Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2015/16

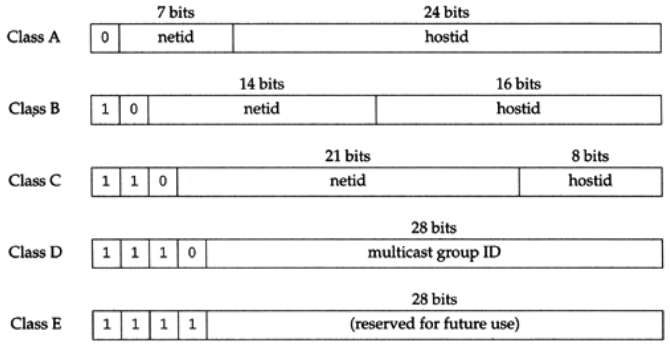
Lezione III: Dal livello link a quello di trasporto

IP

Occorre istradare i pacchetti fra media differenti.

- Ogni nodo è identificato da un numero IP da 32 bit (IPv4), tradizionalmente scritto come 4 ottetti (notazione in base 256)
- L'istradamento (*routing*) avviene tramite nodi gateway che si interfacciano con due o piú LAN

Classi di indirizzo



Classe	intervallo	uso
A	0.0.0.0–127.255.255.255	reti tradizionali
B	128.0.0.0–191.255.255.255	reti tradizionali
C	192.0.0.0–223.255.255.255	reti tradizionali
D	224.0.0.0–239.255.255.255	multicast
E	240.0.0.0–255.255.255.255	altri usi speciali

MAP OF THE INTERNET
THE IPV4 SPACE, 2006

Sottoreti e netmask

La netmask è una sequenza di 32 bit che identifica quali bit sono comuni negli IP all'interno di una LAN (sottorete)

01110111 01110111 01110111 11110111 — 119.119.119.247

7 bit per i nodi — $2^7 = 128$

CIDR

Normalmente si usano i primi bit (non obbligatorio), quindi è comoda la notazione CIDR (Classless InterDomain Routing)

`159.149.30.0/24` 24 bit per le sottoreti, $32 - 24 = 8$ per gli host

Riassumendo

- Il protocollo IP definisce il formato degli indirizzi dei nodi e delle reti in cui essi si trovano
- Il numero IP contiene entrambi

ARP

In una rete locale, il numero IP è *superfluo:* è sufficiente (e necessario) il numero MAC.

- ARP (Address Resolution Protocol): numero MAC da un numero IP

Come funziona

- Ogni nodo mantiene una tabella (ARP cache) in cui ci sono le associazioni già note
- altrimenti si chiede a tutti i nodi della rete locale **chi** ha un certo numero IP

ARP cache poisoning

L'assunzione di **trust** nella LAN...

1. Chi ha il numero IP 192.168.0.2?
2. Sono io: 00:23:a2:d6:f2:15
3. Le comunicazioni dirette a 192.168.0.2 vanno a chi riceve i frame destinati a 00:23:a2:d6:f2:15

In realtà funziona con arp reply (o anche request!) anche non sollecitate.

Che fare?

Una possibile difesa è l'uso di tabelle ARP statiche.

Attenzione: l'ARP poisoning ha anche usi perfettamente legittimi: p.es. per ridondanza o per fare convergere il primo collegamento verso un server di autenticazione.

Riassumendo

- Le reti locali assumono che i nodi collegati condividano una relazione di fiducia
- ARP poisoning: permette di *impersonare* uno o piú nodi della LAN