



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

Sicurezza dei sistemi e delle reti¹

Mattia Monga

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

a.a. 2014/15

¹ © 2011–15 M. Monga. Creative Commons Attribuzione — Condividi allo stesso modo 4.0 Internazionale. <http://creativecommons.org/licenses/by-sa/4.0/deed.it>. Derivato con permesso da © 2010 M. Cremonini.



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

Lezione III: Dal livello link a quello di trasporto

Ethernet



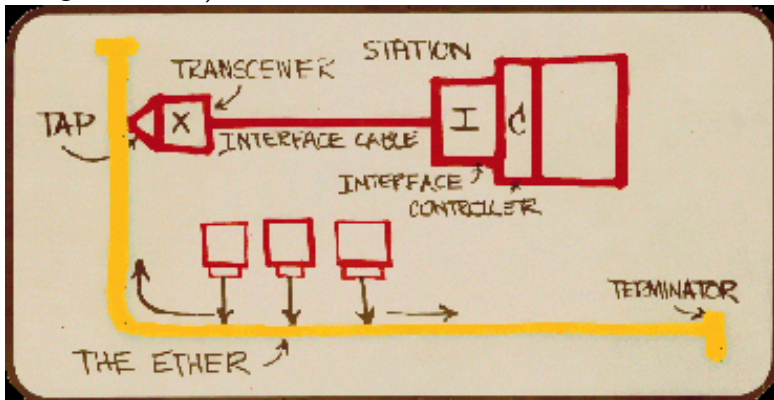
Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

comunicare tramite un medium condiviso (analogo al famigerato *etere*)





Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

- Carrier Sense, Multiple Access with Collision Detection
- indirizzi a 48 bit
- maximum transmission unit (MTU): 1500 bytes
- ... ma c'è anche una dimensione minima: 46 byte (ciò costringe al *padding*)



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

Tutti i nodi connessi (LAN) ricevono **tutti** i frame: scartano quelli non diretti a loro.

Hub e switch



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

L'estensione della rete si amplia con:

Hub semplici ripetitori di segnale
(tutt'al più aiutano nella
collision detection producendo
i *jam frame*)



Hub e switch



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

L'estensione della rete si amplia con:

Switch definiscono diversi *collision domain*: logicamente LAN differenti, che non condividono fra loro il medium





Le schede di rete sono identificate da un numero seriale, che viene utilizzato come indirizzo all'interno della LAN.

- 48 bit, i primi 24 identificano il produttore
- notazione esadecimale (MAC: 00:23:a2:d6:f2:15 (Motorola Mobility, Inc.))



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

Avendo i privilegi adeguati, è quasi sempre possibile (e facile) cambiare il numero MAC usato nella produzione dei frame. Quindi: conoscendo il MAC di una macchina assente, è immediato impersonarla.



La separazione dei collision domain è, in definitiva, solo **logica**.

- La separazione è ottenuta tramite una CAM (*content addressable memory*) che contiene le associazioni MAC-porta dello switch



Se la tabella è generata dinamicamente (molto comodo: basta attaccare i nodi allo switch, l'amministratore divide i collision domain per porta) è possibile saturarla.

La tabella satura non viene utilizzata!



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

- Le reti locali assumono che i nodi collegati condividano una relazione di fiducia
- I numeri MAC sono un identificatore debole
- **MAC flooding**: permette di violare i collision domain imposti dagli switch



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 più LAN

Classi di indirizzo

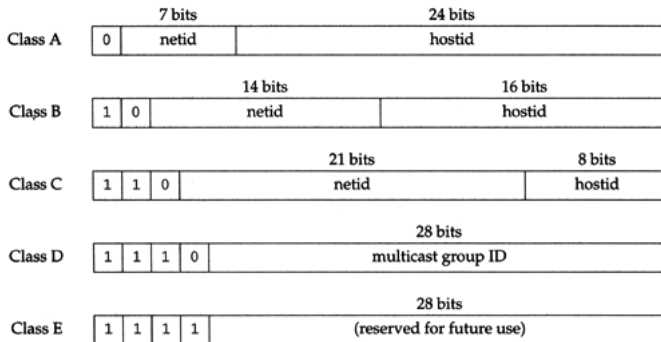


Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP



Classi di indirizzo



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

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

Classi di indirizzo



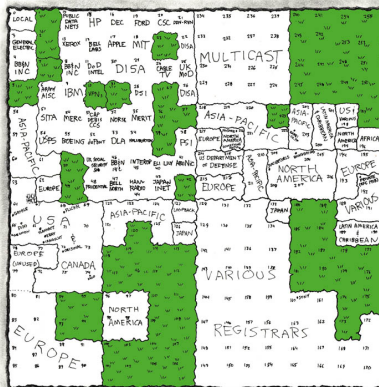
Sicurezza delle reti

Monga

Link layer:
Ethernet

IP

MAP OF THE INTERNET
THE IPv4 SPACE, 2006



THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING--ANY CONSECUTIVE STRING OF IP's WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IP's THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.

0 1 14 15 16 19 →
3 2 13 12 17 18
4 7 8 11
5 6 9 10



= UNALLOCATED BLOCK



Classe	intervallo	uso
A	10.0.0.0–10.255.255.255	intranet
B	172.16.0.0–172.31.255.255	intranet
C	192.168.0.0–192.168.255.255	intranet

Secondo le specifiche i router devono *scartare* (o manipolare. . .) i pacchetti contrassegnati con questi indirizzi.



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 $2^7 = 128$



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



Sicurezza delle
reti

Monga

Link layer:
Ethernet

IP

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