Livello di Rete

Ultimo livello nella pila protocollare a base di punto-punto senza pensare a cosa ci sotto

Il percorso è determinato con strategia di circuito virtuale o Datagram

Ognuno ha i suoi vantaggi e svantaggi

	Datagram	Circuito virtuale
Creazione circuito	NO	SI
Info di stato	Indirizzi nei singoli pacchetti	indirizzo di circuito
Instradamento	No-info	Ogni circuito va identificato
Effetti di guasti	Nessuno	Reset di tutti i circuiti che usano il router guasto
Controllo congestione	Complesso	Semplice

Abbiamo nel livello di rete diversi protocolli per:

- instradamento che fanno relazione del percorso
- Protocollo IP | fa conversioni di indirizzamento
  | definisce formato datagram
  | fa conversione per gestione pacchetti
- Protocollo ICMP | gestisce errori
  | gestisce segnalazioni di router

Indirizzo IPV4

Un indirizzo IPV4 è formato da 32 bit.
Gli indirizzi sono raggruppati in classi

classe	Da	A	
A	1.0.0.0	127.255.255.255	← 1 byte per rete, 3 per Host
B	128.0.0.0	191.255.255.255	← 2, 2
C	192.0.0.0	223.255.255.255	← 3, 1
D (multicast)	224.0.0.0	239.255.255.255	
E (riservati)	240.0.0.0		

Ci sono degli altri "pacchetti"

0.0.0.0 this host non valido, a volte rappresenta lo stesso Host

00000 ... xxx Indirizzo valido ma può navigare solo nella rete

255.255.255.255 broadcast

127.0.0.0 - 127.255.255.255 loopback

10.0.0.0 - 10.255.255.255 IP privati

169.254.0.0 - 169.254.255.255 dato dal SO in automatico

Poi ne abbiamo altri privati

172.16.0.0 - 172.31.255

192.168...

La suddivisione in classi è vista, mentre le maschere di sottorete (rete, sottorete, host) → a.b.c.d/x ← maschera (numero dei primi bit a 1 che definiscono l'indirizzo sottorete)

rete – sottorete – host

$0 \leq x \leq 32$

indirizzo sottorete

151.097.252.066
AND
255.255.254.000 ← maschera

} op. di masking

Indicare x o la maschera è equivalente

la maschera di sottorete serve a mascherare l'host (serve per dividere la parte di rete, sottorete e host)

Assegnamento indirizzi IP

Ci sono vari enti che si occupano dell'assegnamento degli indirizzi

RIR – Continente

Sotto abbiamo i LIR (in Italia GARR – LIR) che gestiscono a livello locale.

Formato datagram IPV4

Foto slide

- 4 bit : versione
- 4 ... 7 : IHL (lenght intestazione)
- 8 ... 15 : tos ossia il tipo
- 16 ... 31 lenght datagram
- ID, flags offset : per frammentazione, identifica il datagram
- TTL contatore di salti (per loop infiniti)
- Protocol : ci indica il transport layer
- checksum : se ci sono errori di bit
- Source e dest IP
- Dati e opzioni

Maschera: fatta da 111...000 ci dà un modo per ottenere l'indirizzo di rete, subnet e host.
Essa è applicata con l'AND, in hardware ha il vantaggio di non dover avere per forza il blocco/viaggio del byte, ma lavora bit a bit.

Frammentazione

Si fa perché c'è il MTU = Maximum transfer unit

A volte è necessario perché abbiamo pacchetti grossi. La frammentazione alla sorgente comporta il rimontaggio alla destinazione. (la frammentazione è evitato il più possibile)

Ogni frammento ha lo stesso ID, offset indica appunto la "distanza" dall'inizio del pacchetto

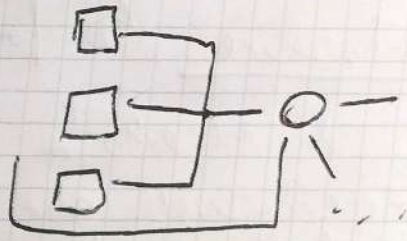
Usano i bit-flag DF, MF.

MF indica se è l'ultimo frammento.

DF indica se è permesso frammentare *1

La maschera serve per isolare gli specifici indirizzi

*1. Identificare una rete



La rete a sinistra ha identificativo 223.1.1.0

Il router al centro ha 3 interfacce di rete, la parte quindi di 3 reti.

Figura 4.17

mento con la rete; quando l'implementazione di IP dell'host vuole inviare un datagramma, lo fa su tale collegamento. Il confine tra host e collegamento fisico viene detto interfaccia. Invece, dato che il compito di un router è ricevere datagrammi da un collegamento e inoltrarli su un altro, questo deve necessariamente essere connesso ad almeno due collegamenti. Anche il confine tra un router e i suoi collegamenti è chiamato interfaccia. Il router presenta più interfacce, una su ciascuno dei suoi collegamenti. Dato che host e router sono in grado di inviare e ricevere datagrammi, IP richiede che tutte le interfacce abbiano un proprio indirizzo IP. Pertanto, l'indirizzo IP

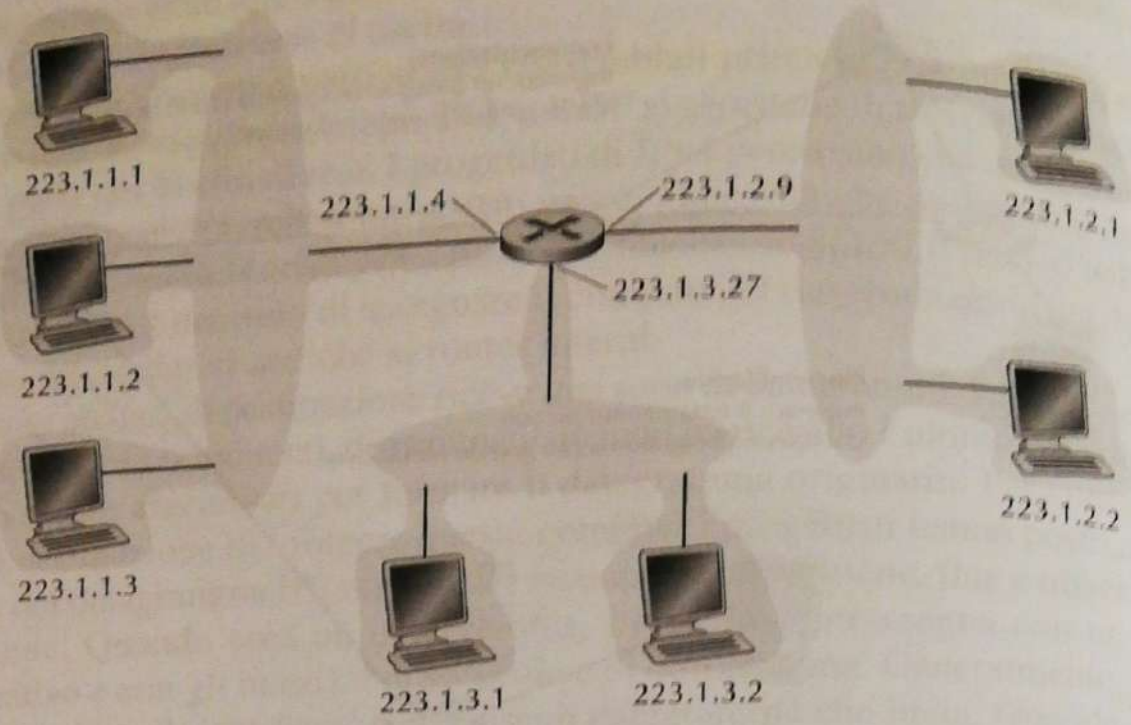


Figura 4.18 Indirizzi delle interfacce e sottoreti.

La Figura 4.18 mostra un router (con tre interfacce) che connette sette host. I tre a sinistra e l'interfaccia del router cui sono connessi hanno un indirizzo IP della forma 233.1.1.xxx: ossia, i 24 bit più a sinistra nell'indirizzo IP sono identici. Le quattro interfacce sono interconnesse da una rete che non contiene router. Se questa rete fosse, per esempio, una LAN Ethernet, le interfacce sarebbero interconnesse da uno switch Ethernet (Capitolo 6) o da un punto di accesso wireless (Capitolo 7). Per adesso rappresentiamo la rete priva di router che connette questi host come una nuvola.

Per IP, questa rete che interconnette tre interfacce di host e l'interfaccia di un router forma una **sottorete** [RFC 950]. Nella letteratura relativa a Internet le sottoreti sono anche chiamate reti IP o semplicemente *reti*. IP assegna a questa sottorete l'indirizzo 223.1.1.0/24, dove la notazione /24, detta anche **maschera di sottorete** (*subnet mask*), indica che i 24 bit più a sinistra dell'indirizzo definiscono l'indirizzo della sottorete. Di conseguenza, la sottorete 223.1.1.0/24 consiste di tre interfacce di host (223.1.1.1, 223.1.1.2, 223.1.1.3) e di un'interfaccia di router (223.1.1.4). Ogni altro host connesso alla sottorete 223.1.1.0/24 deve avere un indirizzo della forma 223.1.1.xxx. La Figura 4.19 riporta gli indirizzi delle tre sottoreti.

dove x indica il numero di bit nella prima parte dell'

Gli x bit più a sinistra di un indirizzo della forma *a.b.c.d/x* costituiscono la porzione di rete dell'indirizzo IP e sono spesso detti **prefisso** (di rete) dell'indirizzo. A un'organizzazione viene generalmente assegnato un blocco di indirizzi contigui con un prefisso comune (si veda al riguardo il Box 4.1) per tutti gli indirizzi IP dei dispositivi che si trovano al suo interno. Quando tratteremo il protocollo di instradamento BGP (Paragrafo 5.4) vedremo che i router esterni alla rete dell'organizzazione considerano solo gli x bit del prefisso, cioè, quando un router all'esterno dell'organizzazione inoltra un datagramma avente un indirizzo di destinazione che è interno, dovrà considerare solo i primi x bit dell'indirizzo. Questo riduce in modo considerevole la dimensione della tabella di inoltro dei router, dato che una sola riga della forma *a.b.c.d/x* è sufficiente per far pervenire i pacchetti all'organizzazione.

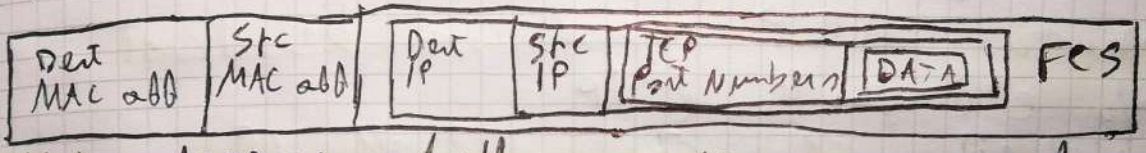
I rimanenti 32-x bit di un indirizzo possono essere usati per distinguere i dispositivi interni dell'organizzazione, che hanno tutti lo stesso prefisso di rete. Saranno quindi i router della rete interna che utilizzeranno i restanti bit dell'indirizzo per indirizzarli al dispositivo destinatario. Tali bit potrebbero presentare un'aggiuntiva struttura di sottorete, come quella trattata precedentemente. Per esempio, supponiamo che

MAC-ADDRESS ogni scheda di rete ne ha una

Per ogni interfaccia di rete abbiamo un indirizzo IP e un MAC ADDRESS

Protocollo ARP per traduzione IP e MAC ADDRESS

Incapsula tutti i pacchetti per creare quello che viene effettivamente spedito (pacchetto ethernet)



Il MAC-ADDRESS della macchina serve solo per comunicare le schede sulla stessa rete

Il MAC ADDRESS si trova a livello LAN, è dato dal costruttore.

Quando una macchina vuole comunicare con un'altra deve avere un modo per passare da IP a MAC ADDRESS e viceversa
L'IP è legato alla posizione nella LAN, il MAC no.
Si usa ARP che fa la "traduzione"
(Le frame viaggiano usando il MAC)
ARP significa Address Resolution Protocol

- Supponiamo di conoscere l'IP del dest.
Prima inviamo ARP request in broadcast, nella info c'è scritto l'IP
È una richiesta che sta a livello IP
Tutte le macchine la analizzano ma solo una non la scarta
La reply verrà inviata solo a chi aveva fatto la request, ma conterrà il MAC-addr che il destinatario voleva sapere.

Qui si usa un TTL pure
Problemi: pagina prima ↩

52

- ARP non prevede autenticazione
- Una reply può essere inviata senza richiesta
- Quando un host riceve pacchetto ARP aggiorna la sua cache ARP

Conseguenza: il traffico IP è facilmente dirottabile