



Sicurezza delle reti¹

Mattia Monga

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

a.a. 2010/11

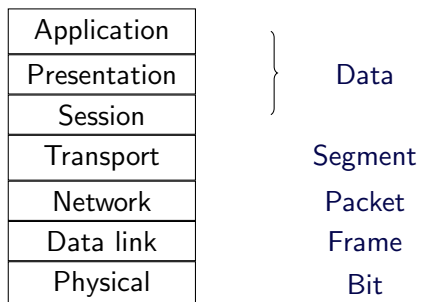
¹ © 2011 M. Monga. Creative Commons Attribuzione-Condividi allo stesso modo 2.5 Italia License.
<http://creativecommons.org/licenses/by-sa/2.5/it/>. Materiale derivato da © 2010 M. Cremonini.



Lezione II: I protocolli di base

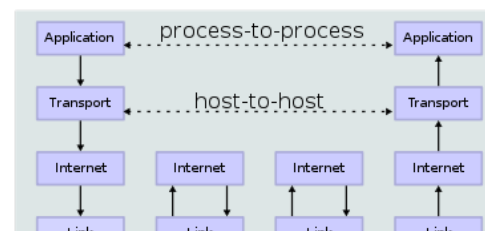
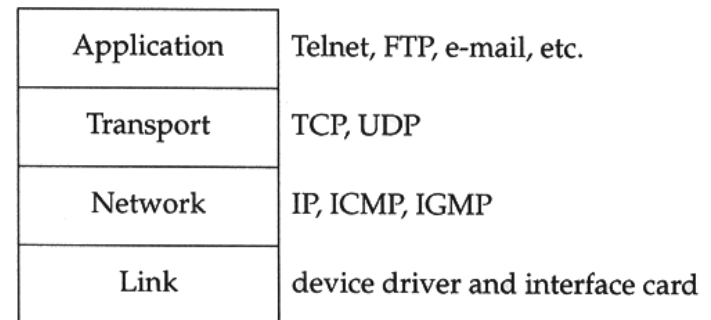


Il modello di riferimento OSI



Stack dei protocolli Internet

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



Principi architetturali



Sicurezza delle reti

Monga

La pila protocollare

Ethernet

IP

ARP

ARP cache poisoning

Riassunto

end-to-end principle L'*intelligenza* sta ai vertici della rete, che ha l'unico compito di trasmettere i dati nella maniera piú efficiente possibile;

robustness approach Conservatori nel mandare, liberali nel ricevere.

Entrambi questi principi hanno importanti ricadute dal punto di vista della sicurezza.

16

Ethernet



Sicurezza delle reti

Monga

La pila protocollare

Ethernet

IP

ARP

ARP cache poisoning

Riassunto

- Protocollo pensato per comunicare tramite un medium condiviso (analogo al famigerato *etere*)
- 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*)

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

17

Hub e switch



Sicurezza delle reti

Monga

La pila protocollare

Ethernet

IP

ARP

ARP cache poisoning

Riassunto

Per ampliare l'estensione della rete, i nodi Ethernet possono essere collegate tramite:

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

18

MAC



Sicurezza delle reti

Monga

La pila protocollare

Ethernet

IP

ARP

ARP cache poisoning

Riassunto

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
- normalmente indicati con notazione esadecimale (MAC: 00:23:a2:d6:f2:15 (Motorola Mobility, Inc.))

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*.

19



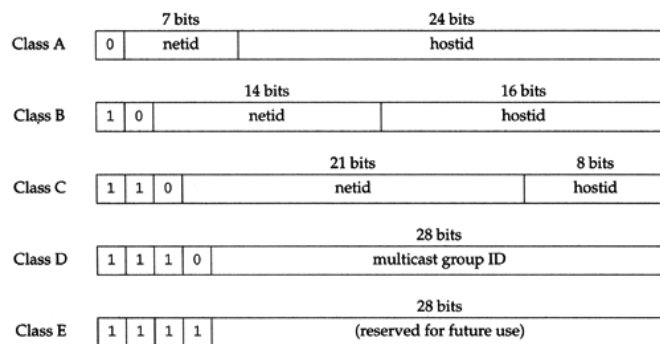
Gli switch, separando i collision domain, limitano la condivisione del medium di trasmissione. La separazione, però, è solo logica.

- 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 saturata con tecniche di MAC flooding non viene più utilizzata e i frame arrivano a tutti, come se lo switch non ci fosse!



Il livello network prevede nodi potenzialmente appartenenti a LAN differenti: 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'istridamento (*routing*) avviene tramite nodi gateway che si interfacciano con due o più LAN



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



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 (anche se non è obbligatorio), per cui risulta comoda la notazione CIDR (Classless InterDomain Routing)
159.149.30.0/24 24 bit per le sottoreti, 32 – 24 = 8 per gli host



All'interno di una rete locale, il numero IP è *superfluo*: per comunicare con un altro nodo è sufficiente (e necessario) il numero MAC.

- ARP (Address Resolution Protocol) serve a ricavare il numero MAC a partire da un numero IP
- 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



Il protocollo ARP mette in luce in maniera molto chiara l'assunzione di *trust* fra i nodi di una rete che condivide il medium di trasmissione

- 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
- 4 Possibile far coincidere molti numeri IP con un unico numero MAC!

Una possibile difesa è l'uso di tabelle ARP statiche. Si noti che l'ARP poisoning ha anche usi perfettamente legittimi: per esempio spesso nelle reti wireless è il modo utilizzato per fare convergere il primo collegamento verso un server di autenticazione.



- Le reti locali assumono che i nodi collegati condividano una relazione di fiducia
- I numeri MAC sono un identificatore debole
- Attacchi classici
 - MAC flooding: permette di violare i collision domain imposti dagli switch
 - ARP spoofing: permette di *impersonare* uno o più nodi della LAN