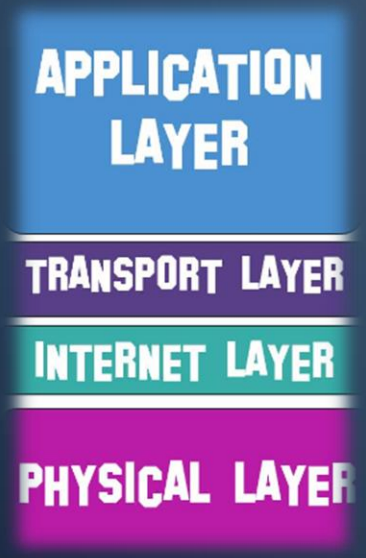
LIVELLO 2: INTERNET LAYER

(VER. 2023)

FONTI:

- E. Baldino, R. Rondano, A. Spano, C. Iacobelli, «Internetworkong sistemi e reti», Juvenilia
- https://it.wikipedia.org/
- https://www.disi.unige.it/person/CostaG/smid_03/dispense_et_al/informatica_generale/reti_internet/2_internet.ppt

LIVELLO INTERNET (O NETWORK)



Il livello internet o network ha due compiti:

- Instradare end-to-end (cioè da un mittente ad un destinatario) i messaggi utilizzando un mezzo come la rete (intesa in senso esteso, quindi un insieme di reti con caratteristiche diverse) dove i trasferimenti sono broadcast (cioè a tutti i terminali in ascolto) e il cammino non è unico
- localizzare eventuali instradamenti alternativi in caso di guasti

N.B. Il protocollo si concentra solo sull'invio del singolo pacchetto e non fa alcun tipo di controllo sulla ricezione che viene fatto eventualmente dal transport layer (protocollo TCP)

Per esempio, l'internet layer non garantisce, né controlla l'ordine di arrivo dei pacchetti (anche questo controllo viene eventualmente eseguito dal transport layer)

IL PROTOCOLLO DI RETE IP

Il protocollo di rete a livello di network più conosciuto e usato è certamente l'**Internet Protocol** (IP) proposto nel 1981

È un protocollo connectionless (senza connessione) e quindi consente a due host di scambiarsi pacchetti (chiamati IP datagram) senza stabilire una sessione (cioè senza verificare l'effettiva presenza in rete del ricevitore) e verificare se il pacchetto è arrivato a destinazione

- L'effettiva garanzia che il pacchetto sia arrivato è garantito dal livello superiore (livello transport) per esempio dal protocollo TCP

Ogni DTE della rete è caratterizzato da un unico indirizzo IP (è come un'indirizzo di un'abitazione)

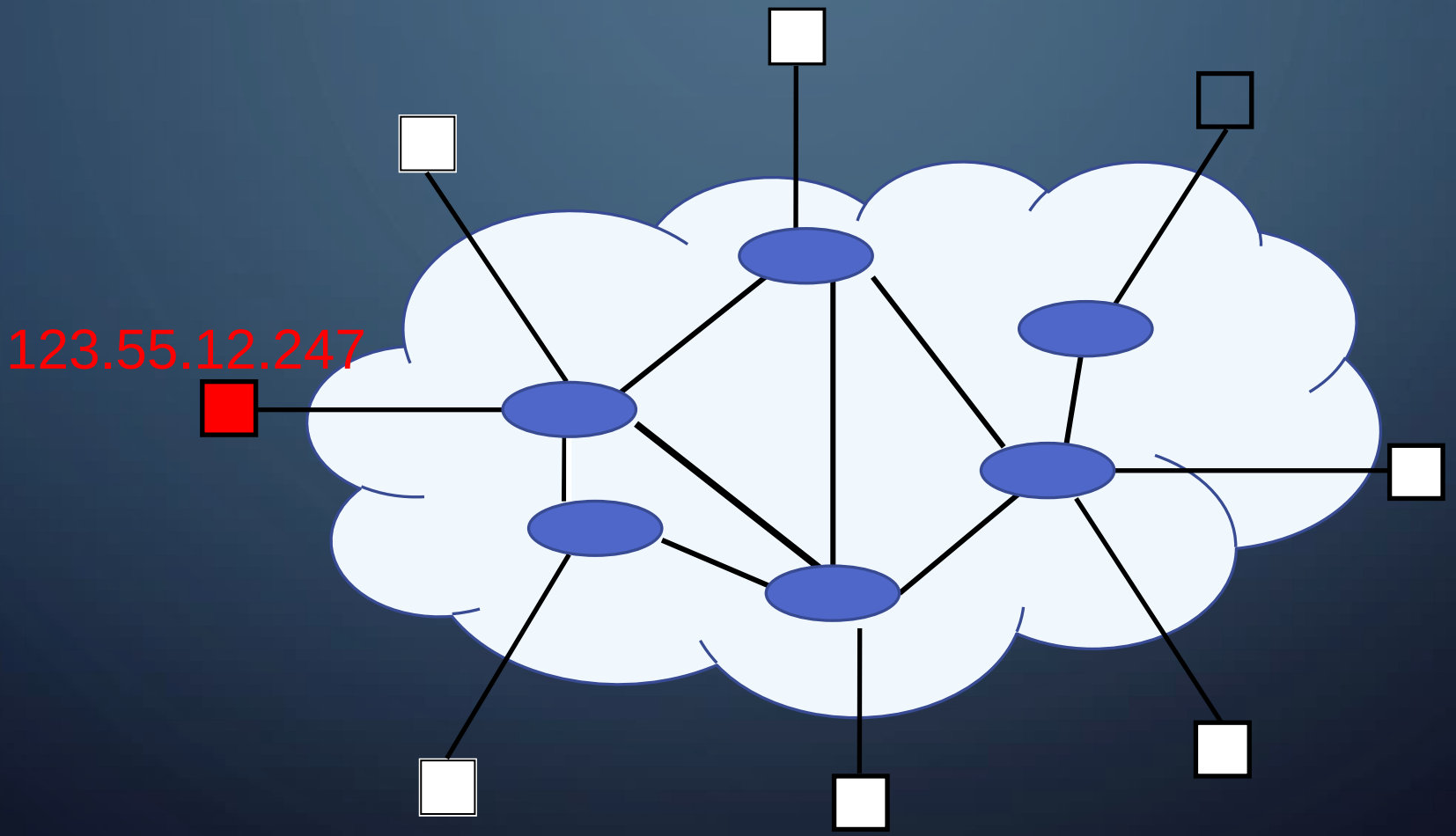
- RICORDA: Mentre **l'indirizzo fisico MAC** è univoco a livello mondiale, **l'indirizzo logico IP** è univoco solo nell'ambito della rete su cui il terminale (host) è operante

Il protocollo IP determina il miglior cammino (detto routing ovvero instradamento) per l'attraversamento della rete attraverso la consultazione delle tabelle di instradamento

- Tali tabelle possono essere di tipo statico (realizzate manualmente dai gestori della rete) o dinamico (composte con l'utilizzo di protocolli di routing tipo l'OSPF, il RIP o il BGP che servono a popolare tali tabelle scambiando tra i vari apparati le informazioni sulle rotte conosciute)

INDIRIZZI IP

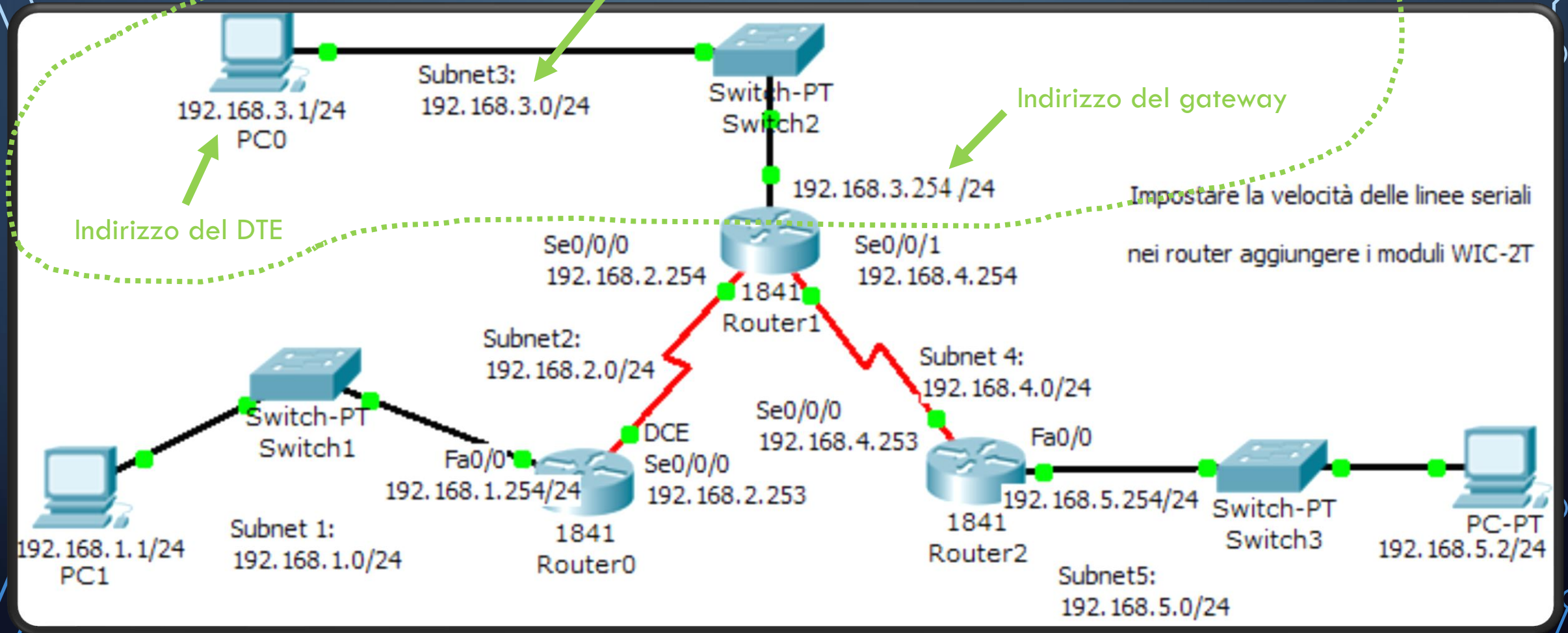
Ogni nodo della rete Internet è individuato da un indirizzo IP (IP= Internet Protocol) unico



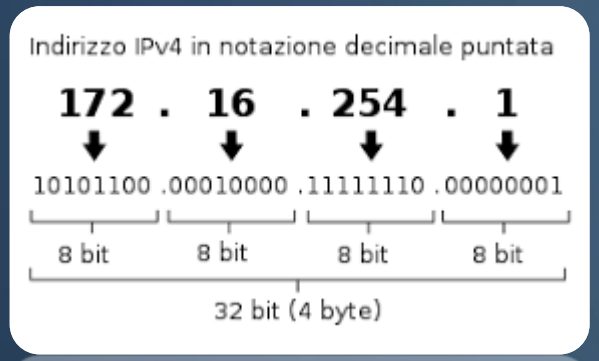
MECCANISMO DI INVIO DI UN PACCHETTO IP

- Il mittente prima di trasmettere un messaggio verifica se il destinatario del datagramma (pacchetto) appartiene alla stessa rete
  - Il mittente confronta i primi bit dell'indirizzo di destinazione dei dati da inviare (quelli che corrispondono ai bit settati a "1" nella sua subnet mask) con il network prefix (già noto) del proprio indirizzo IP
- Se corrispondono, significa che il computer di destinazione è sulla stessa rete locale e il pacchetto viene immesso nella rete
- Se invece non corrispondono, il computer d'origine invia i dati al **gateway** predefinito, il quale si occuperà del loro successivo instradamento verso la rete remota di destinazione
  - il gateway, eventualmente attraverso il meccanismo di NAT (Network Address Translation) si occuperà di trasferire il pacchetto sulla nuova rete (tipicamente la rete pubblica) su cui si affaccia
- non possono coesistere in una stessa rete 2 computer con lo stesso indirizzo IP
  - nel caso di conflitto, il secondo arrivato disattiva la propria scheda di rete

LA RETE


Confine di rete
Indirizzo di rete
Indirizzo di broadcast
192.168.3.255/24
Indirizzo del gateway
Indirizzo del DTE
192.168.3.1/24
PC0
Subnet3:
192.168.3.0/24
Switch-PT
Switch2
192.168.3.254 /24
Impostare la velocità delle linee seriali
nei router aggiungere i moduli WIC-2T
Se0/0/0
192.168.2.254
Se0/0/1
192.168.4.254
1841
Router1
Subnet2:
192.168.2.0/24
Subnet 4:
192.168.4.0/24
Switch-PT
Switch1
Fa0/0
192.168.1.254/24
DCE
Se0/0/0
192.168.2.253
Se0/0/0
192.168.4.253
Fa0/0
192.168.5.254/24
192.168.1.1/24
PC1
Subnet 1:
192.168.1.0/24
1841
Router0
1841
Router2
Switch-PT
Switch3
PC-PT
192.168.5.2/24
Subnet5:
192.168.5.0/24

TIPI DI INDIRIZZI IPV4



32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129.52.6.0
11000000 00000101 00110000 00000011	192.5.48.3
00001010 00000010 00000000 00100101	10.2.0.37
10000000 00001010 00000010 00000011	128.10.2.3
10000000 10000000 11111111 00000000	128.128.255.0

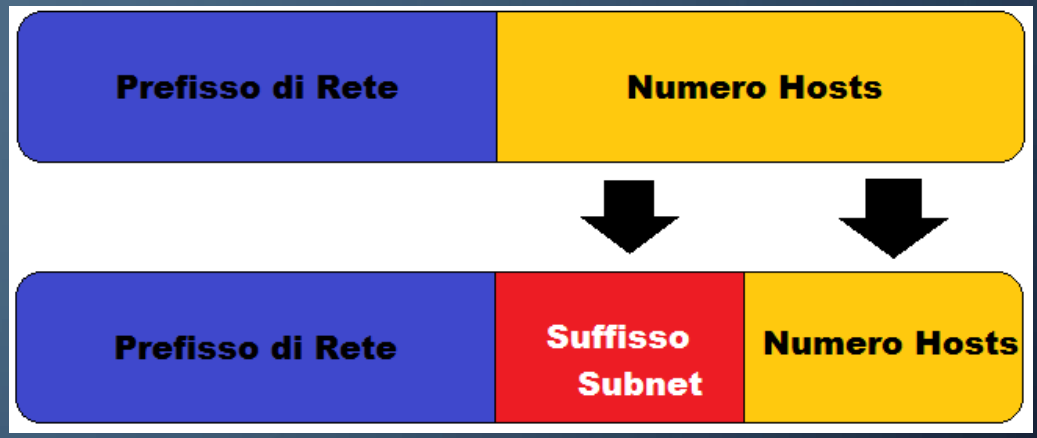
All'interno di una rete ci sono 4 tipi di indirizzo IP:

- Indirizzi che identificano un terminale della rete
- Indirizzo unico che identifica la rete
- Indirizzo unico di broadcast della rete che viene utilizzato quando un pacchetto deve essere inviato a tutti i terminali della rete
- Indirizzo unico del gateway, ovvero del terminale a cui deve essere inviati i pacchetti che devono uscire dalla rete (perché per esempio il destinatario è in un'altra rete)

RETI E SOTTORETI

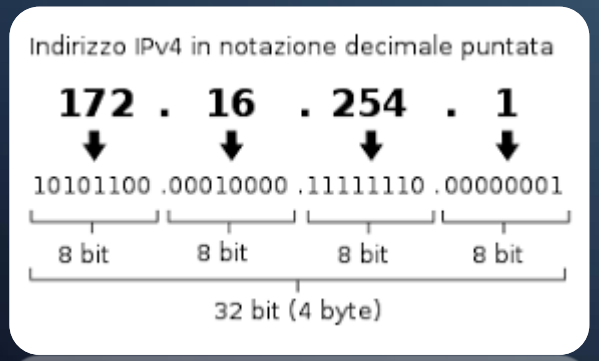
L'operazione di Subnetting rompe una rete in piccoli intervalli per:

- utilizzare lo spazio di indirizzi esistenti in modo più efficiente
- rendere la distribuzione dei pacchetti più efficiente



INDIRIZZI IPV4

N.B.: Non è possibile avere una rete che sia gestita a partire dagli indirizzi MAC (univoci) perché l'instradamento dei pacchetti avverrebbe in modo molto inefficiente



Le classi di indirizzi IP (o classful addressing) sono una formalità per dividere lo spazio di indirizzamento IPv4 introdotta dal RFC 791nel 1981 ed in uso fino all'introduzione del Classless Inter-Domain Routing (CIDR) nel 1993

- L'indirizzo IP rappresenta non solo l'host, ma anche la sottorete a cui appartiene
- Insieme alla **subnet mask** è possibile gestire l'inoltro dei pacchetti fuori della rete (tramite i router) solo quando è necessario

Gli indirizzi IP sono numeri di 32 bit suddivisi in 4 byte

- Vengono solitamente espressi in notazione decimale puntata costituita da 4 numeri compresi tra 0 e 255
  Per esempio: 172.16.254.1

CLASSI IPV4

Forma dell'indirizzo IP in binario
bbbb bbbb.bbbb bbbb.bbbb bbbb.bbbb bbbb

Classe	Bit iniziali	Inizio intervallo	Fine intervallo
A	0	0.0.0.0	127.255.255.255
B	10	128.0.0.0	191.255.255.255
C	110	192.0.0.0	223.255.255.255
D (multicast)	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

Gli indirizzi IPv4 classful si suddividono in 5 classi.

Classe A 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

- Il primo byte rappresenta la rete; gli altri tre, gli host della rete
- In notazione decimale gli IP variano nel modo seguente: 0-127.H.H.H
  - La maschera di rete è 255.0.0.0 (o anche detta /8 in CIDR poiché i bit di rete sono 8)
  - Questi indirizzi in binario iniziano con il bit 0
  - Sono adatti a reti di grandi dimensioni
  - **Sono disponibili 128 reti composte da 16774216 (-2) host**

Classe B 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

- I primi due byte rappresentano la rete; gli altri due gli host per ogni rete
- In notazione decimale gli IP variano nel modo seguente: 128-191.N.H.H con che N varia da 0 a 255
  - La maschera di rete è 255.255.0.0 (o anche detta /16 in CIDR poiché i bit di rete sono 16)
  - Questi indirizzi in binario iniziano con i bit 10
  - Sono adatti a reti di medie dimensioni
  - **Sono disponibili 16384 reti composte da 65536 (-2) host**

CLASSI IPV4

Forma dell'indirizzo IP in binario
bbbb bbbb.bbbb bbbb.bbbb bbbb.bbbb bbbb

Classe	Bit iniziali	Inizio intervallo	Fine intervallo
A	0	0.0.0.0	127.255.255.255
B	10	128.0.0.0	191.255.255.255
C	110	192.0.0.0	223.255.255.255
D (multicast)	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

Classe C 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

- I primi tre byte rappresentano la rete; l'ultimo gli host per ogni rete
- In notazione decimale gli IP variano nel modo seguente: 192-223.N.N.H
  - La maschera di rete è 255.255.255.0 (o anche detta /24 in CIDR poiché i bit di rete sono 24)
  - Questi indirizzi in binario iniziano con i bit 110
  - Sono adatti a reti di piccole dimensioni
  - **Sono disponibili 2097152 reti composte da 256 (-2) host**

Classe D 1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

- È riservata agli indirizzi multicast (trasmissione contemporanea a più destinatari nella rete senza specificare l'indirizzo)
- In notazione decimale gli IP variano nel modo seguente: 224-239.x.x.x
  - Non è definita una maschera di rete, essendo tutti e 32 i bit dell'indirizzo utilizzati per indicare un gruppo, non un singolo host
  - Questi indirizzi in binario iniziano con i bit 1110

Classe E 1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

- Riservata per usi futuri
- In notazione decimale gli IP variano nel modo seguente: 240-255.x.x.x
  - Non è definita una maschera di rete
  - Questi indirizzi in binario iniziano con i bit 1111

INDIRIZZI SPECIALI IPV4

Esistono degli indirizzi speciali nelle reti classful

Indirizzi di rete

- Sono gli indirizzi che identificano la rete e non possono essere assegnati ad un host
- Sono indirizzi che hanno tutti 0 nella parte dedicata agli host
  - Classe A: X.0.0.0
  - Classe B: X.Y.0.0
  - Classe C: X.Y.Z.0

Indirizzi di broadcast

- Sono indirizzi utilizzati per mandare messaggi a tutti gli host della rete
- Hanno tutti 1 nella parte dedicata agli host
  - Classe A: X.255.255.255
  - Classe B: X.Y.255.255
  - Classe C: X.Y.Z.255

Indirizzo di rete di default

- È l'indirizzo 0.0.0.0 ed è utilizzato per il routing o per identificare l'host corrente quando non è stato ancora assegnato

INDIRIZZI SPECIALI IPV4

Indirizzo di broadcast di default

- È l'indirizzo 255.255.255.255 ed è utilizzato per mandare pacchetti a tutta la rete corrente

Indirizzo di rete di loopback

- È l'indirizzo 127.0.0.1 che rappresenta il localhost ovvero l'indirizzo IP dell'host stesso
- I pacchetti inviati all'indirizzo di loopback sono inviati all'host stesso

INDIRIZZI PUBBLICI E PRIVATI

Gli indirizzi che si affacciano sulla rete Internet sono detti **pubblici** e sono univoci in tutto il pianeta

Poiché il numero degli indirizzi IP (4294967292 indirizzi contando anche quelli speciali) non è sufficiente ad indirizzare tutti gli host esistenti, sono stati riservati range di indirizzi **privati** per ogni classe

Questi indirizzi:

- **non possono essere utilizzati per affacciarsi alla rete pubblica Internet perché servono per indirizzare gli host delle reti private**
- **possono ripetersi in rete private diverse non connesse tra loro**

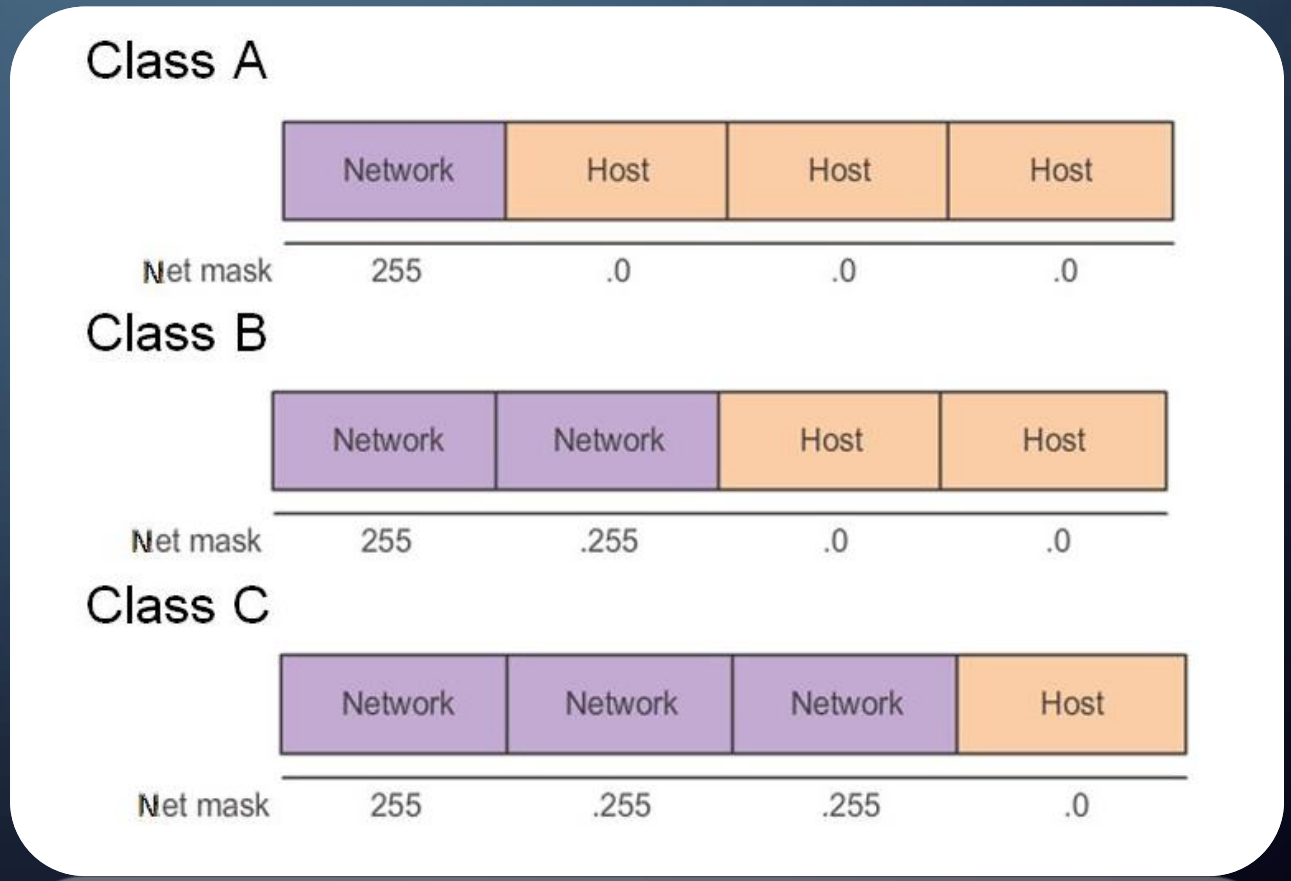
I range di indirizzi privati sono:

- Reti di classe A: 10.x.x.x (da 10.0.0.0 a 10.255.255.255)
- Reti di classe B: 172.16.x.x – 172.31.x.x (da 172.16.0.0 a 172.31.255.255)
- Reti di classe C: **192.168.x.x** (da 192.168.0.0 a 192.168.255.255, il 192.168.0.0 è utilizzabile anche come una classe B avendo gli ultimi due ottetti di bit uguali a 0)

LA SUBNET MASK

La maschera di sottorete (in inglese subnet mask), nell'ambito di una rete TCP/IP, è un parametro di configurazione che definisce la dimensione (intesa come intervallo di indirizzi) della sottorete IP, o subnet, a cui appartiene un host, al fine di ridurre il traffico di rete e facilitare la ricerca e il raggiungimento di un determinato host con relativo indirizzo IP.

Nel caso delle classi classful



INDIRIZZO DI RETE: L'ANDING PROCESS

- L'ANDing process o processo di messa in AND consiste nel fare un'operazione di AND logico tra l'indirizzo IP (per esempio del mittente) e la relativa subnet mask in modo da ottenere l'IDnet ovvero l'indirizzo di rete di un terminale

- Il processo è utile nelle operazioni di routing per capire se mittente e destinatario sono nella stessa sottorete
  - Per esempio, 172.16.2.4 e 172.16.3.5 con subnet mask 255.255.0.0 sono nella stessa sottorete?

    172.16.2.4 in binario è: 10101100 00010000 00000010 00000100

    255.255.0.0 in binario è: 11111111 11111111 00000000 00000000

    L'ANDing process è: 10101100 00010000 00000000 00000000 (IDnet)

    172.16.3.5 in binario è: 10101100 00010000 00000011 00000101

    255.255.0.0 in binario è: 11111111 11111111 00000000 00000000

    L'ANDing process è: 10101100 00010000 00000000 00000000 (IDnet)

    I due host sono nella stessa sottorete

- Quando mittente e destinatario sono nella stessa sottorete il router non fa uscire il pacchetto dalla sottorete ottimizzando il traffico di rete

SLASH NOTATION

È possibile riassumere la coppia indirizzo IP e subnet mask mediante la slash notation nella quale all'indirizzo IP si fa seguire il prefix length, ovvero il numero di bit uguali a 1 nella subnet mask

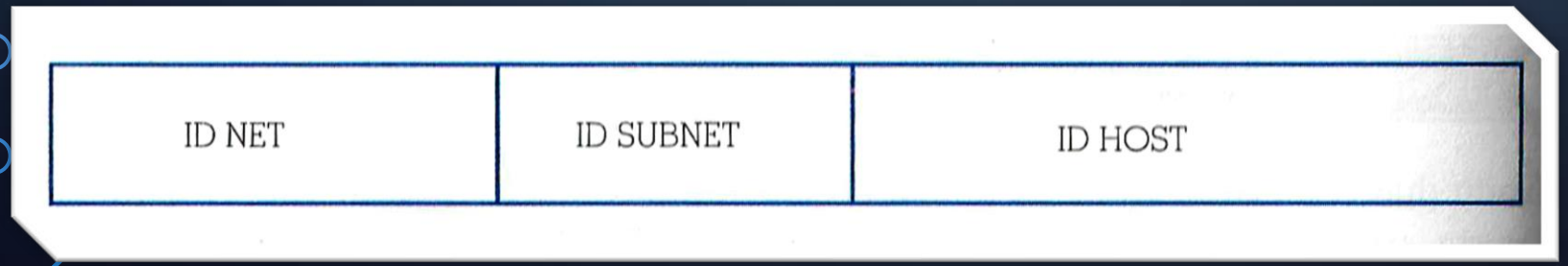
- Per esempio 130.45.1.1 con subnet mask 255.255.255.0 viene indicato con 130.45.1.1/24

IL SUBNETTING VLSM

- Nel 1987, a soli 6 anni dall'introduzione dell'IPv4 con la direttiva RFC 1009 si è introdotta la possibilità di suddividere una rete in sottoreti utilizzando la parte host di un indirizzo IP

- L'operazione viene fatta utilizzando maschere di rete di lunghezza variabile o maschere VLSM (Variable Length Subnet Masking)

Suddivisione dei 32 bit in NET e HOST senza il subnetting



Suddivisione dei 32 bit in NET, SUBNET e HOST per il subnetting

MASCHERE VLSM (VARIABLE LENGTH SUBNET MASKING)

Per esempio se si dispone di un indirizzo IP di classe C, per esempio

192.168.0.0/24

che può contenere al massimo 256-2=254 host con subnetmask 225.255.255.0, la suddivisione VLSM potrebbe dare origine alle seguenti sottoreti:

2 sottoreti con 128-2=126 host ognuna; subnet mash 255.255.255.128 (/25)

192.168.0.0/25
192.168.0.128/25

4 sottoreti con 64-2=62 host ognuna; subnet mash 255.255.255.192 (/26)

192.168.0.0/26
192.168.0.64/26
192.168.0.128/26
192.168.0.64/26

MASCHERE VLSM (VARIABLE LENGTH SUBNET MASKING)

Per esempio se si dispone di un indirizzo IP di classe C, per esempio

192.168.0.0/24

che può contenere al massimo 256-2=254 host con subnetmask 225.255.255.0, la suddivisione VLSM potrebbe dare origine alle seguenti sottoreti:

8 sottoreti con 32-2=30 host ognuna; subnet mash 255.255.255.224 (/27)

192.168.0.0/27
192.168.0.32/27
192.168.0.64/27
192.168.0.96/27
192.168.0.128/27
192.168.0.160/27
192.168.0.192/27
192.168.0.224/27

MASCHERE VLSM (VARIABLE LENGTH SUBNET MASKING)

Per esempio se si dispone di un indirizzo IP di classe C, per esempio

192.168.0.0/24

che può contenere al massimo 256-2=254 host con subnetmask 225.255.255.0, la suddivisione VLSM potrebbe dare origine alle seguenti sottoreti:

16 sottoreti con 16-2=14 host ognuna; subnet mash 255.255.255.240 (/28)

32 sottoreti con 8-2=6 host ognuna; subnet mash 255.255.255.248 (/29)

64 sottoreti con 4-2=2 host ognuna; subnet mash 255.255.255.252 (/30)

IL SUBNETTING VLSM

- La soluzione permette di ottimizzare il traffico in una rete privata di grosse dimensioni, suddividendola in reti più piccole collegate tra loro da router interni
  - all'interno di una singola sottorete l'accesso è multidrop (cioè i pacchetti vendono trasmessi a tutti gli host della sottorete e vengono letti solo dall'host con l'indirizzo IP corretto), quindi più sono gli host, maggiore è la probabilità di collisioni

- Quando il VLSM non viene usato, si dice che gli indirizzi IP sono **classful** in quanto seguono esattamente le regole della classe A-B-C a cui appartengono. Quando invece VLSM è usato, gli indirizzi IP si dicono **classless**

MASCHERE VLSM (VARIABLE LENGTH SUBNET MASKING)

Non solo, applicando ricorsivamente la tecnica, si può pensare di suddividere lo spazio in varie sottoreti di dimensione variabile.

Per esempio se si dispone di un indirizzo IP di classe C (massimo 254 host) e si desidera dividere la rete in due sottoreti una da 100 host e due da 50 host, con la tecnica VLSM si può suddividere lo spazio di indirizzamento prima in due usando la maschera di rete 255.255.255.128 (126 host per sottorete) e successivamente una delle due sottoreti a metà usando la maschera 255.255.255.192 (62 host per sottorete)

CIDR (CLASSLESS INTERDOMAIN ROUTING)

Il CIDR (Classless Inter-Domain Routing) è un nuovo schema di indirizzamento introdotto nel 1993 usato per ottimizzare l'utilizzo di indirizzi di rete di classe C permettendo il supernettig

Il CIDR quindi

- Contiene al suo interno l'indirizzamento VLSM e quindi introduce la possibilità di suddividere efficacemente le reti in sottoreti
- Prevede anche il **supenetting,** ovvero la possibilità di unire insieme più sottoreti in un'unica rete di dimensioni maggiori

La tecnica permette di suddividere ricorsivamente lo spazio degli indirizzi con maschere di lunghezza diversa in modo da utilizzarlo in modo più efficiente

VANTAGGIO DEL CIDR (SUPERNETTING)

Per esempio: un'azienda vuole suddividere la propria rete di 2000 host, in 8 subnet ciascuna con 250 host

- non è possibile farlo con un solo indirizzo di classe C (massimo 254 host) ed è necessario utilizzare un solo indirizzo di classe B sul quale fare subnetting. Se questo viene fatto all'interno di una rete privata non ci sono problemi, ma se per esempio l'azienda ha più sedi ed è necessario usare una rete pubblica il costo dell'indirizzo di classe B è elevato (ammettendo che ne esistano ancora di disponibili)

- l'unica alternativa per contenere i costi sarebbe chiedere 8 indirizzi di classe C; questo però condurrebbe ad un sovraccarico dei routers i quali dovrebbero inserire nelle loro tabelle di istradamento invece di un solo indirizzo (per esempio di classe B), 8 indirizzi di classe C

- con il CIDR il problema è risolto acquistando 8 indirizzi di classe C consecutivi opportuni, chiamati anche CIDR block (Classless Interdomain Routing block), e aggregandoli con una maschera di rete corretta

VANTAGGIO DEL CIDR (SUPERNETTING)

Per esempio nel caso precedente dei 2000 host, supponiamo che venga rilasciato un intervallo di 8 indirizzi di classe C per un totale di 8x254=2032 host, compreso fra 220.78.168.0 e 220.78.175.0

Se convertiamo in binario avremo:

220.78.168.0 = 11011100 01001110 10101***000*** 00000000
220.78.169.0 = 11011100 01001110 10101***001*** 00000000
220.78.170.0 = 11011100 01001110 10101***010*** 00000000
220.78.171.0 = 11011100 01001110 10101***011*** 00000000
220.78.172.0 = 11011100 01001110 10101***100*** 00000000
220.78.173.0 = 11011100 01001110 10101***101*** 00000000
220.78.174.0 = 11011100 01001110 10101***110*** 00000000
220.78.175.0 = 11011100 01001110 10101***111*** 00000000

La parte sottolineata, che come si vede rimane costante, costituisce l'IDNet dell'intera rete, mentre i tre bit del terzo ottetto danno in successione gli otto indirizzi del blocco

A questo punto sarà sufficiente per il router (che naturalmente deve supportare il CIDR) creare una sola entry (CIDR entry) nella sua tabella di routing con il primo indirizzo del blocco (220.78.168.0) e una maschera di supernetting /21 con 21 bit uguali a 1 cioè 11111111111111111 11111000 00000000 per gestire correttamente l'instradamento all'interno della rete

VANTAGGIO DEL CIDR (SUPERNETTING)

In notazione CIDR la rete è identificata con 220.78.168.0/21

Con questa tecnica un singolo indirizzo IP può rappresentare un gruppo di indirizzi IP snellendo le tabelle di routing, quindi semplificando e velocizzando il lavoro dei router e ottimizzando l'uso degli indirizzi IP

Non tutti gli indirizzi contigui vanno bene, per esempio se nel caso precedente il primo indirizzo era 220.78.169 e l'ultimo 220.78.176.0 la maschera non si sarebbe potuta creare opportunamente infatti:

220.78.169.0= 11011100 01001110 10101***001*** 00000000

220.78.176.0 = 11011100 01001110 10110***000*** 00000000

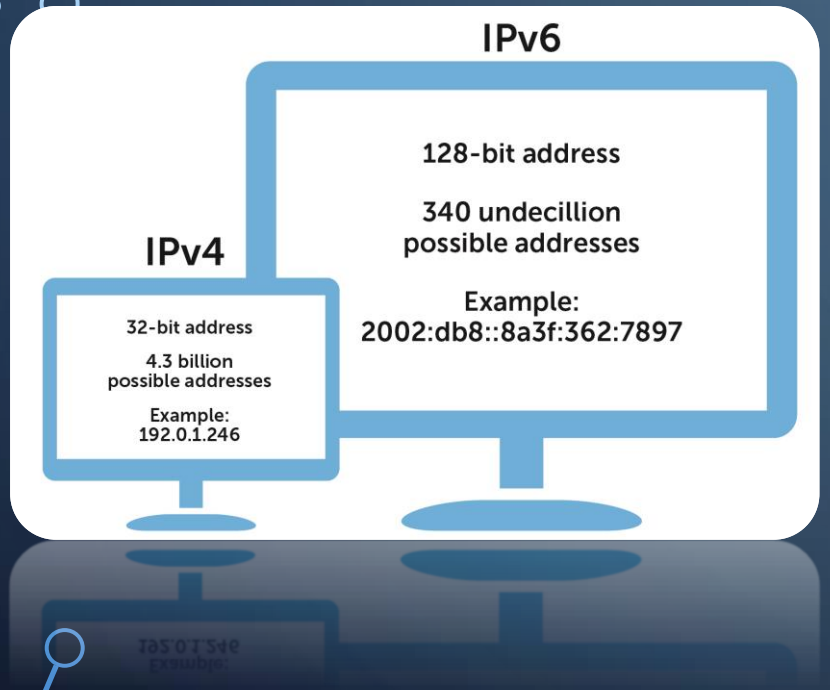
Nel caso specifico gli indirizzi di partenza validi sono a multipli di 8 del tipo:

- 220.78.168.0
- 220.78.176.0
- 200.78.184.0
- ecc.

IL NAT (NETWORK ADDRESS TRANSLATION)

- La **Network Address Translation** (NAT) è un meccanismo che permette di sfruttare gli indirizzi IP privati all'interno delle organizzazioni, rallentando l'utilizzo degli indirizzi IP pubblici disponibili
- Consiste nel modificare gli indirizzi IP contenuti negli header dei pacchetti in transito da parte di un router all'interno di una comunicazione tra due o più host
- Per implementare il NAT, un router ha quindi bisogno di effettuare il tracciamento delle connessioni, ovvero di tenere traccia di tutte le connessioni che lo attraversano in modo da cambiare l'indirizzo IP in modo trasparente
  - Il NAT più utilizzato è l'IP masquerading (chiamato anche NAT dinamico) un caso particolare di NAT alla sorgente, in cui le connessioni generate da un insieme di computer vengono "presentate" verso l'esterno con un solo indirizzo IP pubblico
    - La tecnica è detta anche Port Address translation (PAT), IP Overloading o NAPT (Network Address and Port Translation), in quanto vengono modificati non solo gli indirizzi IP ma anche le porte TCP e UDP delle connessioni in transito. Tale tecnica viene codificata nella RFC2663, col nome di «Network Address Port Translation (NAPT)»
  - In ricezione il NAT può essere utilizzato per bilanciare il carico di lavoro delle connessioni in ingresso su più server oppure per realizzare un **proxy**, ovvero un server che in una memoria temporanea memorizza il contenuto di siti web visitati in precedenza

INDIRIZZAMENTO IPV6



IPv6 è la versione dell'Internet Protocol designata come successore dell'IPv4

Tale protocollo introduce alcuni nuovi servizi e semplifica molto la configurazione e la gestione delle reti IP poiché rende obsoleto il subnetting

La sua caratteristica più importante è il più ampio spazio di indirizzamento

IPv6 riserva 128 bit per gli indirizzi IP e gestisce 2^128 (circa 3,4 × 10^38) indirizzi, ovvero circa 6 per metro quadro di superficie terrestre (oceani e deserti compresi)

- IPv4 riserva 32 bit per l'indirizzamento e gestisce 2^32 (circa 4,3 × 10^9) indirizzi

- La notazione prevede che i 128 bit vengano suddivisi in 8 gruppi da 16 bit e i 16 bit di ogni gruppo vengano rappresentati con 4 cifre decimali. Gli otto gruppi vengono separati dal carattere «:»

TRANSIZIONE DA IPV4 A IPV6

La politica adottata per la transizione a IPv6 consiste in un graduale passaggio da un protocollo all'altro, cercando di far coesistere le due versioni di IP in un'unica rete

- Per far ciò la strada seguita fino a questo momento consiste nel costruire router e switch di livello 2 e 3 in grado di interpretare entrambi i protocolli
- Inoltre da qualche anno i nuovi sistemi operativi sono in grado di generare indirizzi IPv6 e di interpretarli. In questo modo ogni host nella rete è individuabile da almeno due indirizzi, uno dato da IPv4 ed uno da IPv6

- La sostituzione di tutti i router nel mondo risulta un lavoro piuttosto arduo e allora si cerca in qualche modo di aggirare via software la non interpretabilità di IPv4 e IPv6. Le soluzioni finora create possono essere suddivise in tre categorie:
  - dual-stack (Utilizzo del doppio stack IP nella pila protocollare)
  - NAT-PT (conversione dell'indirizzo IPv6 in indirizzo IPv4 e viceversa)
  - tunneling (i pacchetti IPv6 vengono incapsulati dall'host sorgente in pacchetti IPv4, inviati nel tunnel e una volta giunti a destinazione, l'host li decapsula e li tratta di nuovo come pacchetti IPv6)