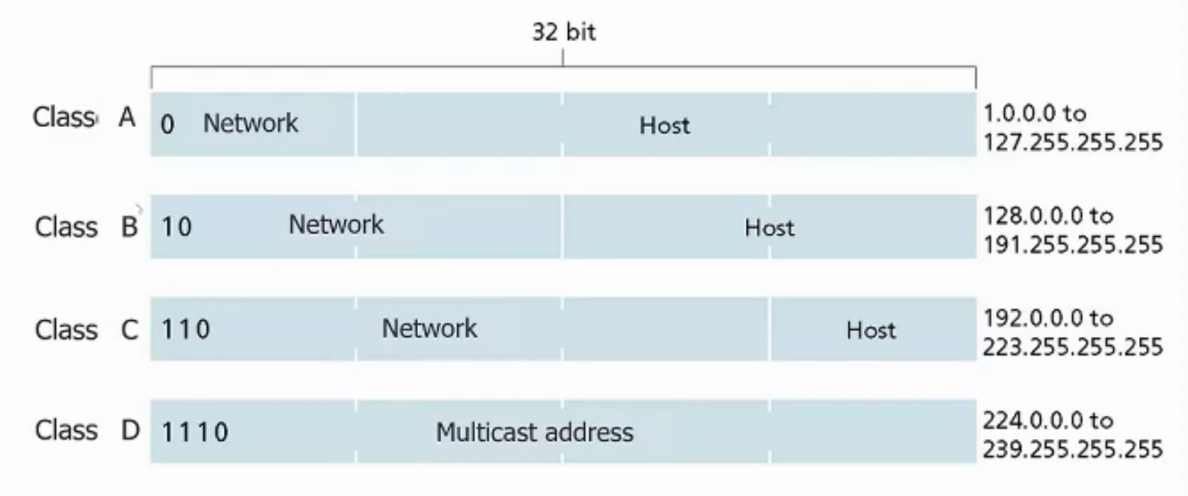
Indirizzamento IPv4

Nella prima formulazione degli indirizzi è stato introdotto il concetto di **classe**: l'indirizzamento a 32 bit era suddiviso in 5 classi:



> La 5° classe è riservata

Le classi più usate sono le classi A, B, C e D; le prime classi A B e C sono impiegate per l'indirizzamento **unicast**, ovvero usato per individuare un singolo destinatario di un datagram IP, mentre gli indirizzi di classe D sono usati per il **multicast**, quindi per consentire l'invio di un datagram ad un gruppo di host, identificati tutti dallo stesso indirizzo multicast.

LE diverse classi si differenziano per il numero di bit riservati per individuare il **prefisso di rete** ed il **suffisso di host**. Si differenziano quindi per numero di host che possono ospitare. In particolare gli indirizzi di classe A prevedono come prefisso di rete il primo byte (più significativo) mentre il suffisso di host è ottenuto con gli altri tre byte meno significativi.

La classe A viene riconosciuta immediatamente per via del bit 0 nella parte più a sinistra (questo perchè il range della classe A va da 0 a 127, ovvero 2^7 bit; di conseguenza il primo bit più significativo è sempre zero), mentre i 7 bit meno significativi sono usati per rappresentare l'host.

Dato un indirizzo di classe A che possiamo pensare essere attribuito ad una rete di tale classe, possiamo avere un numero di host massimo pari a 2^{24} (ovvero 32-7 - 1 = 24).

Sono **indirizzi di classe B** gli indirizzi dove il primo bit è fisso ad 1, ma è seguito da un bit posto a 0; abbiamo quindi **due bit vincolati**. Il range in questo caso va da 128.0.0.0 a 191.255.255.255 .

Sono **indirizzi di classe c** indirizzi di **reti molto piccole** perchè in questo caso il suffisso di host è di solo 8 bit, quindi un solo byte; con un solo byte possiamo rappresentre 2^8 fino a 256 host. Il prefisso di rete in questo caso è vincolato da 3 bit, che sono posti fissi a 110. Il range va da 192.0.0.0 fino a 223.255.255.255 .
Sicuramente riconosciamo questo range proprio perchè è il range più usato nelle reti domestiche.

Sono **Indirizzi di classe D o Multicast** caratterizzati da 4 bit vincolati: 1110. Gli indirizzi variano da 224.0.0.0 a 239.255.255.255 . Sono utilizzati per identificare un gruppo di macchine, e con un singolo datagram IP è possibile raggiungere questo gruppo. E' utile per consegnare lo stesso contenuto a diverse macchine all'interno di una rete locale.

Quindi

Con la suddivisione in classi lo spazio degli indirizzi abilitato dai 32 bit che vengono usati per rappresentare un indirizzo IP è partizionato in modo da avere reti IP di dimensioni diverse.

Indirizzi riservati

Come abbiamo visto prima alcuni indirizzi sono **riservati**; ad esempio l'indirizzo 0.0.0.0 non è assegnato a nessuna classe. Questo indirizzo viene impiegato per rappresentare un host su una rete, ed è un indirizzo assegnato ad un host inizialmente, quando ancora non ha acquisto l'indirizzo finale.

Abbiamo inoltre degli **intervalli** di IP che sono **tre intervalli in tre classi diverse**, tutti usati per usi privati:

- Classe A: 10.0.0.0 - 10.255.255.255
- Classe B: 172.16.0.0 - 172.31.255.255
- Classe C: 192.168.0.0 - 192.168.255.255 molto usato nelle reti domestiche

Riservare gli indirizzi per uso privato è una delle soluzioni individuata nel corso degli anni per far fronte a ciò che inizialmente non si pensava potesse essere un limite: il numero esiguo di indirizzi IP che possiamo rappresentare su 32 bit.

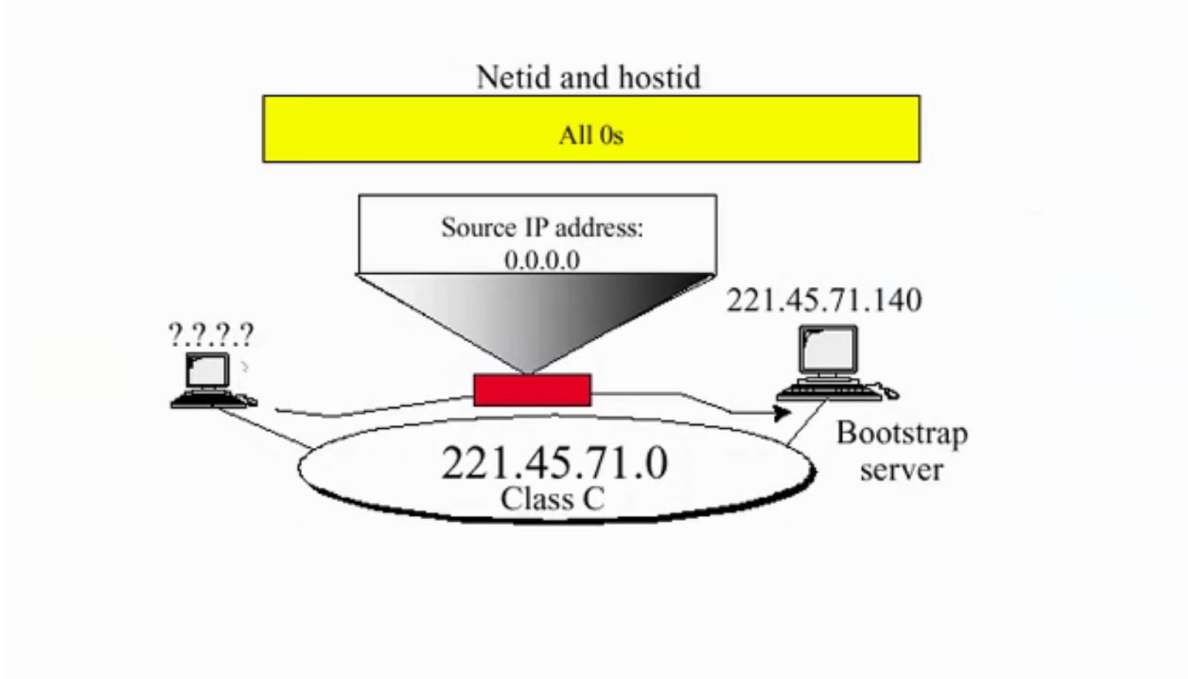
Inizialmente, infatti, si pensava che più di 4 miliardi di indirizzi IP fossero sufficienti per indirizzare tutti i dispositivi, ma con l'avvento dei dispositivi IOT e lo sviluppo del web, questi valori sono diventati addirittura "stretti".

L'idea è stata quindi quella di **riservare un range di indirizzi per uso privato.** Questi indirizzi non sono infatti **instradabili**. E' infatti possibile di creare diverse reti privati senza garantire l'univocità.

E' però possibile però, come sappiamo, che una macchina in una rete privata comunichi con una macchina esterna! Di conseguenza è richiesto che uno di questi indirizzi venga associato ad un indirizzo pubblico.

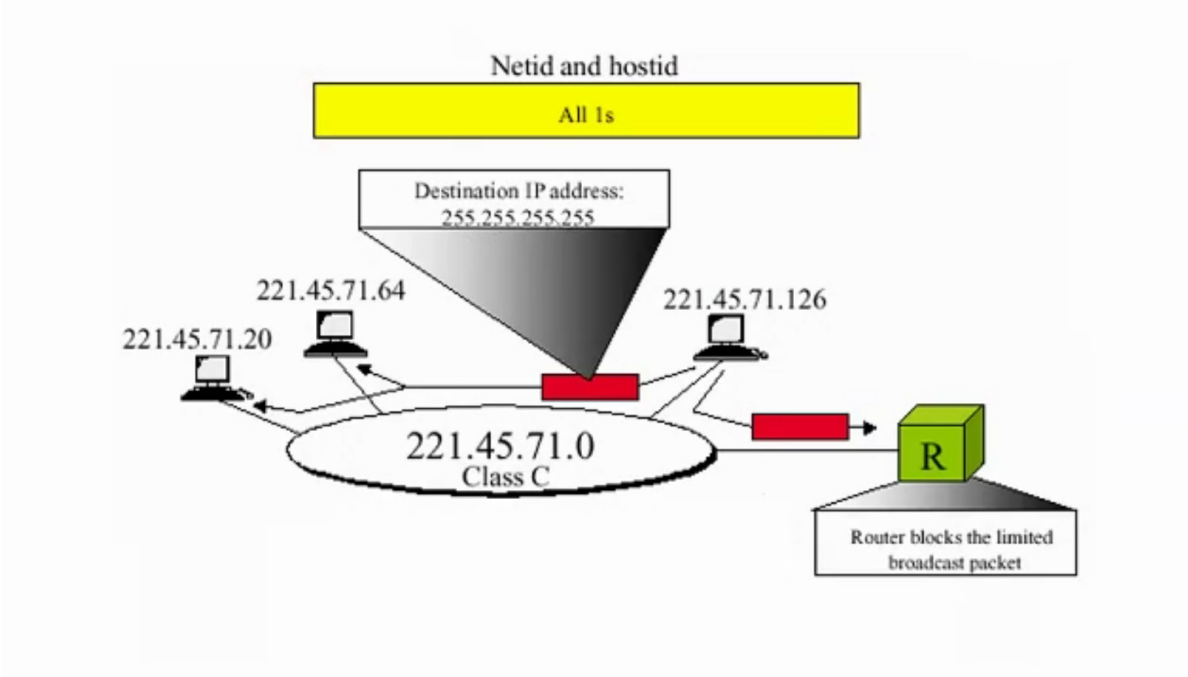
Address Range	Purpose
0.0.0.0	This host on this network
10.0.0.0 – 10.255.255.255	Reserved for private use (RFC 1918)
127.0.0.0 – 127.255.255.255	Reserved for loopback/local address
172.16.0.0 – 172.31.255.255	Reserved for private use (RFC 1918)
192.168.0.0 – 192.168.255.255	Reserved for private use (RFC 1918)
xxx.xxx.xxx.0	Class C network address
xxx.xxx.xxx.255	Direct broadcast towards a class C network
255.255.255.255	Limited broadcast
0.0.0.xxx	A specific host on the current class C network

Un host su questa rete



Un host, inizialmente, ha un indirizzo IP 0.0.0.0, ma dopodichè questo indirizzo viene assegnato o dinamicamente o staticamente da un amministratore. Quando l'host si annuncia e chiede al server l'assegnazione di un indirizzo, usa l'indirizzo 0.0.0.0 .

Broadcast limitato

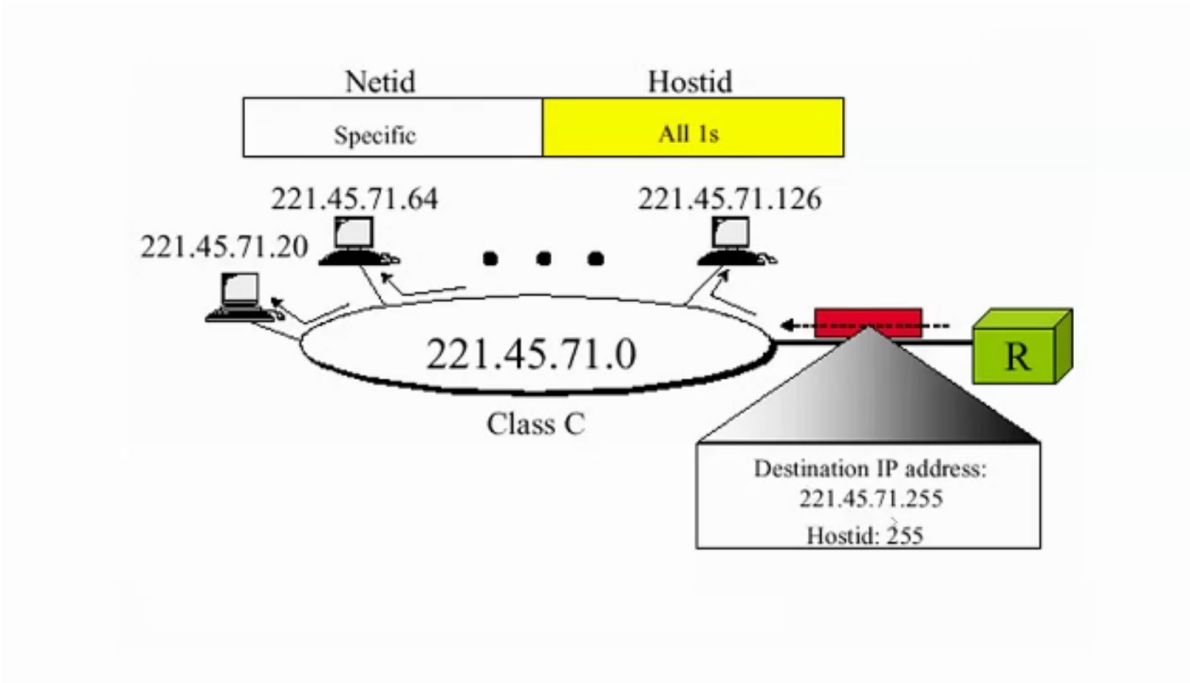


E' rappresentato dall'indirizzo 255.255.255.255; questo indirizzo consente la comunicazione da uno a molti, quindi il datagram spedito da un host viene inviato a tutte le macchine sulla rete (tutte le interfacce di rete).

E' detto **limitato** perchè il datagram che arriva al router viene bloccato da quest'ultimo. Per evitare l'inondazione di internet con datagram di questo tipo si limita l'inoltro, e si fa in modo che il broadcast riguardi solo una singola rete IP.

Broadcast diretto

In questa variante il datagram inviato da una macchina raggiunge una rete e viene inviato a tutte le macchine che fanno riferimento a quella rete internet. A differenza del precedente, l'indirizzo IP prevede un prefisso di rete, che è la rete di destinazione che si vuole raggiungere con un **broadcast diretto**, e per il quale si vuole effettuare "l'inondazione".



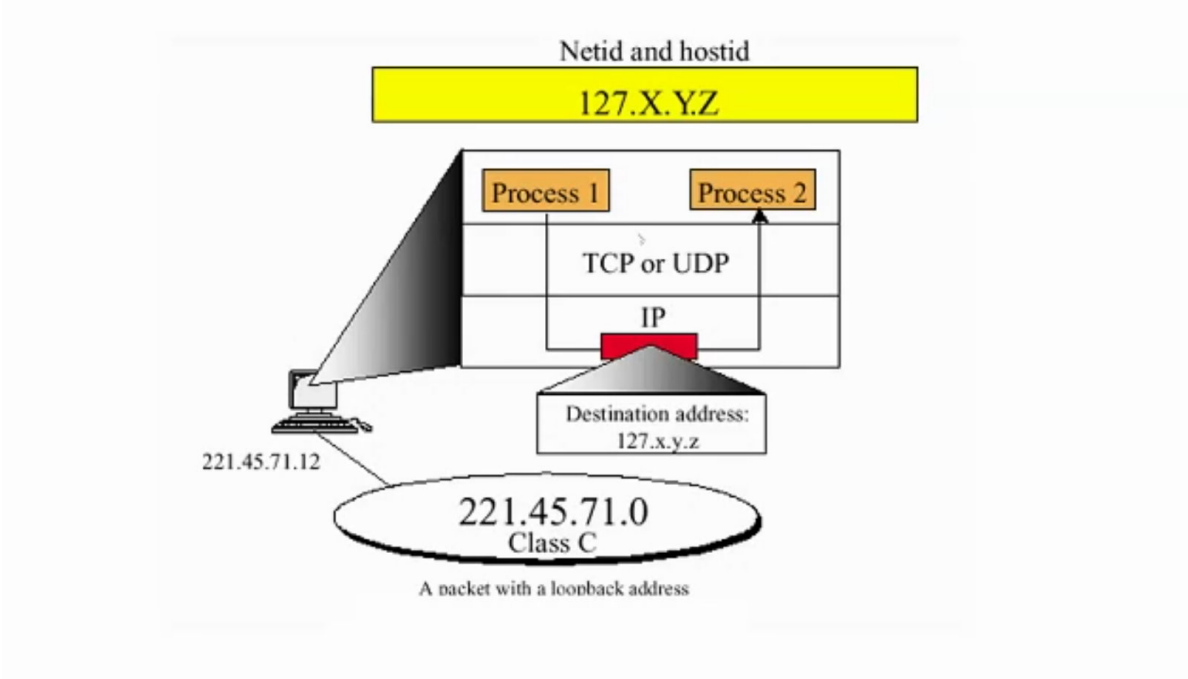
Differenza tra broadcast diretto e limitato

La differenza tra i due broadcast è che nel **broadcast limitato** non esplicitiamo un prefisso di rete, abbiamo un indirizzo che è **unico** (tutti 1 o tutti 255) e quell'indirizzo può essere usato da una macchina all'interno di una rete per invaiare pacchetti a tutte le macchine di **quella rete IP**, di conseguenza non attraverserà il router.

Nel caso del **broadcast diretto** l'indirizzo IP di tipo broadcast diretto presenta un prefisso di rete che consente al datagram di attraversare il router fino a raggiungere la rete di destinazione. Una volta la rete di destinazione si ha l'inondazione del datagram a tutte le interfacce presente in quella rete.

Indirizzi di loopback

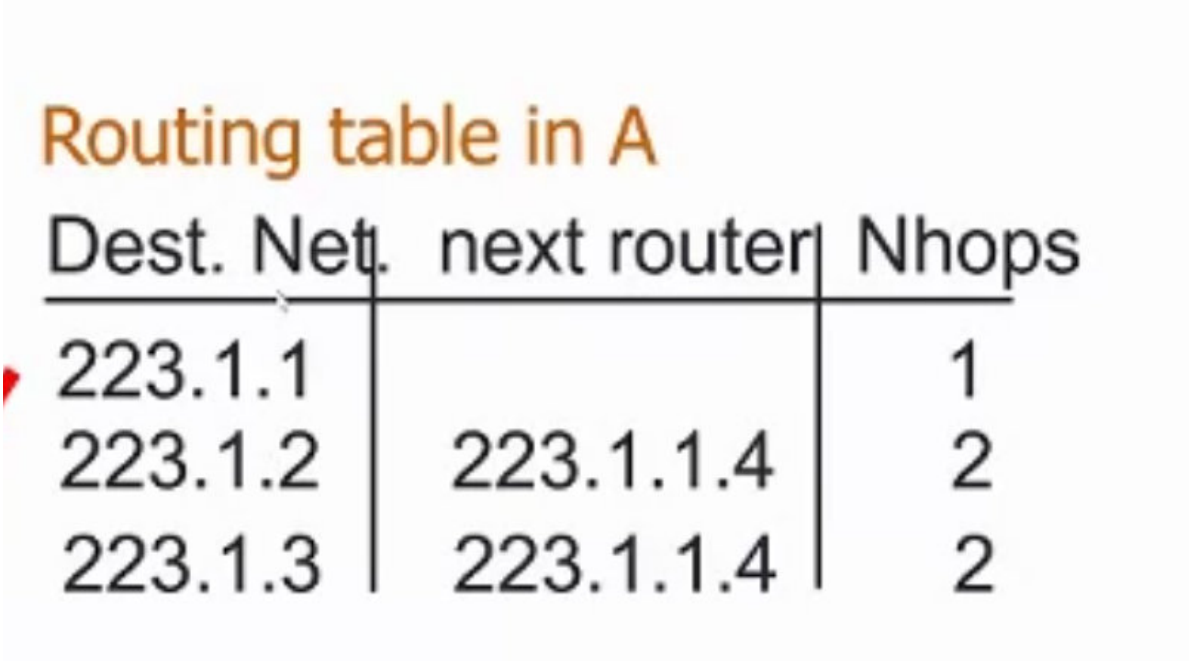
Quando usiamo un indirizzo di loopback il datagram viene **cortocircuitato a livello 3**, non passa quindi al livello 2 e non viene incapsulato in un frame. Il datagram una volta arrivato al layer in cui opera il protocollo IP viene consegnato al processo sulla stessa macchina **attraverso ad una socket associata all'indirizzo 127.0.0.1**.



Il fatto che il datagram non arrivi al livello 2 fa si che la comunicazione sia particolarmente veloce. Due processi sulla stessa macchina potrebbero comunicare anche in modo diverso: inviano datagram all'indirizzo IP che caratterizza quella macchina; se la macchina ha un'interfaccia di rete alla quale è assegnato l'indirizzo 221.45.71.12 (classe c) un processo potrebbe comunicare con un altro processo usando come indirizzo di destinazione quello mensionato poc'anzi.

IP forwarding

Per consentire l'inoltro ci aspettiamo che nell'intestazione di un datagram IP ci siano due campi che sono l'indirizzo IP dell'interfaccia mittente ed indirizzo IP dell'interfaccia di destinazione. Troveremo inoltre una tabella chiaamta **routing table**, che presenta queste informazioni:

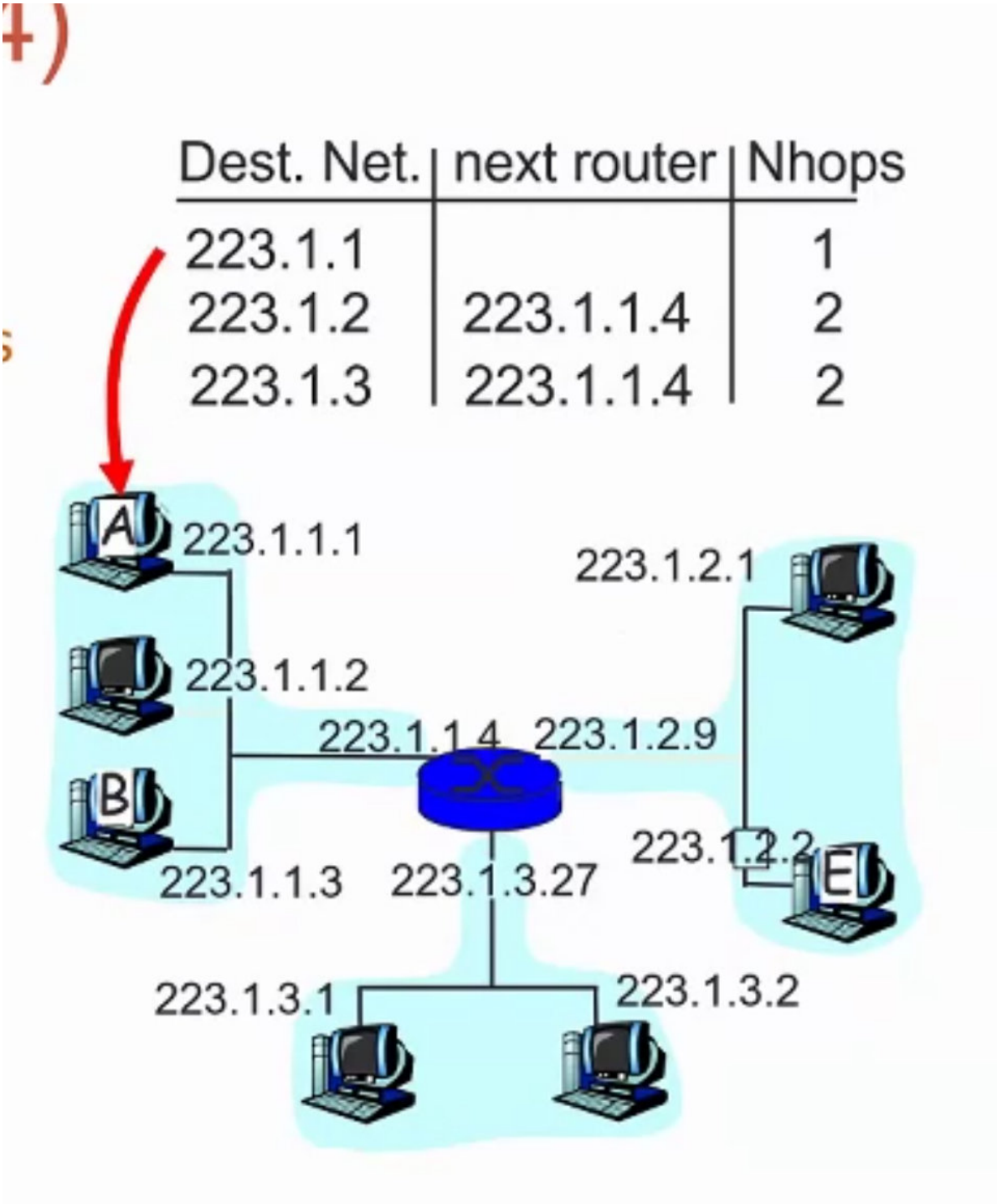


- Colonna indirizzo di destinazione
- Colonna del prossimo router da raggiungere
- Colonna che ci dice quanti salti dobbiamo fare per arrivare alla destinazione

Ogni macchina interessata alla comunicazione ha una visione locale della rete. Nella sua tabella avrà anche l'informazione sulla destinazione, ma per il momento sa solo che deve consegnare il datagram ad un certo router (il prossimo). Una volta inseriti gli indirizzi all'interno di un datagram, **questi non vengono più modificati**.

Primo esempio

La macchina A vuole spedire alla macchina B, collocata sulla stessa sottorete della macchina A:

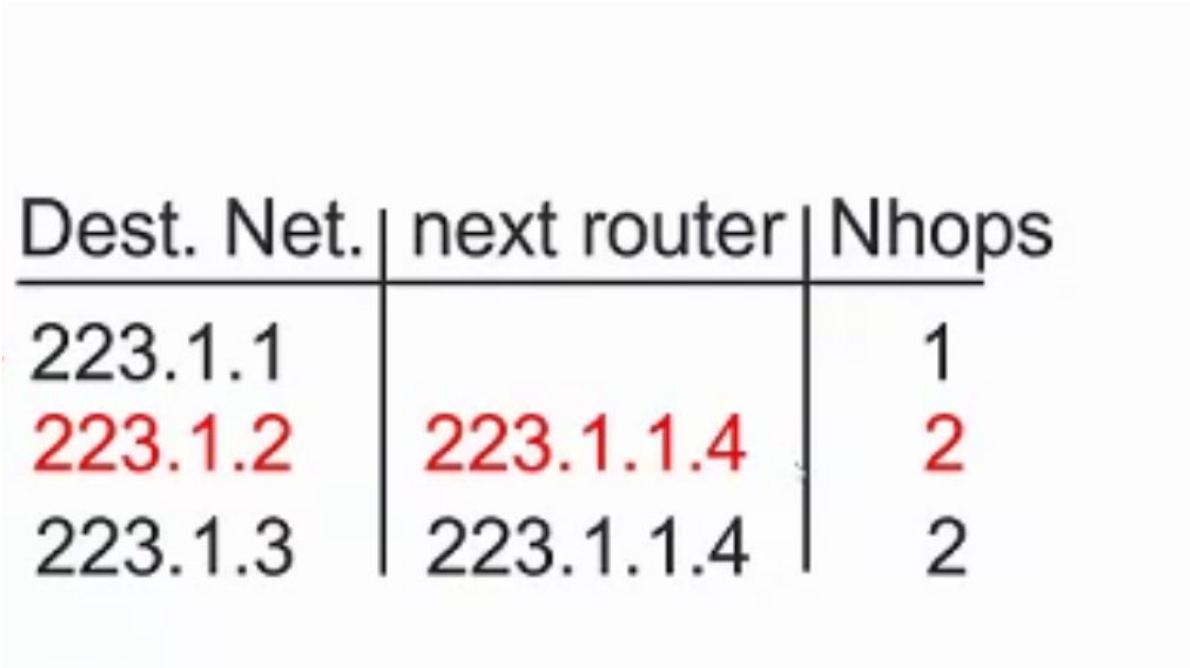


A costruisce un datagram con le informazioni di controllo con l'indirizzo IP del mittente 223.1.1.1 e dest IP è 223.1.1.3 .

A capisce che si parla di un indirizzo di classe C, ed essendo di classe C preleva i primi 3 byte che rappresentano il **prefisso di rete** e li confronta con i primi 3 byte dell'indirizzo sorgente. Siccome coincidono, A capisce che la macchina B che si vuole raggiungere è sulla stessa rete IP .

Di conseguenza il router non sarà interessato; siccome le due macchine sono sulla stessa rete IP, e connesse tramite lo switch, il livello 3 non viene toccato.

Nel caso in cui la macchina A vuole comunicare con la macchina E, il prefisso di rete è diverso, e quindi A capisce **dall'analisi del prefisso di rete** che la macchina di destinazione identificata dall'indirizzo IP, è su una rete diversa.
Dobbiamo quindi consultare la Routing Table usando come chiave l'indirizzo di destinazione. Per la destinazione 223.1.2 (corrispondente a 223.1.2.0), l'interfaccia router da raggiungere è **223.1.1.4**:



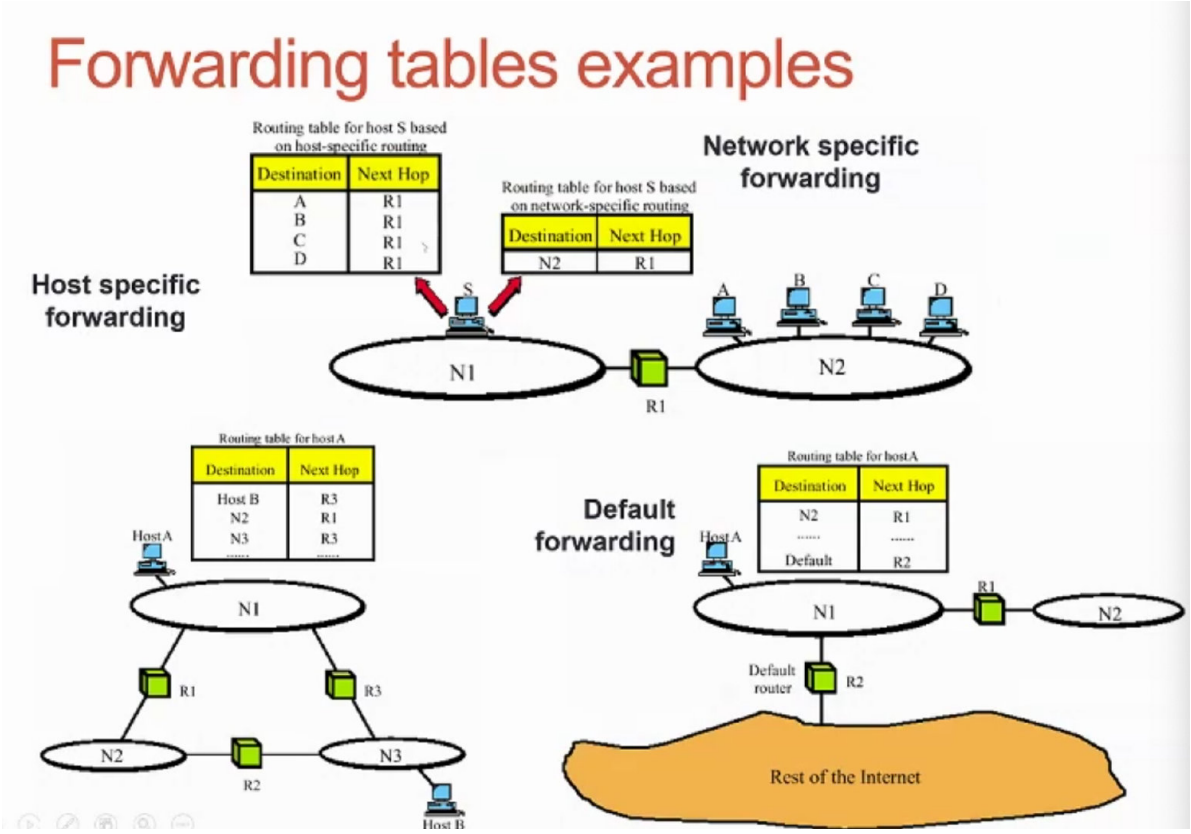
Dest. Net.	next router	Nhops
223.1.1		1
223.1.2	223.1.1.4	2
223.1.3	223.1.1.4	2

> tabella costruita dagli algoritmi di routing

Una volta consultata la tabella fornisce l'indirizzo IP dell'interfaccia del router che deve essere raggiunto. Il datagram che parte da A e deve arrivare ad E, deve essere inviato a quell'interfaccia di rete.
Non possiamo cambiare il contenuto del datagram, quindi recuperato l'indirizzo fisico dell'interfaccia, viene costruito un frame che ha indirizzo di destinazione l'indirizzo fisico di corrispondente.

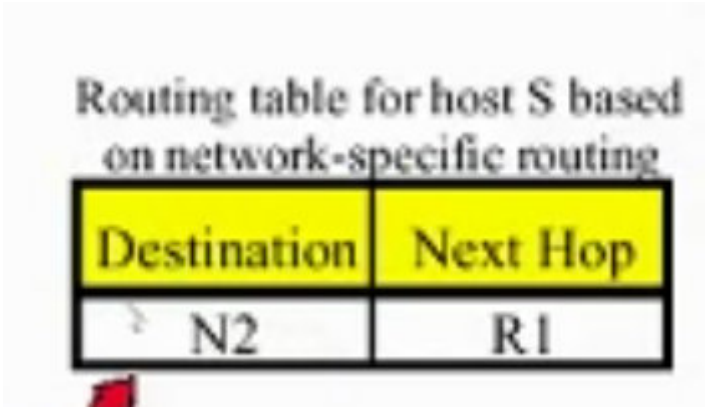
Quindi il datagram viene spedito al prossimo router, e sarà compito di quel router di effettuare il forwarding a sua volta.

Esempi di Routing table



Possiamo trovare all'interno della tabella di inoltro diverse destinazioni. Possiamo avere direttamente gli indirizzi degli host (invece delle interfacce di rete). Per ogni host la tabella ci dice quale router dobbiamo attraversare.

Per ciascuno di questi indirizzi (indicati con A B C D) la tabella ci dice che dobbiamo attraversare il router R1. Questa tabella può essere **compattata** nel seguente modo: invece di indicare tutti gli host di una rete che possiamo raggiungere attraversando un router, possiamo semplicemente dire che per raggiungere **la rete N2** è necessario attraversare il router R1, ottenendo la nuova tabella compattata:



Algoritmo di forwarding usato dai router in presenza di classi

Quando un'interfaccia che deve inoltrare riceve un datagram la prima cosa che fa è estrarre l'indirizzo IP di destinazione e lo analizza; verifica se il prefisso di rete coincide con il prefisso di rete dell'interfaccia mittente. Se i due indirizzi sono uguali allora il compito del livello 3 è finito e si affida al livello 2.

Se le due reti non sono direttamente connesse si verifica se nella routing table esiste una riga dove compare completamente l'indirizzo di destinazione. Se è presente quindi una riga diretta verso l'host di destinazione si usa quella. Se non esiste una **rotta specifica** allora si verifica se esiste una rotta **verso la rete di destinazione** (e non specifico host!); se non esiste una destinazione per la rete a cui appartiene l'indirizzo, si passa a **default**, ovvero si invia il datagram ad un router di default e sarà poi compito suo far arrivare il datagram ad destinazione.

Se non è presente un router di default allora viene ritornato un errore.

Limitazioni dell'addressing basato su classi

E' facilmente intuibile il problema in questo caso: una rete di classe B prevede 16 bit per gli host, quindi è una rete che può ospitare fino a 65234 host. Un indirizzo di classe B che può ospitare tanti host è spesso usato per gestire reti di piccole dimensioni. Venivano usate queste classi di indirizzi e non quelli di classe C (fino a 254 macchine) perchè le reti di classe B erano più facili da gestire, perchè a parità di macchine consentivano di ridurre la dimensione della tabella di instradamento.

Se consideriamo 3 reti di classe C dobbiamo avere 3 righe in una routing table. Se invece ho una rete di classe B che è in grado di gestire più macchine di quante ne possa gestire la terna di reti di classe C, mi conviene.

Soluzioni "momentanee" ai problemi delgi indirizzi IPv4

CIDR - Classless InterDomain Routing

E' la tecnica che oggi viene usata, e sostituisce il meccanismo delle classi viste in precedenza proprio perchè si usa in assenza di classi. L'instradamento delle reti si effettua senza più considerare le classi.

Se non consideriamo le classi, come fa un router a capire da un indirizzo qual è il prefisso di rete? Cambia completamente il modo con cui viene inferito il prefisso di rete: si usa insieme all'indirizzo **una maschera da 32 bit**.

Gli uno presenti all'interno della maschera sono solitamente **contigui**. La maschera viene applicata all'indirizzo di destinazione. con un'operazione di **AND bit a bit**, andando quindi ad effettuare un **filtraggio sull'indirizzo**. Il risultato dell'operazione di AND è **proprio il prefisso di rete.**

A differenza di quanto avveniva con le classi, con il CIDR dobbiamo aggiungere ad ogni indirizzo una maschera e questa maschera sarà usata in AND con gli indirizzi di destinazione. Poichè con le maschere possiamo gestire meglio il prefisso di rete, usiamo una notazione diversa per indicare l'appartenenza di un indirizzo ad una "sorta di classe" (non più presente).

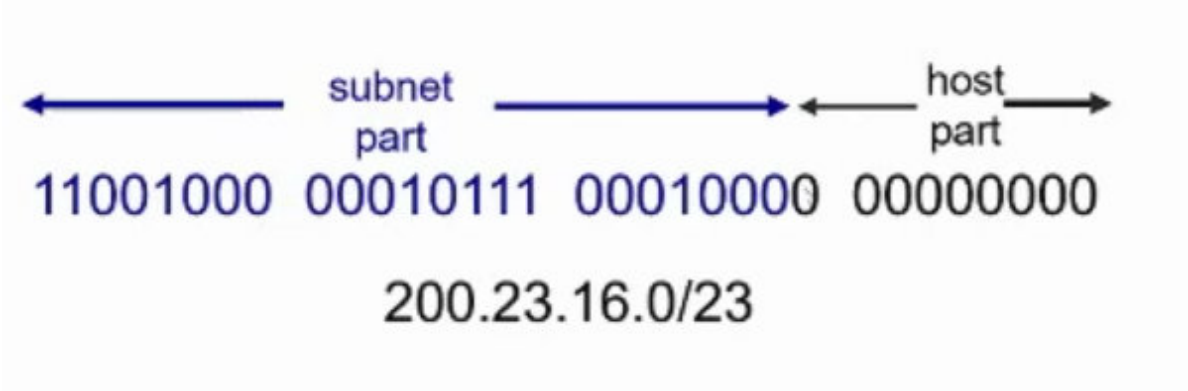
Notazione usata

a.b.c.d è un generico indirizzo IP, mentre **/x** rappresenta un numero che individua il numero di bit nell'indirizzo da considerare come prefisso di rete.

Ad esempio 192.168.10.3/16 dice che questo indirizzo va considerato come un indirizzo il cui prefisso di rete è dato dai primi 16 bit, o primi due byte! Quindi il prefisso di rete sarà **192.168**. Di conseguenza, dire **/16** o di classe **B** non cambia nulla.

La peculiarità potente di questa notazione è che "10.3" potrebbe essere visto come un prefisso di rete diverso, posso scrivere **/24**, e quindi i primi 24 bit saranno considerati come prefisso di rete, e non i primi 16. Possiamo quindi usare un prefisso di rete arbitrario.

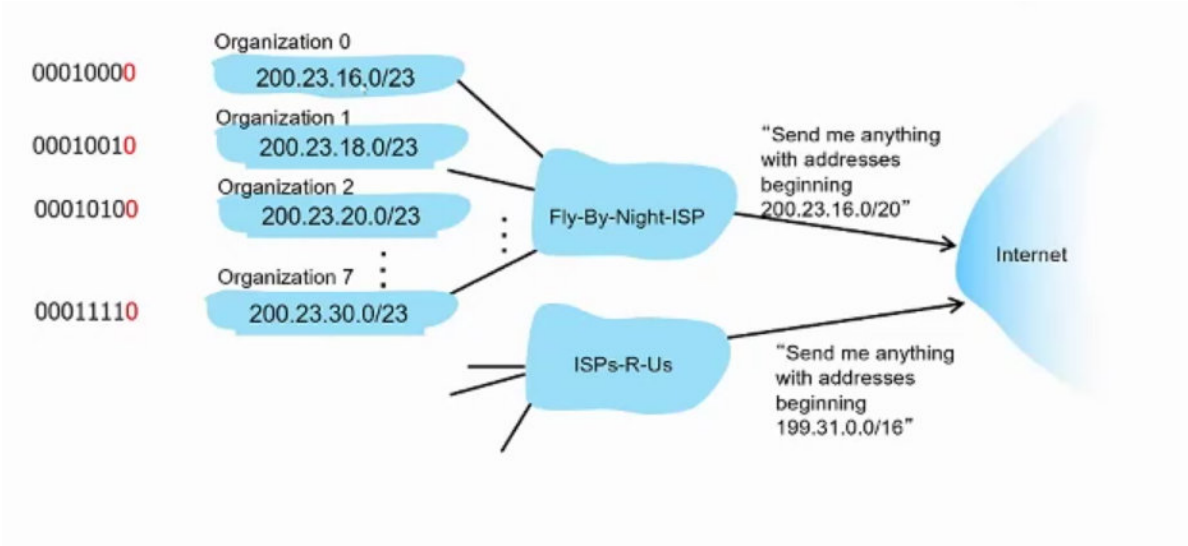
Notazione usata in CIDR



Partiamo con un indirizzo di classe C ma con la notazione /23 stiamo dicendo che l'ultimo bit del terzo byte che apparteneva al prefisso di rete (con le classi), adesso è escluso. Di conseguenza se prima potevamo rappresentare reti pari a 2^8 bit, ora abbiamo aggiunto un bit portando le possibili reti indirizzabili a 2^9 bit, ovvero 510 (512 senza escludere gli indirizzi speciali) bit.

Addressing Gerarchico

Un effetto positivo del CIDR è quello di poter aggregare reti.



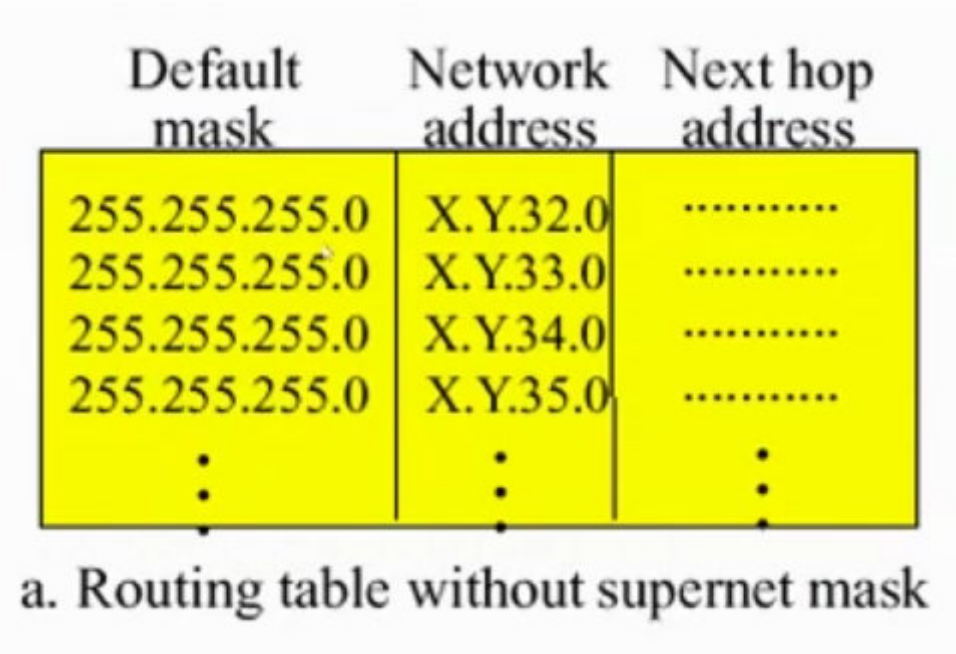
La rete 200.23.16.0/23 , 200.23.18.0/23 , 200.23.20.0/23 ... fino a 200.23.30.0/23 possono essere viste all'esterno con un indirizzo più compatto, che consente di inviare datagram a queste reti attraversando un solo router; posso pensare le maschere (notazione /x) per ridurre le righe all'interno delle routing table, annunciando verso le reti esterne (internet) una rotta con un indirizzo di destinazione compatto, come il seguente: **200.23.16.0/20**.

In questo modo sto aggregando tutte le reti precedenti, e faccio in modo che un datagram destinato ad una di queste reti raggiunga queste reti usando all'interno di internet una routing table che prevede **una sola riga per tutte queste reti**.

Esempio - Supernetting

L'idea è di poter gestire un insieme di reti che sono raggiungibili attraverso **lo stesso router**.
L'idea è di poter usare all'interno delle routing table in internet un'unica riga per raggiungere tutte le destinazioni del router.

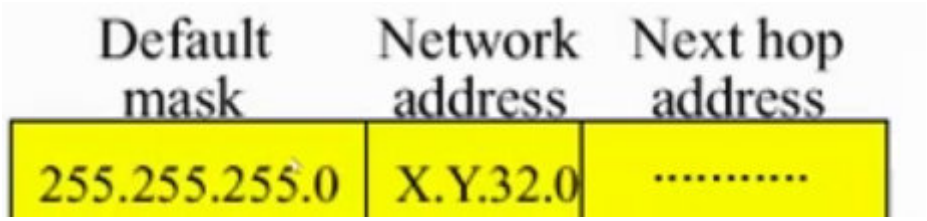
Se non facessi nulla, la tabella di instradamento che dovrei avere in internet per raggiungere le 4 reti di cui abbiamo parlato prima, dovremmo avere qualcosa del genere:



> con CIDR viene aggiunta la colonna che contiene le maschere IP

L'indirizzo IP di destinazione del datagram che deve essere inoltrato che arriverà al router che ha questa tabella, sarà messo in AND con la maschera `255.255.255.0`, ed il risultato di questa operazione sarà confrontato con l'indirizzo (ad esempio X.Y.32.0).

Facciamo un esempio: arriva un datagram con indirizzo IP X.Y.32.10. Applichiamo la maschera 255.255.255.0 e filtriamo il quarto byte; il risultato è X.Y.32.0. Corrisponde con l'indirizzo :



Arriva un altro datagram con indirizzo X.Y.32.20, applichiamo la maschera ed otteniamo X.Y.32.0, ancora una volta corrisponde all'indirizzo IP.

Se arriva un datagram con indirizzo X.Y.34.5, una volta applicata la maschera ci accorgiamo di non avere una corrispondenza con X.Y.32.0 ma con X.Y.34.0.

Quindi come comprimiamo la tabella?

Per comprimere la tabella andiamo a considerare questi indirizzi di rete:

32 →0010000

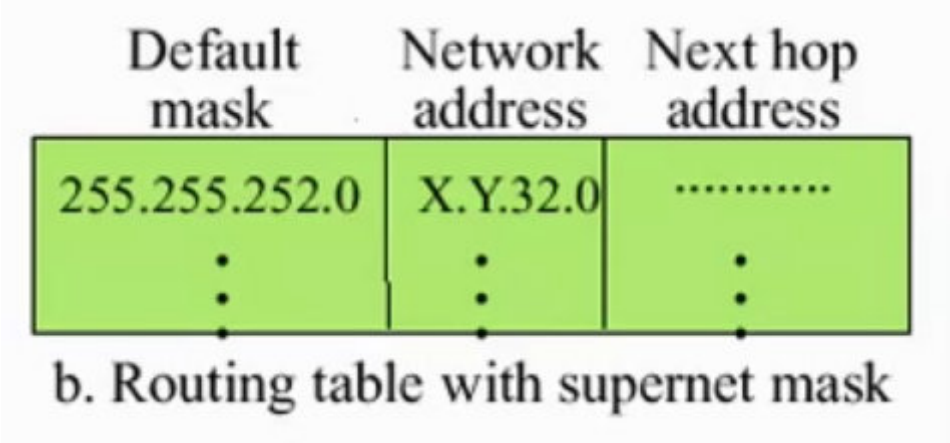
33 →0010001

34 →0010010

35 →0010011

Cerchiamo quindi di capire cosa cambia: dalle notazioni acquisite in campo notazione binaria ci accorgiamo che solo gli ultimi due bit cambiano. Se non considerassimo questi bit finali (meno significativi) del **terzo byte dell'indirizzo**, avrei un ottetto in byte sempre uguale (0010000 -> 32).

Come filtriamo questi bit? Dobbiamo usare una maschera che mi permetta di escludere questi due bit: 11111100 (tutti uno tranne gli ultimi due bit); se convertiamo in decimale questa stringa binaria otteniamo **252**, quindi la maschera da usare per compattare la routing table è:



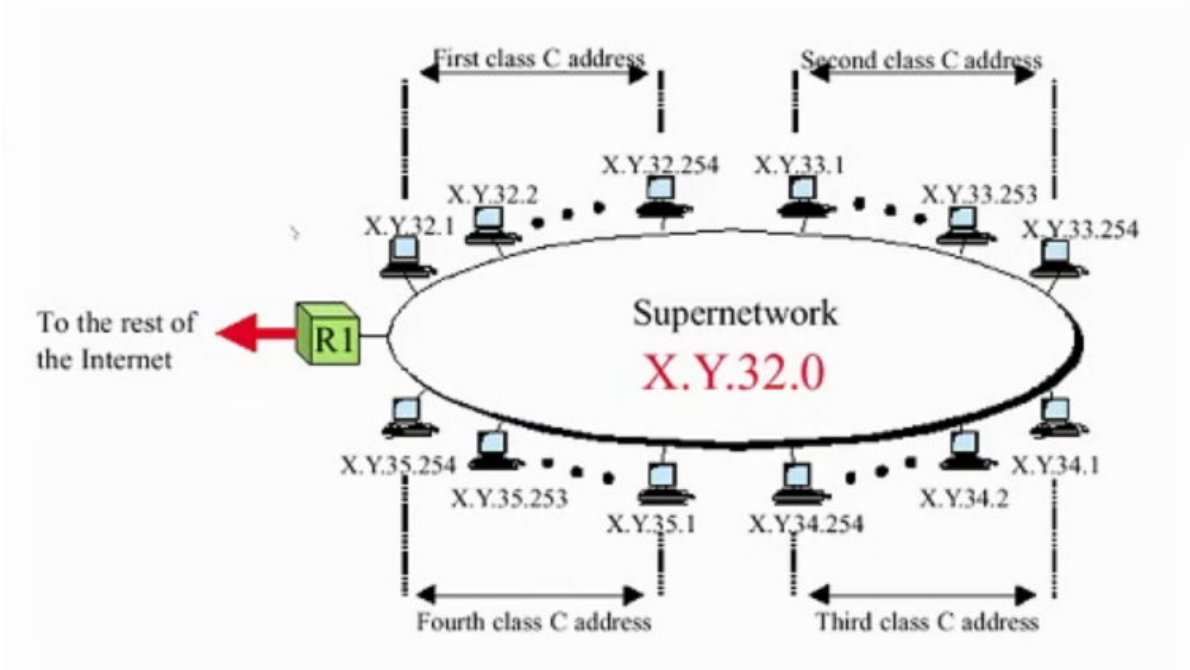
b. Routing table with supernet mask

Di conseguenza, il **prefisso di rete da usare** non è più /24, ma **/22**, per escludere gli ultimi due bit del 3 byte.

Funziona?

Se arriva un datagram che ha un indirizzo di destinazione X.Y.34.5 l'ultimo byte viene completamente filtrato perchè nella maschera l'ultimo byte è posto a zero. Il 34 sarà filtrato parzialmente dal byte **254**, che ha i due bit più a destra a zero.

Di conseguenza otteniamo sempre 00100000, ovvero 32. Qualunque indirizzo IP che ricade in una delle reti da X.Y.32 a X.Y.35.0, con questa maschera (255.255.254.0) produrrà sempre lo stesso indirizzo: X.Y.32.0 .
Di conseguenza **un'unica riga nella routing table** ci consentirà di instradare datagram verso tutte le reti che sono oltre R1:



> Questo ovviamente è fattibile solo quando tutte le reti in questione sono contigue e collocate dietro lo stesso router.

Longest Match Routing Rule

Quando nella tabella di instradamento sono presenti diverse corrispondenze, ovvero applicando la maschera ad un indirizzo di destinazione otteniamo una corrispondenza con la colonna dell'indirizzo di destinazione per diverse righe, viene scelta per la quale il match è avvenuto con una maschera con il maggior numero di 1.

Di conseguenza avere un maggiore di 1 nella maschera significa usare un prefisso di rete più selettivo, e sicuramente da preferire ad una maschera con un numero di bit ad 1 più basso (che probabilmente ha prodotto lo stesso risultato per puro caso).

---

fine lezione 6