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 II: Il modello di riferimento

Il modello di riferimento OSI

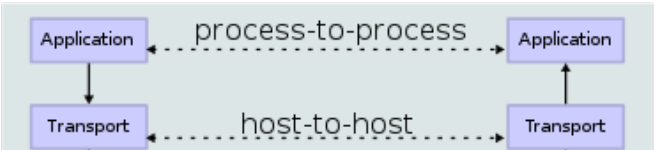
Application	Data
Presentation	
Session	
Transport	Segment
Network	Packet
Data link	Frame
Physical	Bit

Stack dei protocolli Internet

Un modello semplificato (*TCP/IP Illustrated*, W. Stevens)

Application	Telnet, FTP, e-mail, etc.
Transport	TCP, UDP
Network	IP, ICMP, IGMP
Link	device driver and interface card

È uno stack narrow waist: lo strato IP è molto difficile da cambiare.



Principi architetturali

end-to-end principle L'*intelligenza* ai vertici della rete, che trasmette i dati nella maniera piú efficiente;

robustness approach Conservatori nel mandare, liberali nel ricevere.

Lettura obbligatoria: E. Allman. *The robustness principle reconsidered.* CACM 54, 8 (August 2011), 40–45.

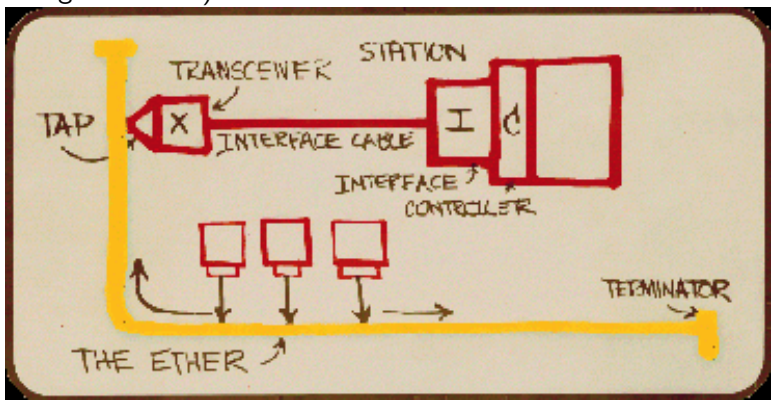
Riassumendo

La suite TCP/IP è basata su:

- 4 livelli: *link, network, transport, application*
- *end-to-end principle*
- *robustness approach*

Ethernet

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



Caratteristiche del protocollo

- 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*)

Dal punto di vista della sicurezza

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

Hub e switch

L'estensione della rete si amplia con:

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

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

MAC

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.)`)

Affidabilità dei MAC number

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*.

Sicurezza con gli switch

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

MAC flooding

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!

Riassumendo

- 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